DEPARTMENT OF HOMELAND SECURITY

Cybersecurity and Infrastructure Security Agency

6 CFR Part 226

[Docket No. CISA-2022-0010]

RIN 1670-AA04

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS

ACTION: Proposed rule.

SUMMARY: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

DATES: Comments and related material must be submitted on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: You may send comments, identified by docket number CISA-2022-0010, through the Federal eRulemaking Portal available at http://www.regulations.gov.

Instructions: All comments received must include the docket number for this rulemaking. All comments received will be posted to https://www.regulations.gov, including any personal information provided. If you cannot submit your comment using https://www.regulations.gov, contact the person in the FOR FURTHER INFORMATION

CONTACT section of this proposed rule for alternate instructions. For detailed instructions on sending comments and additional information on the types of comments that are of particular interest to CISA for this proposed rulemaking, see the "Public Participation" heading of the SUPPLEMENTARY INFORMATION section of this document.

Docket: For access to the docket and to read background documents mentioned in this proposed rule and comments received, go to https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Todd Klessman, CIRCIA Rulemaking Team Lead, Cybersecurity and Infrastructure Security Agency, circia@cisa.dhs.gov, 202-964-6869.

SUPPLEMENTARY INFORMATION:

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS FREQUENTLY USED IN THIS DOCUMENT

ARIN	American Registry for Internet Numbers
ATO	Authority to Operate
BES	Bulk Electric System
CFATS	Chemical Facility Anti-Terrorism Standards
CFTC	Commodity Futures Trading Commission
CHS	U.S. House Committee on Homeland Security
CIA	Confidentiality, Integrity, and Availability
CIP	Critical Infrastructure Protection
CIRC	Cyber Incident Reporting Council
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended
CISA	Cybersecurity and Infrastructure Security Agency
CSP	Cloud Service Provider
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DNS	Domain Name System
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EPA	Environmental Protection Agency
ESA	Educational Service Agency
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FDIC	Federal Deposit Insurance Corporation

FedRAMP	Federal Risk and Authorization Management Program
FERC	Federal Energy Regulatory Commission
FHFA	Federal Housing Finance Agency
FICU	Federally Insured Credit Union
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
GAO	Government Accountability Office
GCC	Government Coordinating Council
GSA	General Services Administration
gTLD	Generic Top-Level Domain
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HSGAC	U.S. Senate Committee on Homeland Security and Governmental Affairs
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IHE	Institute of Higher Education
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
IT	Information Technology
K-12	Kindergarten through 12th Grade
LEA	Local Educational Agency
MTSA	Maritime Transportation Security Act
NAICS	North American Industry Classification System

NCF	National Critical Function
NCUA	National Credit Union Administration
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NORS	Network Outage Reporting System
NPRM	Notice of Proposed Rulemaking
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OCC	Office of the Comptroller of the Currency
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OT	Operational Technology
OTRB	Over-the-Road Bus
POTW	Publicly Owned Treatment Works
PPD	Presidential Policy Directive
PRA	Paperwork Reduction Act
PTPR	Public Transportation and Passenger Railroads
RFI	Request for Information
RIR	Regional Internet Registry
RTR	Research and Test Reactor
RSO	Root Server Operator
SBA	Small Business Administration
SCC	Sector Coordinating Council
SEA	State Educational Agency
SEC	Securities and Exchange Commission

SLTT	State, Local, Tribal, or Territorial
SRMA	Sector Risk Management Agency
SSP	Sector-Specific Plan
TLD	Top-Level Domain
TSA	Transportation Security Administration
TTP	Tactics, Techniques, and Procedures
USCG	United States Coast Guard
USDA	United States Department of Agriculture
VoIP	Voice over Internet Protocol

I. Public Participation

The Cybersecurity and Infrastructure Security Agency (CISA) views public participation as essential to effective rulemaking and invites interested persons to participate by submitting data, comments, and other information on the content and assumptions made in this proposed rule. Your comments can help shape the outcome of this rulemaking. CISA is particularly interested in comments on the following:

a. *Proposed Definitions*. The proposed definition of covered cyber incident and the other definitions CISA is proposing to include in the regulation (see proposed § 226.1 and Section IV.A in this document);

b. *Applicability.* The proposed description of covered entity, the scope of entities to whom this regulation applies (see proposed § 226.2 and Section IV.B in this document);

c. *Examples of Reportable Covered Cyber Incidents*. The examples of substantial cyber incidents included in this Notice of Proposed Rulemaking (NPRM) (see Section IV.A.ii.3.e in this document);

d. *CIRCIA Reporting Requirements and Procedures.* The proposed reporting requirements and procedures for CIRCIA Reports, specifically the manner, form, and content of CIRCIA Reports (see proposed §§ 226.6 through 226.12 and Section IV.E.i-iii in this document), including CISA's proposal to use a single, dynamic, web-based form as the primary means of submission for all CIRCIA Reports (see Section IV.E.i.2 in this document);

e. *Proposed CIRCIA Report Submission Deadlines*. The proposed deadlines for submitting CIRCIA Reports and CISA's proposed interpretations of these submission deadline requirements (see proposed § 226.5 and Section IV.E.iv in this document);

f. *Data and Records Preservation Requirements.* The proposed data and records preservation requirements and preservation period (see proposed § 226.13 and Section

IV.F in this document);

g. *Enforcement Procedures*. The proposed enforcement procedures, including the procedures related to issuance of a Request for Information (RFI) or subpoena and the proposed subpoena withdrawal and appeals process (see proposed §§ 226.14 through 226.17 and Section IV.G in this document);

h. *Treatment of Information and Restrictions on Use*. The proposed rules governing the protections and restrictions on the use of CIRCIA Reports, information included in such reports, and responses to RFIs (see proposed § 226.18 and Section IV.H.i in this document); and

i. *Procedures for Protecting Privacy and Civil Liberties*. The proposed procedures governing the protection of personal information contained in CIRCIA Reports and responses to RFIs (see proposed § 226.19 and Section IV.H.ii in this document), which are further described in the draft Privacy and Civil Liberties Guidance for CIRCIA (this draft document is available in the docket for this proposed regulatory action (CISA-2022-0010)).

CISA is including in the docket a draft privacy and civil liberties guidance document that would apply to CISA's retention, use, and dissemination of personal information contained in a CIRCIA Report and guide other Federal departments and agencies with which CISA will share CIRCIA Reports. CISA encourages interested readers to review this draft guidance and to submit comments on it. Commenters should clearly identify which specific comment(s) concern the draft guidance document.

CISA will accept comments no later than the date provided in the **DATES** section of this document. Interested parties may submit data, comments, and other information using any of the methods described in the **ADDRESSES** section of this document. To ensure appropriate consideration of your comment, indicate the specific section of this proposed rule and, if applicable, the specific comment request number associated with the

topic to which each comment applies; explain a reason for any suggestion or recommendation; and include data, information, or authority that supports the recommended course of action. Comments submitted in a manner other than those described above, including emails or letters sent to Department of Homeland Security (DHS) or CISA officials, will not be considered comments on the proposed rule and may not receive a response from CISA.

Instructions to Submit Comments. If you submit a comment, you must submit it to the docket associated with CISA Docket Number CISA-2022-0010. All submissions may be posted, without change, to the Federal eRulemaking Portal at www.regulations.gov and will include any personal information that you provide. You may choose to submit your comment anonymously. Additionally, you may upload or include attachments with your comments. Do not upload any material in your comments that you consider confidential or inappropriate for public disclosure. Do not submit comments that include trade secrets, confidential commercial or financial information, Protected Critical Infrastructure Information, Sensitive Security Information, or any other protected information to the public regulatory docket. Please submit comments containing protected information separately from other comments by contacting the individual listed in the FOR FURTHER INFORMATION CONTACT section of this document for instructions on how to submit comments that include protected information. CISA will not place comments containing protected information in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. CISA will hold such comments in a separate file to which the public does not have access and place a note in the public docket documenting receipt. If CISA receives a request for a copy of any comments submitted containing protected information, CISA will process such a request consistent with the Freedom of Information Act (FOIA), 5 U.S.C. 552, and the

Department's FOIA regulation found in part 5 of title 6 of the Code of Federal Regulations (CFR).

To submit a comment, go to www.regulations.gov, type CISA-2022-0010 in the search box and click "Search." Next, look for this *Federal Register* notice of proposed rulemaking in the Search Results column, and click on it. Then click on the **Comment** option. If you cannot submit your comment by using https://www.regulations.gov, call or email the point of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Viewing material in docket. For access to the docket and to view documents mentioned in this NPRM as being available in the docket, go to https://www.regulations.gov, search for the docket number provided in the previous paragraph, and then select "Supporting & Related Material" in the Document Type column. Public comments will also be placed in the docket and can be viewed by following instructions on the Frequently Asked Questions webpage https://www.regulations.gov/faq. The Frequently Asked Questions page also explains how to subscribe for email alerts that will notify you when comments are posted or if another *Federal Register* document is published. CISA will review all comments received. CISA may choose to withhold information provided in comments from public viewing or to not post comments that CISA determines are off-topic or inappropriate.

Public meeting. CISA does not plan to hold additional public meetings at this time, but may consider doing so if CISA determines from public comments that a meeting would be helpful. If CISA decides to hold a public meeting, a notice announcing the date, time, and location for the meeting will be issued in a separate *Federal Register* notice.

II. Executive Summary

A. Purpose and Summary of the Regulatory Action

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. See 6 U.S.C. 681 – 681g; Pub. L. 117-103, as amended by Pub. L. 117-263 (Dec. 23, 2022). CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report. 6 U.S.C. 681b(a)(1)-(3). CIRCIA further requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing an NPRM no later than March 15, 2024, and a final rule within 18 months of publication of the NPRM. 6 U.S.C. 681b(b). CISA is issuing this NPRM to solicit public comment on proposed regulations that would codify these reporting requirements.

This NPRM is divided into six sections. Section I – Public Participation describes the process for members of the public to submit comments on the proposed regulations and lists specific topics on which CISA is particularly interested in receiving public comment. Section II – Executive Summary contains a summary of the proposed regulatory action and the anticipated costs and benefits of the proposed regulations. Section III – Background and Purpose contains a summary of the legal authority for this proposed regulatory action; an overview of the current regulatory cyber incident reporting landscape; a description of the purpose of the proposed regulations; a discussion of efforts CISA has taken to harmonize these proposed regulations with other Federal cyber incident reporting regulations; a discussion of information sharing activities related to the proposed regulations; and a summary of the comments CISA received in response to an RFI issued by CISA on approaches to the proposed regulations and during listening sessions hosted by CISA on the same topic. Section IV – Discussion of Proposed Rule includes a detailed discussion of the proposed rule, the justification for CISA's specific proposals, and the alternatives considered by CISA. Section V –

Statutory and Regulatory Analyses contains the analyses that CISA is required by statute or Executive Order to perform as part of the rulemaking process prior to issuance of the final rule, such as the Initial Regulatory Flexibility Analysis and Unfunded Mandates Reform Act analysis. Section VI contains the proposed regulatory text.

The proposed rule is comprised of 20 sections, §§ 226.1 through 226.20, beginning with a section containing definitions for a number of key terms used throughout the proposed regulation. Among other definitions, § 226.1 includes proposed definitions for the terms used to describe and ultimately scope what types of incidents must be reported to CISA (i.e., cyber incident, covered cyber incident, ransom payment, and substantial cyber incident) and the term used to describe the different types of reports that must be submitted (i.e., CIRCIA Reports).

The next section of the proposed rule, § 226.2, describes the applicability of the proposed rule to certain entities in a critical infrastructure sector, i.e., those entities that are considered covered entities and to whom the operative provisions of the rule would apply.

The next section of the proposed rule, § 226.3, describes the circumstances under which a covered entity must submit a CIRCIA Report to CISA. This includes when a covered entity experiences a covered cyber incident, makes a ransom payment, has another entity make a ransom payment on its behalf, or acquires substantial new or different information after submitting a previous CIRCIA Report. See § 226.3; Section IV.C in this document. CISA is proposing three exceptions to these reporting requirements for covered entities, which are in § 226.4 of the proposed regulation and described in Section IV.D in this document. These exceptions include when a covered entity reports substantially similar information in a substantially similar timeframe to another Federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency; when an

incident impacts certain covered entities related to the Domain Name System (DNS); and when Federal agencies are required by the Federal Information Security Modernization Act of 2014 (FISMA) to report incidents to CISA. See § 226.4 of the proposed regulation and Section IV.D of this document.

Section 226.5 of the proposed regulation contains the submission deadlines for the four different types of CIRCIA Reports (i.e., Covered Cyber Incident Reports; Ransom Payment Reports; Joint Covered Cyber Incident and Ransom Payment Reports; Supplemental Reports). These deadlines, including how to calculate them, are discussed further in Section IV.E.iv in this document. Section 226.6 of the proposed regulation sets forth the proposed manner and form of reporting, which CISA proposes to be through a web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director. Additional details on the proposed manner and form of reporting and related submission procedures are contained in Sections IV.E.i, ii and v in this document. The information CISA proposes that covered entities must include in each of the four types of CIRCIA Reports is enumerated in §§ 226.7 through 226.11 and expanded upon in Section IV.E.iii in this document.

A covered entity may use a third party to submit a CIRCIA Report to CISA on the covered entity's behalf to satisfy the covered entity's reporting obligations. See 6 U.S.C. 681b(d). The proposed procedures and requirements for using a third party to submit a CIRCIA Report on behalf of the covered entity are contained in § 226.12 of the proposed regulations and discussed in detail in Section IV.E.v.3 in this document. The proposed regulation also affirms the statutorily mandated obligation for a third party to advise the covered entity of its ransom payment reporting obligations under CIRCIA when the third party knowingly makes a ransom payment on behalf of a covered entity. See 6 U.S.C. 681b(d)(4), § 226.12(d) of the proposed regulations, and Section IV.E.v.3.e of the NPRM.

Section 226.13 of the proposed regulation sets forth the proposed data and records preservation requirements. It includes a recitation of the types of data and records that a covered entity must preserve; the required preservation period; the format or form in which the data and records must be preserved; and the storage, protection, and allowable uses of the preserved data and records. See § 226.13 and Section IV.F in this document.

CIRCIA authorizes CISA to use various mechanisms to obtain information from a covered entity about a covered cyber incident or ransom payment that was not reported in accordance with CISA's proposed regulatory reporting requirements. 6 U.S.C. 681d. These mechanisms include the issuance of an RFI; the issuance of a subpoena; a referral to the Attorney General to bring a civil action in District Court to enforce a subpoena; and acquisition, suspension, and debarment enforcement procedures. The proposed procedures for each of these enforcement mechanisms are contained in §§ 226.14 through 226.17 of the proposed regulation and discussed in Section IV.G.i – vi in this document.

CIRCIA provides a variety of requirements related to the treatment and restrictions on the use of CIRCIA Reports, information contained in such reports, as well as information submitted in response to an RFI. See 6 U.S.C. 681e(b), 681e(a)(1), (5). CIRCIA also provides liability protection for the submission of a CIRCIA Report in compliance with the reporting requirements established in the CIRCIA regulation. 6 U.S.C. 681e(c). To ensure that such requirements related to the treatment and restrictions on the use of CIRCIA Reports are applied consistently, CISA proposes to include them in § 226.18, as discussed in Section IV.H.i in this document. CISA additionally proposes steps to minimize the collection of unnecessary personal information in CIRCIA Reports and additional procedures for protecting privacy and civil liberties related to the submission of CIRCIA Reports and responses to RFIs. These proposed procedures for protecting privacy and civil liberties are contained in § 226.19 of the proposed regulation

and discussed further in Section IV.H.ii in this document as well as in the guidance document posted to the docket for this proposed rule.

The final section of the proposed regulation, § 226.20, proposes two distinct procedural provisions. The first proposed provision provides that any person who knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, RFI response, or reply to an administrative subpoena is subject to penalties under 18 U.S.C. 1001. § 226.20(a). The second proposed provision is a severability clause, which states CISA intends the various provisions of this part to be severable from each other to the extent practicable, such that if a court of competent jurisdiction were to vacate or enjoin any one provision, the other provisions remain in effect unless they are dependent upon the vacated or enjoined provision. § 226.20(b). These are discussed in Sections IV.G.vii and IV.I in this document, respectively.

B. Summary of Costs and Benefits

CISA estimates the cost of this proposed rule would be $2.6 billion over the period of analysis[1] (undiscounted). CISA estimates that there will be 316,244 entities potentially affected by the proposed rule (i.e., covered entities) who collectively will submit an estimated total of 210,525 CIRCIA Reports over the period of analysis, resulting in $1.4 billion (undiscounted) in cost to industry and $1.2 billion (undiscounted) in cost to the Federal Government. The cost over the period of analysis discounted at 2% would be $2.4 billion ($1.3 billion for industry, $1.1 billion for government), with an annualized cost of $244.6 million, as presented in the Preliminary Regulatory Impact Analysis (RIA) included in the docket. The main industry cost drivers of this proposed

[1] CISA used an 11-year period of analysis spanning from 2023–2033 to reflect that CISA began incurring costs related to CIRCIA implementation in 2023, one year prior to the publication of the NPRM. See the Executive Summary section of the *CIRCIA Regulation Proposed Rulemaking Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis* for additional detail on the period of analysis.

rule are the initial costs associated with becoming familiar with the proposed rule, followed by the recurring data and records preservation requirements, and then reporting requirements. Other industry costs include those associated with help desk calls and enforcement actions. Government costs include costs CISA anticipates incurring associated with the creation, implementation, and operation of the government infrastructure needed to run the CIRCIA program. This includes both personnel and technology costs necessary to support the receipt, analysis, and sharing of information from CIRCIA Reports submitted to CISA.

The Preliminary RIA also discusses the qualitative benefits of the proposed rule. From a qualitative benefits perspective, the proposed reporting requirements, analytical activities, and information sharing will lead to Federal and non-Federal stakeholders having the ability to adopt an enhanced overall level of cybersecurity and resiliency, resulting in direct, tangible benefits to the nation. For example:

- By supporting CISA's ability to share information that will enable non-Federal and Federal partners to detect and counter sophisticated cyber campaigns earlier with the potential for significant avoided or minimized negative impacts to critical infrastructure or national security, CIRCIA's mandatory reporting requirements reduce the risks associated with those campaigns.
- By facilitating the identification and sharing of information on exploited vulnerabilities and measures that can be taken to address those vulnerabilities, incident reporting enables entities with unremediated and unmitigated vulnerabilities on their systems to take steps to remedy or mitigate those vulnerabilities before they also fall victim to cyberattack.
- By supporting sharing of information about common threat actor tactics, techniques, and procedures with the IT community, cyber incident reporting

will enable software developers and vendors to develop more secure products or send out updates to add security to existing products, better protecting end users.

- By enabling rapid identification of ongoing incidents and increased understanding of successful mitigation measures, incident reporting increases the ability of impacted entities and the Federal government to respond to ongoing campaigns faster and mitigate or minimize the consequences that could result from them.
- Law enforcement entities can use the information submitted in reports to investigate, identify, capture, and prosecute perpetrators of cybercrime, getting malicious cyber actors off the street and deterring future actors.
- By contributing to a more accurate and comprehensive understanding of the cyber threat environment, incident reporting allows for CISA's Federal and non-Federal stakeholders to more efficiently and effectively allocate resources to prevent, deter, defend against, respond to, and mitigate significant cyber incidents.

These benefits, which stem from CISA receiving cyber incident and ransom payment reporting for aggregation, analysis, and information sharing, directly contribute to a reduction in economic, health, safety, and security consequences associated with cyber incidents by reducing the number of cyber incidents successfully perpetrated and mitigating the consequences of those cyber incidents that are successful by catching them earlier. It is worth noting that these benefits are not limited to covered entities required to report under CIRCIA, but also inure to entities not subject to CIRCIA's reporting requirements as they too will receive the downstream benefits of enhanced information sharing, more secure technology products, and an ability to better defend their networks based on sector-specific and cross-sector understandings of the threat landscape.

CISA also anticipates qualitative benefits stemming from the data and record preservation requirements of this proposed rule. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom.

III. Background and Purpose

A. Legal Authority

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. See 6 U.S.C. 681 – 681g; Pub. L. 117-103, as amended by Pub. L. 117-263 (Dec. 23, 2022). CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made. 6 U.S.C. 681b(a). Among other benefits, this new authority will enhance CISA's ability to identify trends and track cyber threat activity across the cyber threat landscape beyond the Federal agencies that are already required to report information on certain cyber incidents to CISA pursuant to the FISMA, 44 U.S.C. 3554(b)(7)(C)(ii) and 6 U.S.C. 652(c)(3). CIRCIA requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing a Notice of Proposed Rulemaking no later than March 15, 2024, and a final rule within 18 months of the NPRM's publication. 6 U.S.C. 681b(b).

CIRCIA also authorizes CISA to request information and engage in administrative enforcement actions to compel a covered entity to disclose information if it has failed to comply with its reporting obligations. 6 U.S.C. 681d. CIRCIA establishes information treatment requirements and restrictions on use, including certain protections against liability and exemptions from public disclosure, for required reports and

information submitted to CISA. 6 U.S.C. 681e, 681d(b)(2), 681c(c). CIRCIA also provides for Federal interagency coordination and sharing of information on cyber incidents, including ransomware attacks, reported to Federal departments and agencies, and covered cyber incidents and ransom payments reported to CISA. 6 U.S.C. 681a(a)(10), (b), 681g.

Although CIRCIA requires CISA to implement new reporting requirements through regulation, CISA's rulemaking authority under CIRCIA does not supersede, abrogate, modify, or otherwise limit any authority to regulate or act with respect to the cybersecurity of an entity vested in any United States Government officer or agency. 6 U.S.C. 681b(h). Therefore, covered entities that are obligated to report covered cyber incidents or ransom payments pursuant to another Federal regulatory requirement, directive, or similar mandate will remain obligated to do so even if the reporting requirements differ from those established by CIRCIA. Where CIRCIA imposes regulatory requirements that may overlap or duplicate other Federal regulatory requirements, CISA is committed to working with other Federal partners to explore options to minimize unnecessary duplication between CIRCIA's reporting requirements and other Federal cyber incident reporting requirements and welcomes public comment regarding options to minimize unnecessary duplication or identification of specific Federal cyber incident reporting requirements where such duplication is likely to occur. Additionally, CIRCIA does not permit or require a provider of a remote computing service or electronic communication service to the public to disclose information not otherwise permitted or required to be disclosed under 18 U.S.C. 2701-2713 (commonly known as the "Stored Communications Act"). 6 U.S.C. 681e(e).

CIRCIA also provides that entities may voluntarily report cyber incidents or ransom payments to CISA that are not required to be reported under the CIRCIA regulations, and applies the same information treatment requirements on use (including

liability protections) and restrictions on use to such voluntarily submitted reports. 6 U.S.C. 681c(a), (c); 681e. CISA is not, however, proposing to address entirely voluntary reporting (e.g., how such reports may be submitted) in this rulemaking.

B. Current Cyber Incident Reporting Landscape

The cyber incident reporting landscape currently consists of dozens of Federal and state, local, tribal, or territorial (SLTT) cyber incident reporting requirements that may apply to entities operating within the United States, depending on where an entity or its customers are located and the type of business in which the entity is engaged. At the Federal level alone, more than three dozen different cyber incident reporting requirements currently are in effect, with a number of additional proposed regulatory reporting requirements in various stages of development. At the SLTT level, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, and all 50 states have laws that require reporting and/or public disclosure of at least some cyber incidents that result in data breaches.

Despite these myriad Federal and SLTT reporting requirements, prior to the enactment of CIRCIA, there was no Federal statute or regulation supporting a comprehensive and coordinated approach to understanding cyber incidents across critical infrastructure sectors. Nor was there a Federal department or agency charged with coordinating cross-sector sharing of information related to cyber incidents with Federal and non-Federal stakeholders. Indeed, during the lead up to the passage of CIRCIA, Congress stated "[t]oday no one U.S. Government agency has visibility into all cyber-attacks occurring against U.S. critical infrastructure on a daily basis. This bill would change that—enabling a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the U.S."[2] The enactment of

[2] U.S. Senate Committee on Homeland Security and Governmental Affairs (HSGAC), *Cyber Incident Reporting for Critical Infrastructure Act* at 1 (Dec. 17, 2021), available at

CIRCIA authorized CISA to fill these key gaps in the current cyber incident reporting landscape.

There are a number of different reasons why a government entity may establish cyber incident reporting requirements. A recent DHS report to Congress based on the work of the Cyber Incident Reporting Council (CIRC)[3] titled *Harmonization of Cyber Incident Reporting to the Federal Government* suggests that these reasons generally can be organized into two primary categories.[4] The first category consists of regulations primarily focused on national security, economic security, public health and safety, and/or the resiliency of National Critical Functions (NCFs). A majority of Federal reporting regimes appear to be solely or primarily animated by these concerns. The remaining Federal cyber incident reporting regimes, as well as virtually all SLTT cyber incident reporting regimes, are designed primarily to address privacy, consumer protection, or investor protection considerations. This second category includes all the reporting regimes often referred to as data breach notification laws.

Outside of state data breach notification laws, most existing cyber incident reporting requirements target specific communities with common characteristics. Some focus on entities within a specific industry or sector (e.g., commercial nuclear power reactors; financial services institutions) while others cover entities across sectors that possess certain shared characteristics (e.g., entities possessing threshold quantities of certain chemicals of interest that render those entities high-risk of being targeted by

---

https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf (hereinafter, "*HSGAC Fact Sheet*").

[3] CIRCIA established an intergovernmental Cyber Incident Reporting Council. Chaired by the Secretary of Homeland Security, the CIRC is responsible for coordinating, deconflicting, and harmonizing Federal incident reporting requirements, including those issued through regulations. 6 U.S.C. 681f.

[4] Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* at 5 (Sept. 19, 2023), available at https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government (hereinafter, "*the DHS Report*").

terrorists; entities located upon navigable bodies of water where they present the risk of a transportation security incident; entities that maintain personal health-related records).

Central aspects of cyber incident reporting regimes, such as what constitutes a reportable incident, the process for reporting an incident, which entity receives the report, what information must be reported, and how long an entity has to report the incident, can vary widely from regime to regime, with the purpose of the regime frequently impacting these variables. For instance, reporting regimes focused on national or economic security tend to have shorter deadlines for reporting than those regimes focused on privacy or consumer protections. Similarly, reporting regimes focused on national or economic security almost universally require reporting to a Federal department or agency, while regimes with a primary purpose of privacy or consumer protections often require reporting to the impacted individual and sometimes credit reporting agencies, instead of, or in addition to, reporting to the governing Federal or SLTT entity.

Given the number and variety of different cyber incident reporting regimes, and their continued evolution, CISA does not intend to describe each one of them as part of this section. Instead, CISA is providing the following brief summaries of some of the major regulatory programs that require reporting of cyber incidents and that are concerned at least in part with national security, economic security, public safety, and/or the resiliency of NCFs[5]:

- *Chemical Facility Anti-Terrorism Standards (CFATS).* CISA's CFATS program worked for the prior 16 years to identify and regulate high-risk chemical facilities to ensure security measures are in place to reduce the risk of certain chemicals of interest from being weaponized by terrorists. See 6 CFR part 27. Under CFATS Risk-Based Performance Standard 15, CFATS-covered facilities were expected to

[5] Individuals interested in learning more about existing Federal cyber incident reporting requirements are encouraged to review the Federal Cyber Incident Reporting Requirements Inventory contained in Appendix B of the *DHS Report*, *supra* note 4.

establish protocols governing the identification and reporting of significant cyber incidents to the appropriate facility personnel, local law enforcement, and/or CISA. On July 28, 2023, the statutory authority for the CFATS program expired, but CISA anticipates that CFATS will be reauthorized prior to the publication of the CIRCIA Final Rule.

- *Defense Federal Acquisition Regulation Supplement (DFARS).* Pursuant to 32 CFR 236.1-236.7 and 48 CFR 252.204-7012, Department of Defense (DOD) contractors must report to DOD all cyber incidents (1) involving covered defense information on their covered contractor information systems or (2) affecting the contractor's ability to provide operationally critical support. Contractors subject to these requirements, who are members of the Defense Industrial Base sector, must report cyber incidents to DOD at https://://dibnet.dod.mil.
- *Department of Energy (DOE) DOE-417 reporting requirements.* DOE's Office of Cybersecurity, Energy Security, and Emergency Response requires certain Energy Sector entities to report certain cybersecurity incidents to DOE pursuant to 15 U.S.C. 772(b). Entities subject to the reporting requirements include Balancing Authorities, Reliability Coordinators, some Generating Entities, and Electric Utilities, including those located in Puerto Rico, the Virgin Islands, Guam, or other U.S. possessions.
- *Federal Communications Commission's (FCC) Network Outage Reporting System (NORS) Requirements.* Under 47 CFR part 4, providers of telecommunications services and Voice over Internet Protocol (VoIP) providers are required to report to the FCC communications service outages, including those caused by cyber incidents, that meet certain minimum requirements for duration and magnitude. The goal of this regulation, which applies to wireline, wireless, VoIP, cable, satellite, Signaling System 7, submarine cable, covered 911 service,

and covered 988 service providers, is to provide rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of the Nation and help ensure the public's access to emergency services.

- *Federal Information Security Modernization Act of 2014.* FISMA requires Federal civilian departments and agencies to report cybersecurity incidents to CISA within one hour of discovery.[6] CISA uses information received in FISMA incident reports to, among other things, provide technical assistance to victims of cyber incidents, compile and analyze incident information to identify cyber threats and vulnerabilities, and share guidance with others on how to detect, handle, and prevent similar incidents.[7] Federal agencies are also required to report major incidents under FISMA and pursuant to OMB Guidance, including those that implicate personal information.[8]
- *Federal Risk and Authorization Management Program (FedRAMP).* FedRAMP requires any cloud service providers (CSPs) with a Federal agency-issued Authority to Operate (ATO) or a FedRAMP-issued provisional ATO to report suspected and confirmed information security incidents to the FedRAMP Program Management Office within the General Services Administration (GSA), CISA, and the affected agency.[9]
- *Financial Services Sector Regulations.* Most of the primary Financial Services Sector regulators have adopted cyber incident reporting requirements for their regulated communities. Among other things, these reporting requirements have been established to help promote early awareness of emerging threats to banking

[6] 44 U.S.C. 3554(b)(7)(C)(ii).
[7] 44 U.S.C. 3556(a).
[8] 44 U.S.C. 3554(b)(7)(C)(iii).
[9] See *FedRAMP*, GSA, https://www.gsa.gov/technology/government-it-initiatives/fedramp (last visited Nov. 27, 2023).

organizations and the broader financial system, and to help the regulating entities react to these threats before they can cause systemic impacts across the financial system. Included among these are cyber incident reporting requirements managed by the Office of the Comptroller of the Currency (OCC) (12 CFR part 53), the Federal Reserve Board (FRB) (12 CFR part 225), the Federal Deposit Insurance Corporation (FDIC) (12 CFR part 304), the Commodity Futures Trading Commission (CFTC) (see, e.g., 17 CFR 38.1051 (designated contract markets); 17 CFR 37.1401 (swap execution facilities); 17 CFR 39.18 (derivatives clearing organizations); 17 CFR 49.24 (swap data repositories); 17 CFR 23.603 (swap dealers)), the National Credit Union Administration (NCUA) (12 CFR part 748), the Securities and Exchange Commission (SEC) (see, e.g., 17 CFR parts 229, 232, 239, 240, 242, and 249), and the Federal Housing Finance Agency (FHFA) (Advisory Bulletin 2020-05).

- *Maritime Transportation Security Act (MTSA).* Under MTSA (33 CFR parts 104, 105, or 106) entities that own vessels or facilities, including outer continental shelf facilities, subject to MTSA must report cyber incidents to the U.S. Coast Guard's (USCG) National Response Center. These cyber incident reporting requirements are part of a larger suite of security requirements for vessels and facilities to identify, assess, and prevent transportation security incidents (TSIs) in the marine transportation system. USCG is also in the process of updating its maritime security regulations by adding cybersecurity requirements to existing Maritime Security regulations.[10]
- *North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard CIP-008-6: Cyber Security – Incident Reporting and*

[10] See Office of Management and Budget, *Office of Information and Regulatory Affairs Unified Agenda*, available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1625-AC77.

Response Planning. Certain electric grid entities, designated as "responsible entities," are required to report cyber incidents to both CISA and the Electricity Information Sharing and Analysis Center (ISAC), a component of NERC. See 18 CFR part 40 and CIP-008-6. The goal of these reporting requirements, which were developed pursuant to the authority granted NERC in Section 215 of the Federal Power Act (16 U.S.C. Ch 12, as amended through Pub. L. 115–325) to develop mandatory and enforceable reliability standards subject to Federal Energy Regulatory Commission (FERC) review and approval, is to mitigate the risk to the reliable operation of the Bulk Electric System (BES) as the result of a cybersecurity incident.

- *Nuclear Regulatory Commission (NRC) Cyber Security Event Notification Regulation.* Owners and operators of commercial nuclear power reactors are required to report cyber incidents impacting safety, security, or emergency preparedness functions to the NRC.[11]
- *The Food and Drug Administration (FDA) Medical Device Regulations*. Under section 519 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 360i), as implemented by the Medical Device Reporting Regulations (21 CFR part 803) and the Medical Device Reports of Corrections and Removals Regulations (21 CFR part 806), manufacturers and importers must report certain device-related adverse events and product problems, including those caused by cyber incidents, to the FDA. For example, medical device manufacturers are required to report to the FDA when they learn that any of their devices may have caused or contributed to a death or serious injury. Manufacturers must also report to the FDA when they become aware that their device has malfunctioned and would be likely to cause or contribute to a death or serious injury if the malfunction were to recur. Medical

[11] 10 CFR 73.77.

device manufacturers and importers also must report to FDA any correction or removal of a medical device initiated to reduce a risk to health posed by the device or to remedy a violation of the Federal Food, Drug, and Cosmetic Act, including those caused by cyber incidents, caused by the device that may present a risk to health. A report must be made even if the event was caused by user error.

- *Transportation Security Administration (TSA) Security Directives and Security Program Amendments*. TSA has issued several Security Directives and Security Program Amendments requiring various Transportation Systems Sector entities to report cybersecurity incidents to CISA.[12] These include, among other provisions, reporting requirements for certain passenger railroad carrier and rail transit systems, hazardous and natural gas pipeline owners and operators, freight railroad carriers, airport operators, aircraft operators, indirect air carriers, and Certified Cargo Screening Facilities. TSA is also in the process of codifying the requirements for surface transportation through a rulemaking (TSA's regulations provide for changes to aircraft operator security programs through an amendment process).[13]

C. Purpose of Regulation

While the legislative history and statutory text shed some light on the goals that Congress hoped to achieve through this regulation, Congress did not include an explicit statement of purpose in CIRCIA. CISA believes considering the specific intended purpose behind a cyber incident reporting regulation during the development of the regulations is important as the purpose likely impacts key aspects of the regulation, such as what entities are required to report, what types of incidents must be reported, how

[12] See, e.g., TSA Security Directive Pipeline-2021-01 series, *Enhancing Pipeline Cybersecurity*; TSA Security Directive 1580-21-01 series, *Enhancing Rail Cybersecurity*, available at https://www.tsa.gov/sd-and-ea.

[13] See Office of Management and Budget, *Office of Information and Regulatory Affairs Unified Agenda*, available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1652-AA74.

quickly incidents must be reported, what information must be included in incident reports, and to whom the reports must be provided.

Many stakeholders echoed this belief in remarks made during CIRCIA listening sessions or through comments provided in response to the CIRCIA RFI, which encouraged CISA to articulate the goals of the regulation to help inform the best regulatory proposal.[14] This section of the NPRM is intended to provide insight into what CISA interprets to be the purposes of the regulation that has informed the development of CISA's proposed regulation.

i. Purposes of the CIRCIA Regulation

CIRCIA's legislative history indicates that the primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety. For example, in December 2021, HSGAC issued a fact sheet on the proposed legislation acknowledging the "serious national security threat" posed by cyberattacks and stating that CIRCIA would help enable a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the United States.[15] Similarly, the U.S. House Committee on Homeland Security (CHS) issued a fact sheet on the proposed legislation stating that CIRCIA would provide CISA and its Federal partners the visibility needed to bolster cybersecurity, identify malicious cyber

---

[14] See 87 FR 55833 (Sept. 12, 2022); comments submitted by Information Technology Industry Council, CISA-2022-0010-0097 ("[I]t is vital that CISA articulate its tactical goals and/or plan for actualizing CIRCIA, as only upon understanding what CISA hopes to accomplish with these reports can industry stakeholders provide more specific commentary on key scoping and reporting threshold questions."); National Grain and Feed Association, CISA-2022-0010-0104 ("CISA should also identify the specific purpose of reporting an incident. For example, if the data will be used by the government for trend identification."); G. Rattray, CISA-2022-0010-0159 ("[CISA] will have to decide whether it is reporting that serves the purpose of characterizing threats or you're trying to understand risks and vulnerability. Both are probably viable analytically, but those would lead to different sort of reporting requirements.").

[15] *HSGAC Fact Sheet*, *supra* note 2, at 1.

campaigns in early stages, identify longer-term threat trends, and ensure actionable cyber threat intelligence is getting to the first responders and Federal officials who need it.[16]

The plain language that Congress used throughout CIRCIA reflects the purpose discussed in CIRCIA's legislative history. For example, CIRCIA requires CISA to review covered cyber incidents that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States" and to "identify and disseminate ways to prevent or mitigate similar incidents in the future." 6 U.S.C. 681(9); 6 U.S.C. 681a(a)(6). CIRCIA also requires CISA to "assess potential impact of cyber incidents on public health and safety," and to consider, when describing covered entities, both "the consequences that disruption to or compromise of [a covered entity] could cause to national security, economic security, or public health and safety" and "the extent to which damage, disruption, or unauthorized access to such an entity . . . will likely enable the disruption of the reliable operation of critical infrastructure." 6 U.S.C. 681a(a)(1); 6 U.S.C. 681b(c)(1)(A), 681b(c)(1)(C).

Both CIRCIA's legislative history and statutory text highlight a number of more discrete purposes within the broader goals of enhancing national and economic security, and public health and safety. Some examples of these purposes include trend and threat analysis (i.e., the performance of cybersecurity threat and incident trend analysis and tracking, to include the analysis and identification of adversary tactics, techniques, and procedures (TTPs));[17] vulnerability and mitigation assessment (i.e., the identification of

---

[16] CHS, *The Cyber Incident Reporting for Critical Infrastructure Act* at 1, 3 (Aug. 2021), available at https://democrats-homeland.house.gov/download/incident-reporting-bill-draft-fact-sheet (hereinafter, "*CHS Fact Sheet*").

[17] See, e.g., *id.* at 3; *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021 Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security*, 117th Cong. 64 (2021), available at https://www.congress.gov/event/117th-congress/house-event/114018/text (hereinafter, "*Stakeholder Perspectives Hearing*") (statement of Rep. Yvette Clarke) ("One of the goals in drafting this legislation was to provide CISA with enough information to analyze and understand threats . . . ."); 6 U.S.C. 681a(a)(1) (CISA must aggregate and analyze reports to

cyber vulnerabilities and the assessment of countermeasures that might be available to address them);[18] the provision of early warnings (i.e., the rapid sharing of information on cyber threats, vulnerabilities, and countermeasures through the issuance of cybersecurity alerts or other means);[19] incident response and mitigation (i.e., rapid identification of significant cybersecurity incidents and offering of assistance—e.g., personnel, services—in incident response, mitigation, or recovery);[20] supporting Federal efforts to disrupt threat actors;[21] and advancing cyber resiliency (i.e., developing and sharing strategies for improving overall cybersecurity resilience; facilitating use of cyber incident data to

---

identify TTPs adversaries use and to enhance situational awareness of cyber threats across critical infrastructure sectors).

[18] See, e.g., *Responding to and Learning from the Log4Shell Vulnerability Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. 2 (2022) (statement of Sen. Gary Peters, Chairman, S. Comm. on Homeland Security and Governmental Affairs), available at https://www.hsgac.senate.gov/hearings/responding-to-and-learning-from-the-log4shell-vulnerability/ (hereinafter, "*Log4Shell Vulnerability Hearing Peters Statement*") ("This legislation will help our lead cybersecurity agency better understand the scope of attacks, including from vulnerabilities like Log4j. . . ."); 6 U.S.C. 681a(a)(1) (CISA must aggregate and analyze reports to assess the effectiveness of security controls).

[19] See, e.g., *Log4Shell Vulnerability Hearing Peters Statement*, *supra* note 18, at 2 ("This legislation will help our lead cybersecurity agency . . . warn others of the threat, prepare for potential impacts. . . ."); Minority Staff of S. Comm. on Homeland Security and Governmental Affairs, 117th Cong., America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies vi (Comm. Print 2022), available at https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/ ("This legislation will enhance the Federal Government's ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through the sharing of timely and actionable threat information."); 6 U.S.C. 681a(a)(3)(B) (CISA must provide entities with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, cyber threat indicators and defensive measures); 6 U.S.C. 681a(a)(5)-(7) (CISA must identify and disseminate ways to prevent or mitigate cyber incidents, and must review reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to stakeholders).

[20] See, e.g., *HSGAC Fact Sheet*, *supra* note 2, at 1 ("This information will allow CISA to provide additional assistance to avoid cyber-attacks against our critical infrastructure, like the attacks on Colonial Pipeline and JBS Foods."); *Log4Shell Vulnerability Hearing Peters Statement*, *supra* note 18 ("This legislation will help our lead cybersecurity agency . . . help affected entities respond and recover.").

[21] See, e.g., Press Release, S. Comm. on Homeland Security and Governmental Affairs, *Portman, Peters Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyberattacks* (Sept. 28, 2021), available at https://www.hsgac.senate.gov/media/dems/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks/ ("As cyber and ransomware attacks continue to increase, the federal government must be able to quickly coordinate a response and hold these bad actors accountable."); Letter from Sen. Rob Portman, Ranking Member, S. Comm. on Homeland Security and Governmental Affairs, to Vanessa Countryman, Secretary, SEC, Re: RE: SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File No. S7-09-22, 3 (May 9, 2022), available at https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf ("When considering the legislation, Congress noted if the FBI is 'provided information from reports under the process outlined in the statute, [it] may, as appropriate, use information contained in the reports and derived from them' for a range of investigatory activities. This is consistent with the statute which states incident reports can be used for 'the purpose [of] preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident' reported under the law. This allows law enforcement agencies to disrupt and deter hostile cyber actors . . . ." (footnotes omitted)).

further cybersecurity research; engagement with software/equipment manufacturers on vulnerabilities and how to close them).[22]

ii. How the Regulatory Purpose of CIRCIA Influenced the Design of the Proposed CIRCIA Regulation

Based on CISA's understanding of the purposes of CIRCIA, CISA identified two fundamental principles that influenced the design of the proposed CIRCIA regulation in key areas. First, to achieve many of the desired goals of the proposed regulation—such as conducting analysis to identify adversary TTPs and providing early warnings to enhance situational awareness of cyber threats across critical infrastructure sectors—CISA needs to receive a sufficient quantity of Covered Cyber Incident Reports and Ransom Payment Reports from across the spectrum of critical infrastructure. As noted by the Cyberspace Solarium Commission, the government's cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its cyber risk identification and assessment efforts rely on comprehensive data and, prior to the passage of CIRCIA, the Federal government lacked a mandate to systematically collect cyber incident information reliably and at the scale necessary.[23] Sufficient data also is central to being able to differentiate campaigns from isolated incidents and support the development of more generalizable conclusions.[24]

---

[22] See, e.g., 6 U.S.C. 681a(a)(9) (CISA must proactively identify opportunities to leverage and utilize data on cyber incidents to enable and strengthen cybersecurity research carried out by academia and private sector organizations).

[23] Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report* at 103 (Mar. 2020), available at https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/ (hereinafter "*Cyberspace Solarium Commission Report*"); see also Sandra Schmitz-Berndt, "Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive," *Journal of Cybersecurity* at 2 (Apr. 5, 2023) ("[L]ow reporting levels result in a flawed picture of the threat landscape, which in turn may impact cybersecurity preparedness."), available at https://academic.oup.com/cybersecurity/article/9/1/tyad009/7160387.

[24] See, e.g., CISA, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* at 49 (Oct. 26, 2020) (reliance on limited data sources such as those based on convenience samples "means that no statistical representativeness can be claimed [which] limits the ability to support inference for generalizing results beyond the studied samples."), available at https://www.cisa.gov/resources-tools/resources/cost-cyber-incident-systematic-review-and-cross-validation.

If CISA designs the proposed regulations in a way that overly limits the quantity and variety of reports it receives from across critical infrastructure sectors, CISA will lack sufficient information to support reliable trend analysis, vulnerability identification, provision of early warnings, and other key purposes of the proposed regulation as indicated by CIRCIA. This fundamental principle was particularly important for CISA as it considered different options related to which entities should be required to report, what types of cyber incidents should be reported, and the scope and amount of technical detail necessary in CIRCIA Reports to enable CISA to conduct threat analysis, track campaigns, and provide early warnings as required by CIRCIA.

Many stakeholders provided comments in response to the RFI issued in September 2022 cautioning CISA that collecting too many reports could result in data overload and hinder CISA's ability to identify important trends and vulnerabilities. While CISA agrees that there could be some point at which the number of reports submitted begins to yield diminishing marginal returns, CISA believes that, due to advances in technology and strategies for managing large data sets, the potential challenges associated with receiving large volumes of reports can be mitigated through technological and procedural strategies. Additionally, as discussed in Section IV.E.ii in this document, CISA proposes to design the reporting form in a manner that is easy for a covered entity or third-party submitter to complete, encourages the submission of useful information, and provides information to CISA in a manner that facilitates analysis and review. As a result, CISA is less concerned about receiving too many reports and more concerned about not receiving enough reports to support the intended regulatory purposes of the CIRCIA regulations. As noted by Microsoft President Brad Smith during his testimony in front of the U.S. Senate Select Committee on Intelligence during a hearing on the "Hack of U.S. Networks by a Foreign Adversary," in the wake of the supply chain compromise of the SolarWinds Orion product, "one of the challenges in this space is the nature of all

threat intelligence, whether it's cyber-based or physically based, is that it's always about connecting dots. So the more dots you have, the more likely you are to see a pattern and reach a conclusion. . . . And then they're spread out across different parts of the public sector as well. So this notion of aggregating them is key."[25]

CISA is cognizant of the fact that reporting does not come without costs, however, so CISA is not seeking simply to capture the maximum number of reports possible under the statutory language (i.e., by scoping both the applicability of the rule and covered cyber incidents as broadly as legally permissible). CISA's goal is to identify and achieve the proper balance among the number of reports being submitted, the benefits resulting from their submission, and the costs to both the reporting entities and the government of the submission, analysis, and storage of those reports.

The second major principle CISA identified that influenced aspects of the proposed regulation was the importance of timeliness in both the receipt of reports and in CISA's ability to analyze and share information gleaned from those reports. To achieve the very important early visibility and warning aspects of this regulatory regime and increase the likelihood that entities across the critical infrastructure community will be able to address identified vulnerabilities and secure themselves against the latest adversary TTPs before falling victim to them, time is of the essence. CISA kept this second principle in mind as CISA considered options for when a covered entity's reporting obligations begin under the proposed regulation and the manner, form, and procedures for reporting.

Similar to the first principle, CISA recognizes that potential drawbacks to overprioritizing timely reporting exist, such as potentially impacting a covered entity's ability to conduct preliminary incident response and mitigation. CISA also recognizes

---

[25] Testimony of Brad Smith to the U.S. Senate Select Committee on Intelligence, "Hearing on Hack of U.S. Networks by a Foreign Adversary" (Feb. 23, 2021), available at https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

that a covered entity may not have all the information in the early aftermath of incident discovery, and that some preliminary determinations made at the outset of an incident response process may later be determined to be inaccurate when the entity is afforded time to conduct further investigation and analysis. Accordingly, CISA has sought to balance the critical need for timely reporting with the potential challenges associated with rapid reporting in the aftermath of a covered cyber incident. For example, CISA recognizes that covered entities may require some limited time to conduct preliminary analysis before establishing a reasonable belief that a covered cyber incident has occurred and thereby triggering the 72-hour timeframe for reporting. See Section IV.E.iv.1 in this document. Additionally, to the extent that information that is required to be reported under the regulation is evolving or unknown within the initial reporting deadline for a covered cyber incident, CISA is proposing to allow covered entities to submit new or updated information in a Supplemental Report as additional information becomes known about the covered cyber incident. See Section IV.E.iii.4 in this document.

D. Harmonization Efforts

Given the number of existing cyber incident reporting requirements at the Federal and SLTT levels, CISA recognizes that covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents. In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal. CISA is already engaged in several efforts in furtherance of harmonization of cyber incident reporting, including: (1) serving as a member of the CIRC and participating in the CIRC's efforts to coordinate, deconflict, and harmonize Federal cyber incident reporting requirements; (2) participating in the Cybersecurity Forum for Independent and

Executive Branch Regulators; (3) performing extensive outreach with Federal and non-Federal entities to gain a fulsome understanding of the existing cyber incident reporting regulatory landscape and gather perspectives on how to harmonize existing cyber incident reporting requirements; and (4) engaging with other Federal departments and agencies that implement cyber incident reporting requirements to determine whether covered entities could potentially take advantage of the proposed substantially similar reporting exception to CIRCIA reporting (discussed further in Section IV.D.i in this document).

CISA actively participated in the CIRC to help identify potential approaches to harmonizing Federal cyber incident reporting requirements and to support the identification of recommended practices that could be considered by CISA and other Federal departments and agencies as they develop or update their respective cyber incident reporting regimes. Specifically, CISA participated in various DHS-led working groups to identify potential recommended practices and areas of harmonization related to Federal cyber incident reporting requirements, many of which are reflected in the DHS Report.[26] CISA considered the DHS Report and its recommendations as it developed this proposed rule and attempted to leverage the model definition and reporting form recommended in the DHS Report to the extent practicable and consistent with the unique regulatory authority granted to CISA under CIRCIA and the purpose of the CIRCIA regulation (described in Sections III.A and C in this document).

CISA has also been an active participant in the Cybersecurity Forum for Independent and Executive Branch Regulators. The goal of this forum, which was initially launched in 2014, is to increase the overall effectiveness and consistency of Federal regulatory authorities related to cybersecurity by enhancing communication among regulatory agencies, sharing best practices, and exploring ways to align, leverage,

[26] *DHS Report*, *supra* note 4, at 5.

and deconflict approaches to cybersecurity regulation.[27] Current participants in the Forum include, among others, FCC, CISA, CFTC, Consumer Product Safety Commission, Department of Health and Human Services (HHS), DHS, Department of the Treasury, FERC, FHFA, FRB, Federal Trade Commission, FDA, NRC, OCC, SEC, TSA, USCG, and the Office of the National Cyber Director.

Additionally, CISA has performed, and as required by CIRCIA, plans on continuing to perform, outreach to both Federal partners and non-Federal stakeholders to learn about existing and proposed cyber incident reporting regulations and ways in which CISA may be able to design and implement the CIRCIA requirements to harmonize with those reporting requirements to the extent practicable. In addition to the RFI and listening sessions described in Section III.F in this document, CISA held a series of consultations with each Sector Risk Management Agency (SRMA), all Federal departments and agencies that currently oversee cyber incident reporting requirements, and various other Federal departments and agencies with equities in cyber incident and ransom payment reporting. During these engagements, CISA has sought to learn about existing and proposed Federal regimes that require the reporting of cyber incidents or ransom payments and discuss areas where CISA and its Federal counterparts might want to, and be able to, harmonize their respective reporting requirements. CISA leveraged the information gained via the RFI, listening sessions, and Federal consultations in the development of this NPRM, and intends to continue to engage Federal partners during the development and implementation of the final rule in an attempt to harmonize reporting requirements and reduce the burden on potential covered entities, where practicable.

Finally, CISA intends to work with other Federal departments and agencies to explore opportunities to reduce duplicative reporting of covered cyber incidents through a

---

[27] See Cybersecurity Forum for Independent and Executive Branch Regulators Charter (2014), available at https://www.nrc.gov/docs/ML1501/ML15014A296.pdf.

proposed substantially similar reporting exception to CIRCIA. Under this exception, which is authorized under 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report information to another Federal entity that is substantially similar to the information that must be reported under CIRCIA and is required to submit the report in a substantially similar timeframe to CIRCIA's reporting deadlines, may be excepted from reporting it again under CIRCIA. Per the statute, for covered entities to be able to leverage this specific exception, CISA and the respective Federal entity must enter into an interagency agreement, referred to as a CIRCIA Agreement, and establish an information sharing mechanism to share reports. To the extent practicable, CISA is committed to working in good faith with its Federal partners to have CIRCIA Agreements finalized before the effective date of the final rule. Additional details on the substantially similar reporting exception to CIRCIA are discussed in Section IV.D.i in this document.

CISA welcomes all comments on all aspects of harmonizing CIRCIA's regulatory reporting requirements with other cyber incident and ransom payment reporting requirements, including:

1. Potential approaches to harmonizing CIRCIA's regulatory reporting requirements with other existing Federal or SLTT laws, regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments.
2. How to reduce actual, likely, or potential duplication or conflict between other Federal or SLTT laws, regulations, directives, or policies and CIRCIA's reporting requirements.

E. Information Sharing Required by CIRCIA

Sharing information on cyber incidents, ransomware attacks, and the broader cyber threat landscape is central to CIRCIA. In fact, CIRCIA imposes several

requirements upon CISA and other Federal departments and agencies related to the sharing of information received through cyber incident and ransom payment reporting programs, including the CIRCIA proposed regulations. As Congress imposed these obligations solely on Federal departments and agencies, they are not included in the CIRCIA proposed rule; however, information sharing will be an integral part of the overall CIRCIA implementation, and CISA is committed to working with its Federal partners to share cyber threat information across the Federal government and, as appropriate, with non-Federal stakeholders.

As required by 6 U.S.C. 681a(a)(10) and (b), CISA will make information received via CIRCIA Reports or in response to an RFI or subpoena available to appropriate SRMAs and other appropriate Federal departments and agencies, as determined by the President or a designee of the President, within 24 hours of receipt. CIRCIA also includes a reciprocal requirement, where any Federal department or agency that receives a report of a cyber incident shall provide the report to CISA within 24 hours of receiving the report. See 6 U.S.C. 681g(a)(1). Upon receipt of a report from another Federal agency pursuant to this requirement, CISA must share the report with other Federal agencies as it would any other report submitted to CISA under CIRCIA. 6 U.S.C. 681a(a)(10), 681a(b), 681g(a)(1). In addition to any otherwise generally applicable laws (such as the Privacy Act of 1974[28] and the E-Government Act of 2002[29]), pursuant to 6 U.S.C. 681g(a)(3), CISA must protect the reports it receives from Federal partners under these provisions in accordance with any privacy, confidentiality, or information security requirements imposed upon the originating Federal department or agency. CIRCIA also requires CISA to "coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments." 6 U.S.C. 681a(a)(2).

---

[28] See 5 U.S.C. 552a.
[29] See 44 U.S.C. 3501 note, Pub. L. 107–347.

CIRCIA imposes requirements on CISA related to sharing cyber threat information with non-Federal stakeholders as well. For example, 6 U.S.C. 681a(a)(7) requires CISA to immediately review Covered Cyber Incident Reports or voluntary reports submitted to CISA pursuant to 6 U.S.C. 681c to the extent they involve ongoing cyber threats or security vulnerabilities for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders. Similarly, for a covered cyber incident or group of covered cyber incidents that satisfies the definition of a significant cyber incident, CISA must conduct a review of the details surrounding the incident(s) and identify and disseminate ways to prevent or mitigate similar incidents in the future. 6 U.S.C. 681a(a)(6). CISA must also "publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations" based on Covered Cyber Incident Reports. 6 U.S.C. 681a(a)(8). In addition to limiting sharing of information as may otherwise be required by laws that are generally applicable to information received by the Federal government, such as the Trade Secrets Act,[30] when sharing with critical infrastructure owners and operators and the general public any information received via CIRCIA Reports or responses to RFIs, CISA must anonymize information related to the victim who reported the incident. See 6 U.S.C. 681e(d).

F. Summary of Stakeholder Comments

While developing this NPRM, CISA sought feedback from an array of public and private sector stakeholders in an effort to identify the most effective potential approach to implementing CIRCIA's reporting requirements. CISA published an RFI in the *Federal Register*;[31] held in-person, public listening sessions around the country;[32] conducted

---

[30] 18 U.S.C. § 1905.

[31] The RFI, which was published in the *Federal Register* on September 12, 2022, solicited inputs on potential aspects of the proposed regulation prior to the publication of this NPRM. CISA did not limit the type of feedback commenters could submit in response to the RFI, but did specifically request comments on definitions for and interpretations of the terminology to be used in the proposed regulation; the form,

virtual, sector-specific listening sessions;[33] and consulted with SRMAs and other relevant Federal departments and agencies, all with the goal of receiving meaningful input from entities that will potentially be impacted by this regulation. CISA has considered this feedback when developing the proposals set forth in this NPRM. A summary of the most salient points received in response to the RFI and during the CIRCIA listening sessions follows. All comments received in response to the RFI, as well as transcripts from all the public and sector-specific listening sessions, are available in the electronic docket for this rulemaking.

i. General Comments

In general, several commenters told CISA that the regulations should be easy to comply with, such that individuals who are not cybersecurity professionals can complete the required reporting, and avoid overly burdensome requirements.[34] Commenters recommended that compliance with the regulation be incentive-based and supportive, rather than punitive,[35] and commenters also expressed concerns about the confidentiality of reported information.[36] Commenters also urged CISA to consider the landscape of existing cyber incident reporting requirements and expressed general concern about the

---

manner, content, and procedures for submission of reports required under CIRCIA; information regarding other incident reporting requirements including the requirement to report a description of the vulnerabilities exploited; and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulation. The comment period was open through November 14, 2022, and CISA received 131 individual comments in response to the RFI. 87 FR 55833.

[32] Between September 21, 2022, and November 16, 2022, CISA hosted ten listening sessions in Salt Lake City, Utah; Chicago, Illinois; Fort Worth, Texas; New York, New York; Philadelphia, Pennsylvania; Washington, D.C.; Oakland, California; Boston, Massachusetts; Seattle, Washington; and Kansas City, Missouri. 87 FR 55830; 87 FR 60409.

[33] Because CIRCIA defines covered entities with reference to critical infrastructure sectors, CISA held sector-specific listening sessions for each of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21, see https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, as well as a separate session for the Aviation Subsector. Transcripts from these sessions can be viewed in the docket for this rulemaking by going to www.regulations.gov and searching for CISA-2022-0010.

[34] See, e.g., Comments submitted by the Confidentiality Coalition, CISA-2022-0010-0030; Credit Union National Association, CISA-2022-0010-0050; SAP, CISA-2022-0010-0114; Federation of American Hospitals, CISA-2022-0010-0063; Epic, CISA-2022-0010-0090.

[35] See, e.g., Comments submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA-2022-0010-0022; SolarWinds, CISA-2022-0010-0027.

[36] See, e.g., Comments submitted by Google Cloud, CISA-2022-0010-0109; Tenable, CISA-2022-0010-0032; NCTA - The Internet & Television Association, CISA-2022-0010-0102.

potential negative impacts of unharmonized, complex, and duplicative reporting regimes.[37]

ii. Comments on the Definition of Covered Entity

Several commenters provided suggestions on how to define the term covered entity under this regulation. While some commenters thought the definition of covered entity was straightforward and already understood,[38] others pointed to different criteria or frameworks CISA could use to scope the definition more effectively. These included, among others, a size-based threshold,[39] a risk-based approach, [40] or a focus on the degree to which an entity supported a NCF.[41] Commenters also suggested leveraging existing lists, standards, or definitions, such as the list of critical infrastructure "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," as determined pursuant to Section 9(a) of Executive Order 13636;[42] the NERC CIP standard;[43] the National Institute of Standards and Technology's (NIST's) definition;[44] or definitions used by other countries.[45] Others suggested considering the unique qualities of particular industries and sectors and either creating sector-based definitions or excluding certain sectors and industries from the definition altogether.[46]

---

[37] See, e.g., Comments submitted by CTIA, CISA-2022-0010-0070; R Street Institute, CISA-2022-0010-0125; IBM, CISA-2022-0010-0069; Cybersecurity Coalition, CISA-2022-0010-0105.
[38] See, e.g., Comment submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA-2022-0010-0022.
[39] See, e.g., Comments submitted by the Computing Technology Industry Association, CISA-2022-0010-0122; BlackBerry Corporation, CISA-2022-0010-0036; Cyber Threat Alliance, CISA-2022-0010-0019; SolarWinds, CISA-2022-0010-0027.
[40] See, e.g., Comments submitted by the Information Technology Industry Council, CISA-2022-0010-0097; U.S. Chamber of Commerce, CISA-2022-0010-0075; American Property Casualty Insurance Association, CISA-2022-0010-0064.
[41] See, e.g., Comment submitted by Mitchell Berger, CISA-2022-0010-0004.
[42] See, e.g., Comments submitted by the UnityPoint Health, CISA-2022-0010-0107; National Retail Federation, CISA-2022-0010-0092; National Rural Electric Cooperative Association, CISA-2022-0010-0025.
[43] See, e.g., Comment submitted by the Powder River Energy Corporation, CISA-2022-0010-0099.
[44] See, e.g., Comment submitted by the Credit Union National Association, CISA-2022-0010-0050.
[45] See, e.g., Comment submitted by SAP, CISA-2022-0010-0114.
[46] See, e.g., Comments submitted by the Rural Wireless Association, Inc., CISA-2022-0010-0093 (recommending excluding small telecommunications carriers); TechNet, CISA-2022-0010-0072

iii. Comments on the Definition of Covered Cyber Incident and Substantial Cyber Incident

Many commenters provided thoughts on how to define covered cyber incident and substantial cyber incident, including some who offered their own definitions for CISA to consider.[47] Multiple commenters indicated a desire for a high threshold for reporting to minimize burdens on regulated entities, avoid duplicative reporting, and prevent CISA from being inundated with reports,[48] although at least one commenter noted that a narrow definition could leave CISA with an incomplete understanding of the threat landscape.[49] In recommending high thresholds, commenters suggested that CISA could bound the definition of covered cyber incident in a variety of ways, such as by limiting reporting to "confirmed incidents";[50] incidents that cause "actual harm";[51] only incidents that impact business operations;[52] only incidents that impact an entity's critical infrastructure functions;[53] incidents that directly impact U.S. companies, citizens, economies or national security;[54] and/or those resulting only from malicious intent.[55]

(discussing the "innovation economy"); American Property Casualty Insurance Association, CISA-2022-0010-0064 (recommending exclusion of insurance agencies); NAFCU, CISA-2022-0010-0076 (recommending exclusion of the credit union industry).

[47] See, e.g., Comments submitted by the Cybersecurity Coalition, CISA-2022-0010-0105; Microsoft Corporation, CISA-2022-0010-0058.

[48] See, e.g., Comments submitted by The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; American Council of Life Insurers, CISA-2022-0010-0095; UnityPoint Health, CISA-2022-0010-0107; Cloudflare, Inc., CISA-2022-0010-0074; American Property Casualty Insurance Association, CISA-2022-0010-0064; Jim Wollbrinck, CISA-2022-0010-0151.

[49] See, e.g., Comment submitted by NERC, CISA-2022-0010-0049.

[50] See, e.g., Comments submitted by Mandiant, CISA-2022-0010-0120; Edison Electric Institute, CISA-2022-0010-0079; Connected Health Initiative, CISA-2022-0010-0130; ACT | The App Association, CISA-2022-0010-0129.

[51] See, e.g., Comments submitted by the Internet Infrastructure Coalition, CISA-2022-0010-0055; Independent Community Bankers of America, CISA-2022-0010-0080; Institute of International Finance, CISA-2022-0010-0060.

[52] See, e.g., Comments submitted by IBM, CISA-2022-0010-0069; Edison Electric Institute, CISA-2022-0010-0079; Fidelity National Information Services, CISA-2022-0010-0033; National Technology Security Coalition, CISA-2022-0010-0061.

[53] See, e.g., Comments submitted by IBM, CISA-2022-0010-0069; CrowdStrike, CISA-2022-0010-0128; Microsoft Corporation, CISA-2022-0010-0058; Professional Services Council, CISA-2022-0010-0044; Alliance for Automotive Innovation (Auto Innovators), CISA-2022-0010-0082; Telecommunications Industry Association, CISA-2022-0010-0132.

[54] See, e.g., Comments submitted by Airlines for America, CISA-2022-0010-0066; U.S. Chamber of Commerce, CISA-2022-0010-0075; Express Association of America, CISA-2022-0010-0038; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA-2022-0010-0057.

Several commenters also advocated for considering definitions that already exist, such as the definition created by NIST that is used in FISMA,[56] or definitions that are already used among the 16 critical infrastructure sectors.[57]

Comments received on the potential definition of substantial cyber incident echoed those received on the potential definition of covered cyber incident, though a few commenters noted that the term substantial cyber incident does not have existing legal definitions as does covered cyber incident.[58] One commenter noted that CISA should clarify whether "substantial cyber incidents" are separate from "covered cyber incidents,"[59] and another commenter recommended covered cyber incidents and substantial cyber incidents should be synonymous terms.[60]

iv. Comments on Other Definitions

CISA received a small number of comments on other definitions. A few commenters provided feedback on the meaning of the terms ransom payment and ransomware attack, with several noting that the definitions of ransom payment and

---

[55] See, e.g., Comments submitted by Cloudflare, Inc., CISA-2022-0010-0074; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; Internet Infrastructure Coalition, CISA-2022-0010-0055.
[56] See, e.g., Comments submitted by the National Technology Security Coalition, CISA-2022-0010-0061; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; Mandiant, CISA-2022-0010-0120; Glenn Herdrich, CISA-2022-0010-0158.
[57] See, e.g., Comments submitted by NCTA - The Internet & Television Association, CISA-2022-0010-0102 (generally advocating for a sector-based approach to the definition); Financial Services Sector Coordinating Council, CISA-2022-0010-0094; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; The Clearing House, CISA-2022-0010-0086 (advocating for alignment with the FDIC's Computer-Security Incident Notification Rule); HIMSS Electronic Health Record Association, CISA-2022-0010-0040 (advocating for alignment with the Health Insurance Portability and Accountability Act requirements); Nuclear Energy Institute, CISA-2022-0010-0029; Rich Mogavero, CISA-2022-0010-0139 (advocating alignment with the definition used by the NRC); Electric Power Supply Association, CISA-2022-0010-0045; Edison Electric Institute, CISA-2022-0010-0079 (advocating for alignment with the reporting standards used by the NERC); NTCA - The Rural Broadband Association, CISA-2022-0010-0100 (recommending consideration of the FCC's reporting requirements in developing the definition).
[58] See, e.g., Comments submitted by the Association of Metropolitan Water Agencies, CISA-2022-0010-0088; U.S. Chamber of Commerce, CISA-2022-0010-0075; Fidelity National Information Services, CISA-2022-0010-0033.
[59] See, e.g., Comment submitted by the Professional Services Council, CISA-2022-0010-0044.
[60] See, e.g., Comment submitted by Gideon Rasmussen, CISA-2022-0010-0011.

ransomware attack were understood as defined in CIRCIA and recommending no changes to these terms in the regulation.[61]

A few commenters offered input on the meaning of supply chain compromise, with those who did often acknowledging the statutory definition of the term (see 6 U.S.C. 650(28)),[62] and recommending that CISA align this term as closely as possible with similar, existing terms, such as "supply chain attack" used by NIST or the definition of "supply chain compromise" used by MITRE.[63] Several commenters emphasized a need for clarity regarding when a customer or end user would be expected to report on an incident caused somewhere above them in the supply chain, noting that in many cases the impacted covered entity may have limited visibility into what happened along the supply chain to cause the incident.[64]

v. Comments on Criteria for Determining whether the Domain Name System Exception Applies

The few comments received relating to whether an entity is a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS reflected different views. One commenter recommended that CISA clarify that domain name registries and registrars are "governed by a multistakeholder organization."[65] Another commenter opined that it would not be appropriate to exempt domain name registrars. The same commenter recommended that CISA identify exempted

---

[61] See, e.g., Comments submitted by (ISC)2, CISA-2022-0010-0112; Exelon Corp., CISA-2022-0010-0043; SAP, CISA-2022-0010-0114.
[62] See, e.g., Comment submitted by the Cybersecurity Coalition, CISA-2022-0010-0105.
[63] See *id.*; see, e.g., Comment submitted by the Information Technology Industry Council, CISA-2022-0010-0097.
[64] See, e.g., Comments submitted by the American Water Works Association, CISA-2022-0010-0127; Edison Electric Institute, CISA-2022-0010-0079; NCTA - The Internet & Television Association, CISA-2022-0010-0102; Exelon Corp., CISA-2022-0010-0043.
[65] Comment submitted by the Internet Infrastructure Coalition, CISA-2022-0010-0055.

organizations by name in the final rule, listing Internet Corporation for Assigned Names and Numbers (ICANN) and the Regional Internet Registries for consideration.[66]

vi. Comments on Manner and Form of Reporting, Content of Reports, and Reporting Procedures

Numerous commenters provided recommendations on the manner and form of reporting, with many of those concurring with the use of a web-based form for reporting or other means of electronic reporting.[67] Some explicitly recommended that CISA make a mobile application or otherwise make the form available via a mobile device as well.[68] Several commenters recommended alternative or additional methods of reporting to include phone or email.[69] Multiple commenters emphasized that reporting should not require the download or purchase of new technology.[70] A number of commenters recommended that the same portal be used for Supplemental Reports as for the original reports.[71]

Overall, commenters emphasized the need for a user-friendly reporting form. While several commenters recommended that the reporting form be standardized for all covered entities,[72] at least one commenter noted that a uniform reporting format could

---

[66] See Comment submitted by the Energy Transfer LP, CISA-2022-0010-0037. Regional Internet Registries include ARIN, LACNIC, RIPE NCC, AFRINIC, and APNIC (see Regional Internet Registries | The Number Resource Organization (nro.net)).

[67] See, e.g., Comments submitted by American Council of Life Insurers, CISA-2022-0010-0095; HIMSS Electronic Health Record Association, CISA-2022-0010-0040; Epic, CISA-2022-0010-0090; Cyber Threat Alliance, CISA-2022-0010-0019; League of Southeastern Credit Unions, CISA-2022-0010-0121; Marty Reynolds, CISA-2022-0010-0135; Patrick Thornton, CISA-2022-0010-0144.

[68] See, e.g., Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; OCHIN, CISA-2022-0010-0039; Cybersecurity Coalition, CISA-2022-0010-0105.

[69] See, e.g., Comments submitted by CHIME, CISA-2022-0010-0035; Business Roundtable, CISA-2022-0010-0115; CTIA, CISA-2022-0010-0070; The Clearing House, CISA-2022-0010-0086.

[70] See, e.g., Comments submitted by the Operational Technology Cybersecurity Coalition, CISA-2022-0010-0108; NTCA - The Rural Broadband Association, CISA-2022-0010-0100; Tenable, CISA-2022-0010-0032.

[71] See, e.g., Comments submitted by the Cybersecurity Coalition, CISA-2022-0010-0105; Information Technology Industry Council, CISA-2022-0010-0097; Credit Union National Association, CISA-2022-0010-0050.

[72] See, e.g., Comments submitted by the Alliance for Automotive Innovation, CISA-2022-0010-0082; Lucid Motors, CISA-2022-0010-0078; USTelecom - The Broadband Association, CISA-2022-0010-0067; Palo Alto Networks, CISA-2022-0010-0089.

unintentionally limit the type of information CISA receives.[73] Many commenters recommended that any reporting form include drop-down menus, check-boxes, or other fields that could be pre-populated for ease of submission.[74] Other commenters recommended that the incident reporting form generate questions pertinent to the type of incident being reported, including an indication of which fields were required for each type of report.[75] Several commenters also recommended that CISA assign reference numbers to each report, which would allow entities to more easily locate and return to a specific CIRCIA Incident Reporting Form at a later point.[76] Commenters also recommended existing reporting or submission procedures that CISA could emulate. Some commenters recommended CISA rely on a standardized approach, noting examples such as the National Information Exchange Model[77] or Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII).[78] Other commenters recommended CISA align its reporting approach to that of other Federal departments and agencies such as USCG,[79] TSA,[80] or DOD.[81]

When proposing suggestions for the content of CIRCIA reports, many commenters recommended that CISA require minimal detail at the 72-hour reporting deadline to not divert resources from response efforts,[82] emphasizing that covered entities

---

[73] See, e.g., Comment submitted by the Association of American Railroads, CISA-2022-0010-0117.
[74] See, e.g., Comments submitted by the Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; CTIA, CISA-2022-0010-0070; Anonymous, CISA-2022-0010-0012; National Grain and Feed Association, CISA-2022-0010-0104; Mitchell Berger, CISA-2022-0010-0004; League of Southeastern Credit Unions, CISA-2022-0010-0121; NERC, CISA-2022-0010-0049.
[75] See, e.g., Comments submitted by the Municipal Information Systems Association of California, CISA-2022-0010-0118; City of Roseville, CISA-2022-0010-0111; City of Cerritos, CISA-2022-0010-0084; Cyber Threat Alliance, CISA-2022-0010-0019; (ISC)2, CISA-2022-0010-0112.
[76] See, e.g., Comments submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA-2022-0010-0022; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041.
[77] See, e.g., Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; SolarWinds, CISA-2022-0010-0027; MITRE, CISA-2022-0010-0073.
[78] See, e.g., Comments submitted by ACT | The App Association, CISA-2022-0010-0129; Connected Health Initiative, CISA-2022-0010-0130; Cyber Threat Alliance, CISA-2022-0010-0019; HIMSS, CISA-2022-0010-0119.
[79] See, e.g., Comment submitted by the American Association of Port Authorities, CISA-2022-0010-0126.
[80] See, e.g., Comment submitted by Energy Transfer LP, CISA-2022-0010-0037.
[81] See, e.g., Comment submitted by Trustwave Government Solutions, CISA-2022-0010-0096.

should be required to report only what is absolutely needed.[83] Several commenters recommended a core set of questions be asked for every covered entity,[84] while others suggested the question set could be sector-specific.[85] Many commenters offered their thoughts on specific pieces of data that CISA should consider collecting via the CIRCIA reporting form, many, if not most, of which covered entities are statutorily required to include in either Covered Cyber Incident Reports or Ransom Payment Reports.[86] Some non-statutorily required fields that commenters suggested included: identification of critical infrastructure sector, anyone else that the entity informed, severity of the event, and victim IP addresses.[87]

vii. Comments on the Deadlines for Submission of CIRCIA Reports

---

[82] See, e.g., Comments submitted by BSA | The Software Alliance, CISA-2022-0010-0106; SAP, CISA-2022-0010-0114; Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA-2022-0010-0022; American Chemistry Council, CISA-2022-0010-0098; U.S. Chamber of Commerce, CISA-2022-0010-0075.

[83] See, e.g., Comments submitted by CHIME, CISA-2022-0010-0035; Google Cloud, CISA-2022-0010-0109; The Clearing House, CISA-2022-0010-0086; Information Technology-ISAC, CISA-2022-0010-0048.

[84] See, e.g., Comments submitted by the Institute of International Finance, CISA-2022-0010-0060; National Association of Chemical Distributors, CISA-2022-0010-0056; UnityPoint Health, CISA-2022-0010-0107; Powder River Energy Corporation, CISA-2022-0010-0099.

[85] See, e.g., Comments submitted by HIMSS, CISA-2022-0010-0109; CHIME, CISA-2022-0010-0035; CTIA, CISA-2022-0010-0070.

[86] See, e.g., Comments submitted by the U.S. Chamber of Commerce, CISA-2022-0010-0075 (recommending that CISA focus on the ten elements listed in CISA's *Sharing Cyber Event Information: Observe, Act, Report* document, namely: incident date and time, incident location, type of observed activity; detailed narrative of the event; number of people or systems affected; company/organization name; point of contact details; severity of event; critical infrastructure sector; and anyone else the entity informed.); Cyber Threat Alliance, CISA-2022-0010-0019 (recommending that the form include three "layers," containing fields applicable to all incidents (victim information, incident type, incident information, and threat actor information), incident specific fields (with different fields each for business email compromise, ransomware or other extortion, data theft, financial theft such as banking trojans, service theft, denial of service, disruptive or destructive attack, data manipulation or integrity loss, branding/reputation attack, or unauthorized access), and an optional layer for the provision of technical information (such as victim IP addresses, threat actor groups, MITRE ATT&CK mapping, exploited vulnerabilities)); Municipal Information Systems Association of California, CISA-2022-0010-0118 (recommending that the form include impacted "[a]gency," date of incident, date incident discovered, indicators of compromise, type of data compromised (if applicable), other compliance agencies mandated to receive this report, a description of the incident, steps taken so far, and logs); City of Roseville, CISA-2022-0010-0111 (same); City of Cerritos, CISA-2022-0010-0084 (same); Palo Alto Networks, CISA-2022-0010-0089 (recommending that the template reporting form include the attack vector or vectors that led to the compromise; tactics or techniques used by threat actor; indicators of compromise; information on the affected systems, devices, or networks; information relevant to the identification of the threat actor or actors involved; a point of contact from the affected entity; and impact, earliest known time, and duration of compromise); Mitchell Berger, CISA-2022-0010-0004 (suggesting that CISA include a list of the 16 critical infrastructure sectors, 55 national critical functions, or similar items with boxes to check).

[87] See *id.*

Although the 72-hour reporting deadline for the reporting of a covered cyber incident is codified in the text of CIRCIA itself, several commenters offered thoughts on how to interpret this requirement. Many commenters suggested that CISA provide flexibility in initiating the 72-hour clock due to the challenges entities face in identifying a "reasonable belief" and responding to covered cyber incidents.[88] Similarly, commenters urged that CISA adopt certain flexibilities in considering the deadline to have been met, such as allowing entities to omit fields on a form when information is not yet known[89] or provide extensions to the 72-hour deadline when covered entities are experiencing an external event, such as a natural disaster or pandemic.[90] A few commenters noted that it may not be objective or clear in the moment when a covered entity has a "reasonable belief," and recommended that CISA consider determining whether a reasonable belief exists on a case-by-case basis.[91] Many commenters stated that "reasonable belief" should be defined as a confirmed or validated cyber incident from the perspective of the covered entity and that the 72-hour clock should therefore begin at that time.[92]

Similarly, several commenters recommended specific interpretations for the point at which the 24-hour clock deadline for submission of a Ransom Payment Report should begin. For instance, commenters recommended that the 24-hour clock should begin after the ransom payment is sent,[93] when "funds or items of value are transmitted to the

---

[88] See, e.g., Comments submitted by Cybersecurity Coalition, CISA-2022-0010-0105; TechNet, CISA-2022-0010-0072; Federation of American Hospitals, CISA-2022-0010-0063; National Association of Manufacturers, CISA-2022-0010-0087; American Council of Life Insurers, CISA-2022-0010-0095.
[89] See, e.g., Comment submitted by Google Cloud, CISA-2022-0010-0109.
[90] See, e.g., Comment submitted by HIMSS, CISA-2022-0010-0119.
[91] See, e.g., Comments submitted by NCTA - The Internet & Television Association, CISA-2022-0010-0102; SAP, CISA-2022-0010-0114; CTIA, CISA-2022-0010-0070.
[92] See, e.g., Comments submitted by National Electrical Manufacturers Association, CISA-2022-0010-0026; League of Southeastern Credit Unions, CISA-2022-0010-0121; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA-2022-0010-0057; Trustwave Government Solutions, CISA-2022-0010-0096; Microsoft Corporation, CISA-2022-0010-0058.
[93] See, e.g., Comments submitted by Exelon Corp., CISA-2022-0010-0043; Cybersecurity Coalition, CISA-2022-0010-0105; Credit Union National Association, CISA-2022-0010-0050; National Association of Chemical Distributors, CISA-2022-0010-0056.

extorting party,"[94] or as soon as "any part" of the ransom payment is no longer in possession of the impacted entity or any of its affiliated third parties.[95]

In regards to Supplemental Reports, while some commenters recommended flexibility, including no deadline for timing of submission of Supplemental Reports,[96] others recommended CISA provide a separate deadline for the submission of Supplemental Reports.[97] Recommended deadlines varied from as short as 12 hours after discovering substantially new or different information[98] to as long as one year after the incident.[99] On the question of what should constitute substantially new or different information that would necessitate filing a Supplemental Report, many commenters recommended that covered entities be permitted to decide when new findings necessitate a Supplemental Report.[100] Other commenters suggested the types of material changes that could be considered substantial new or different information, such as changes to the types of data stolen or altered; changes to the number or type of systems impacted; or updates to information regarding the TTPs used in the incident.[101]

viii. Comments on Third-Party Submitters

Of the commenters who offered feedback on the third-party submissions of CIRCIA Reports, most seemed to support the framework already contemplated by statute. For instance, one commenter stated that organizations should be able to identify a third party to submit on their behalf,[102] and more than one stated that the reporting

---

[94] See, e.g., Comment submitted by the Cybersecurity Coalition, CISA-2022-0010-0105.
[95] See, e.g., Comment submitted by Sophos, Inc, CISA-2022-0010-0047.
[96] See, e.g., Comments submitted by the Airlines for America, CISA-2022-0010-0066; SAP, CISA-2022-0010-0114.
[97] See, e.g., Comments submitted by SolarWinds, CISA-2022-0010-0027; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; Telecommunications Industry Association, CISA-2022-0010-0132.
[98] See, e.g., Comment submitted by Sophos, Inc, CISA-2022-0010-0047.
[99] See, e.g., Comment submitted by the Workgroup for Electronic Data Interchange, CISA-2022-0010-0041
[100] See, e.g., Comments submitted by USTelecom - The Broadband Association, CISA-2022-0010-0067; Institute of International Finance, CISA-2022-0010-0060; Exelon Corp., CISA-2022-0010-0043.
[101] See, e.g., Comments submitted by the Institute of International Finance, CISA-2022-0010-0060; League of Southeastern Credit Unions, CISA-2022-0010-0121; Payments Leadership Council, CISA-2022-0010-0031.
[102] See, e.g., Comment submitted by American Chemistry Council, CISA-2022-0010-0098.

mechanisms, guidelines, and procedures should be the same for the third-party submitter as for the covered entity.[103] Many commenters recommend that CISA clarify that the duty to comply with the regulation falls on the covered entity,[104] and that third-party submitters have no obligation to report on the covered entity's behalf.[105]

Some commenters recommended additional safeguards for covered entities using third-party reporters. A few commenters recommended that CISA clarify the types of third parties authorized to submit reports on behalf of the covered entity.[106] One commenter recommended that CISA consider entities like ISACs to be suitable third-party reporters.[107] Multiple commenters also recommended that CISA allow third-party submitters to register with CISA as a known third-party submitter.[108]

ix. Comments on Data and Records Preservation Requirements

Very few commenters offered recommendations related to data and records preservation requirements. Several of those that did recommended CISA not impose additional data and records preservation requirements on covered entities via the CIRCIA regulation, and instead defer to covered entities' existing legal obligations or specific requests from law enforcement.[109] Only one commenter offered suggestions on the type of information that covered entities should preserve,[110] while a small number of

---

[103] See, e.g., Comments submitted by American Chemistry Council, CISA-2022-0010-0098; CrowdStrike, CISA-2022-0010-0128.
[104] See, e.g., Comments submitted by BlackBerry; CISA-2022-0010-0036; American Property Casualty Insurance Association, CISA-2022-0010-0064; Computing Technology Industry Association, CISA-2022-0010-0122.
[105] See, e.g., Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; Airlines for America, CISA-2022-0010-0066; Operational Technology Cybersecurity Coalition, CISA-2022-0010-0108; Information Technology-ISAC, CISA-2022-0010-0048; BlackBerry, CISA-2022-0010-0036.
[106] See, e.g., Comments submitted by Exelon Corp., CISA-2022-0010-0043; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA-2022-0010-0057.
[107] See, e.g., Comment submitted by the Association of Metropolitan Water Agencies, CISA-2022-0010-0088.
[108] See, e.g., Comments submitted by BSA | The Software Alliance, CISA-2022-0010-0106; SAP, CISA-2022-0010-0114; Information Technology Industry Council, CISA-2022-0010-0097.
[109] See, e.g., Comments submitted by Mandiant, CISA-2022-0010-0120; Accenture, CISA-2022-0010-0077; USTelecom - The Broadband Association, CISA-2022-0010-0067.
[110] See, e.g., Comment submitted by Sophos, Inc, CISA-2022-0010-0047 (recommending that information preserved should include at least all logs containing data related to the incident, such as network logs, system logs, and access logs; all correspondence with attackers, including any notes taken during any

commenters recommended lengths of time for how long CISA should require information to be preserved.[111]

x. Comments on Other Existing Cyber Incident Reporting Requirements and the Substantially Similar Reporting Exception

Many commenters offered feedback on the breadth of existing Federal, SLTT, and international cyber incident reporting requirements, and the potential for overlap, conflict, or alignment between CIRCIA and those requirements. CISA will not summarize the specific reporting requirements that commenters mentioned, because CISA provides a high-level summary of these existing reporting requirements in Section III.B in this document.

To avoid duplicative and burdensome reporting, several commenters recommended that CISA align its reporting requirements with existing Federal and SLTT requirements.[112] Commenters frequently recommended that CISA consult with other Federal departments and agencies with pre-existing regulatory authority in the commenters' particular sectors to avoid duplicative requirements in the CIRCIA regulation. Numerous commenters recommended that, alongside harmonization efforts, CISA should establish a single, national point of contact or process for mandatory cyber incident reporting,[113] suggesting that DHS or CISA serve as the primary or sole entity for receiving and disseminating cyber incident report information.[114] Many commenters,

---

unrecorded interactions; all identified TTPs and indicators of compromise; all data related to any ransomware payment; and contact information of individuals and entities that provided tactical support in the incident response and investigation process).

[111] See, e.g., Comments submitted by Sophos, Inc., CISA-2022-0010-0047; SAP, CISA-2022-0010-0114; National Association of Chemical Distributors, CISA-2022-0010-0056.

[112] See, e.g., Comments submitted by National Association of Secretaries of State, CISA-2022-0010-0054; OCHIN, CISA-2022-0010-0039; HIMSS Electronic Health Record Association, CISA-2022-0010-0040; Alliance for Automotive Innovation, CISA-2022-0010-0082; Lucid Motors, CISA-2022-0010-0078; Center for Democracy & Technology, CISA-2022-0010-0068.

[113] See, e.g., Comments submitted by Indiana Municipal Power Agency, CISA-2022-0010-0018; HIMSS, CISA-2022-0010-0119; Exelon Corp., CISA-2022-0010-0043; MITRE, CISA-2022-0010-0073; Options Security Corporation, CISA-2022-0010-0160; Airport Council International North America, CISA-2022-0010-0135; Cameron Braatz, CISA-2022-0010-0154.

noting the language in CIRCIA to this effect, encouraged CISA to implement the reporting exemption for covered entities that submit cyber incident reports with substantially similar information to other Federal departments and agencies, within a substantially similar timeframe.[115] A few commenters offered criteria for determining whether a report submitted to another Federal entity constitutes "substantially similar reported information."[116] Commenters also offered suggestions on which existing reporting obligations should be considered to include substantially similar information. These suggestions included the Cyber Incident Notification Requirements for Federally Insured Credit Unions (FICUs), located at 12 CFR 748.1;[117] the DFARS incident reporting requirement, located at 48 CFR 252.204-7012;[118] Cyber Security Event Notifications for Commercial Nuclear Power Reactors, located at 10 CFR 73.77; TSA Security Directive Pipeline-2021-01 series, Enhancing Pipeline Cybersecurity;[119] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule, located at 45 CFR 164.400-414, and corresponding Health Information Technology for Economic and Clinical Health (HITECH) Act Health Breach Notification

---

[114] See, e.g., Comments submitted by The Associations, CISA-2022-0010-0057: AFPM, AGA, API, APGA, INGAA, LEPA; Google Cloud, CISA-2022-0010-; Express Association of America, CISA-2022-0010-0038; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; Internet Infrastructure Coalition, CISA-2022-0010-0055; American Council of Life Insurers, CISA-2022-0010-0095; Business Roundtable, CISA-2022-0010-0115.

[115] See, e.g., Comments submitted by the American Public Power Association and the Large Public Power Council, CISA-2022-0010-0028; National Rural Electric Cooperative Association, CISA-2022-0010-0025; California Special Districts Association, CISA-2022-0010-0042; Professional Services Council, CISA-2022-0010-0044; American Association of Port Authorities, CISA-2022-0010-0126; Virginia Port Authority, CISA-2022-0010-0052; CHIME, CISA-2022-0010-0035; AHIP, CISA-2022-0010-0091.

[116] See, e.g., Comments submitted by Payments Leadership Council, CISA-2022-0010-0031 (recommending CISA consider a report to include substantially similar information if "the material essence of the incident is reflected in the information contained within the report to the other federal entity"); BSA | The Software Alliance, CISA-2022-0010-0106 (recommending that there be a "rebuttable presumption that a report provided by a covered entity to another federal entity is substantially similar").

[117] See, e.g., Comment submitted by NAFCU, CISA-2022-0010-0076.

[118] See, e.g., Comments submitted by U.S. Chamber of Commerce, CISA-2022-0010-0075; National Defense ISAC, CISA-2022-0010-0144.

[119] See, e.g., Comments submitted by Energy Transfer LP, CISA-2022-0010-0037

Rule, located at 16 CFR part 318, which applies to entities not subject to the HIPAA Breach Notification Rule.[120]

xi. Comments on Noncompliance and Enforcement

A small number of commenters offered recommendations related to noncompliance and enforcement of the CIRCIA regulations. These commenters encouraged CISA to keep in mind that covered entities are victims of an incident[121] and recommended that CISA focus on collaboration, not enforcement.[122] Similarly, a number of commenters recommended that CISA not penalize entities for reporting in good faith under the rule.[123] Such possible penalties that commenters recommended CISA avoid included pursuing enforcement under CIRCIA or allowing CIRCIA Reports to be the basis for enforcement actions by other Federal departments and agencies under separate regulations.[124] One commenter suggested that non-profit, self-incorporated fire and Emergency Management Service departments be excluded from enforcement in the same manner as SLTT Government Entities.[125]

xii. Comments on Treatment and Restrictions on Use of CIRCIA Reports

Numerous commenters provided recommendations on the treatment and restrictions on use of CIRCIA Reports and information therein. One consistent theme throughout the comments on this topic was the notion that CISA should take steps to ensure the confidentiality of the information, including the identity of the victims of

---

[120] See Comment submitted by Nuclear Energy Institute, CISA-2022-0010-0029; see also comment submitted by Blue Cross Blue Shield Association, CISA-2022-0010-0103.
[121] See, e.g., Comments submitted by the National Technology Security Coalition, CISA-2022-0010-0061; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046.
[122] See, e.g., Comments submitted by Airlines for America, CISA-2022-0010-0066; Connected Health Initiative, CISA-2022-0010-0130; ACT – The App Association CISA-2022-0010-0129.
[123] See, e.g., Comments submitted by the Association of American Railroads, CISA-2022-0010-0117; SolarWinds, CISA-2022-0010-0027; NTCA – The Rural Broadband Association, CISA-2022-0010-0100.
[124] *Id.*
[125] See, e.g., Comment submitted by the International Association of Fire Chiefs, CISA-2022-0010-0081.

reported cyber incidents, included in CIRCIA Reports.[126] Some of the procedural strategies recommended by commenters to achieve this include having CISA anonymize and aggregate cyber incident report information prior to sharing it with others,[127] exempting CIRCIA Reports and/or the information contained therein from release under FOIA and similar state laws,[128] and considering treating CIRCIA Reports as Protected Critical Infrastructure Information, "confidential," or "secret."[129] Numerous commenters also stressed the need for CISA to protect information submitted in CIRCIA Reports through strong data protection standards, data security practices, and data privacy safeguards.[130]

Commenters also suggested several different limitations on the use of the information contained in CIRCIA Reports. A number of commenters recommended CISA include adequate liability protections in the proposed regulation.[131] Other commenters recommended CISA clarify that reporting does not result in the waiver of attorney-client privilege, trade secret protections, or other privileges or protections.[132] A few commenters recommended that information contained in CIRCIA Reports be protected from discovery in civil or criminal actions.[133] One commenter recommended that the various protections afforded to CIRCIA Reports still apply even in the event that

---

[126] See, e.g., Comments submitted by IBM, CISA-2022-0010-0069; Gideon Rasmussen, CISA-2022-0010-0011; Institute of International Finance, CISA-2022-0010-0060; Powder River Energy Corporation, CISA-2022-0010-0099.
[127] See, e.g., Comments submitted by Fidelity National Information Services, CISA-2022-0010-0033; UnityPoint Health, CISA-2022-0010-0107; Institute of International Finance, CISA-2022-0010-0060.
[128] See, e.g., Comments submitted by Edison Electric Institute, CISA-2022-0010-0079; HIMSS, CISA-2022-0010-0119; National Grain and Feed Association, CISA-2022-0010-0104; NAFCU, CISA-2022-0010-0076.
[129] See, e.g., Comments submitted by NCTA, CISA-2022-0010-0102; SAP, CISA-2022-0010-0114.
[130] See, e.g., Comments submitted by the Financial Services Sector Coordinating Council, CISA-2022-0010-0094; The Clearing House, CISA-2022-0010-0086; Payments Leadership Council, CISA-2022-0010-0031.
[131] See, e.g., Comments submitted by American Chemistry Council, CISA-2022-0010-0098; SolarWinds, CISA-2022-0010-0027; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046.
[132] See, e.g., Comments submitted by CrowdStrike, CISA-2022-0010-0128; U.S. Chamber of Commerce, CISA-2022-0010-0075; Connected Health Initiative, CISA-2022-0010-0130.
[133] See, e.g., Comments submitted by Connected Health Initiative, CISA-2022-0010-0130; ACT | The App Association, CISA-2022-0010-0129.

a CIRCIA Report is compromised (i.e., accessed by an unauthorized individual or made public in an unauthorized manner).[134]

IV. Discussion of Proposed Rule

A. Definitions

Section 226.1 of the proposed rule contains proposed definitions for certain terms used within the rule. These proposed definitions are intended to help clarify the meaning of various terms used throughout the proposed rule and promote consistency in application of the regulatory requirements.

For a number of the terms, CISA proposes using, either verbatim or with minor adjustments, definitions provided in the Definitions sections of CIRCIA, as amended (6 U.S.C. 681). For several other terms where CIRCIA does not include a CIRCIA-specific definition, CISA proposes using, either verbatim or with minor adjustments, definitions provided in the Definitions sections at Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) or at the beginning of Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650), each as amended, since definitions in those sections also apply to CIRCIA. Proposed definitions that are derived from these legal authorities include: *cloud service provider*; *cyber incident*; *Cybersecurity and Infrastructure Security Agency or CISA*; *cybersecurity threat*; *Director*; *information system*; *managed service provider*; *ransom payment*; *ransomware attack; supply chain compromise;* and *virtual currency*.

Additionally, CISA is proposing definitions for a variety of terms that will have a specific meaning within the proposed regulation. These include *CIRCIA; CIRCIA Agreement*; *CIRCIA Report*; *covered cyber incident*; *Covered Cyber Incident Report*; *covered entity*; *Joint Covered Cyber Incident and Ransom Payment Report; personal information*; *Ransom Payment Report*; *State, Local, Tribal, or Territorial Government*

---

[134] See Comment submitted by submitted by Health-ISAC and the Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, CISA-2022-0010-0123.

entity or SLTT Government entity; *substantial cyber incident*; and *Supplemental Report*. The basis for each of these proposed definitions is discussed in their respective subsection below.

i. Covered Entity

Covered entity is a key term in the proposed regulation as, among other things, it is the operative term used to describe the regulated parties responsible for complying with the covered cyber incident and ransom payment reporting and data and records preservation requirements in the proposed CIRCIA regulation. While the statute includes a definition for the term covered entity, the statute explicitly requires CISA to further clarify the meaning of that term through description in the CIRCIA rulemaking. Specifically, the statute defines covered entity to mean "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title." 6 U.S.C. 681(4). CIRCIA also requires CISA to include a "clear description of the types of entities that constitute covered entities" in the final rule based on various specified factors. 6 U.S.C. 681b(c)(1).

CISA proposes to provide the criteria for covered entities in an Applicability section at § 226.2 of the regulation with a cross-reference to the Applicability section in the Definitions section under the term covered entity. See Section IV.B below and § 226.2 for a detailed discussion of the proposed covered entity criteria and the "clear description of the types of entities that constitute covered entities," required by 6 U.S.C. 681b(c)(1).

ii. Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident

1. Cyber Incident

CISA is proposing to include in the regulation a definition of the term cyber incident. The definition of cyber incident is important as it will help bound the types of incidents that trigger reporting requirements for covered entities under the proposed regulation.

CIRCIA states that the term cyber incident "(A) has the meaning given the term 'incident' in section 2209; and (B) does not include an occurrence that imminently, but not actually, jeopardizes—(i) information on information systems; or (ii) information systems." See 6 U.S.C. 681(5). Section 2209's definition of "incident" has since been moved to Section 2200 and defines the term "incident" as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system." See 6 U.S.C. 650(12).[135]

CISA is proposing to define cyber incident to mean an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system. The definition would use the 6 U.S.C. 650 definition verbatim other than striking the "imminently jeopardizes" clause in that definition, as required by 6 U.S.C. 681(5)(B).

2. Covered Cyber Incident

---

[135] The definition of "incident" was moved from Section 2209 of the Homeland Security Act (6 U.S.C. 659) to Section 2200 of the Homeland Security Act (6 U.S.C 650(12)) as part of the consolidation of definitions in Section 7143 (CISA Technical Corrections and Improvements) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (hereinafter, "CISA Technical Corrections"). Pub. L. 117-263, Div. G, Title LXXI, § 7143, Dec. 23, 2022. Section (f)(2) of the CISA Technical Corrections includes a rule of construction that provides that "[a]ny reference to a term defined in the Homeland Security Act of 2002 (6 U.S.C. 101 *et seq*.) on the day before the date of enactment of this Act that is defined in section 2200 of that Act pursuant to the amendments made under this Act shall be deemed to be a reference to that term as defined in section 2200 of the Homeland Security Act of 2002, as added by this Act." Pursuant to this rule of construction, the cross-reference in CIRCIA's definition of "cyber incident" to the definition of "incident" in Section 2209 of the Homeland Security Act (6 U.S.C. 659) is deemed a reference to the definition of "incident" in Section 2200 of the Homeland Security Act (6 U.S.C. 650).

CIRCIA requires CISA to include within the proposed rule a definition for the term covered cyber incident. See 6 U.S.C. 681(3). Because CIRCIA requires covered entities to report only those cyber incidents that qualify as covered cyber incidents to CISA, this definition is essential for triggering the reporting requirement. CISA is proposing to define the term covered cyber incident to mean a substantial cyber incident experienced by a covered entity. CISA also proposes definitions for both substantial cyber incident and covered entity within this NPRM.

Within CIRCIA, Congress defined a covered cyber incident as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title." See 6 U.S.C. 681(3). CISA believes that defining a covered cyber incident to include all substantial cyber incidents experienced by a covered entity rather than some subset thereof is both consistent with the statutory definition of covered cyber incident and is the least complicated approach to defining covered cyber incidents.

Under this approach, a covered entity simply needs to determine if a cyber incident is a substantial cyber incident for it to be reported, rather than having to perform an additional analysis to determine if a substantial cyber incident meets some narrower criteria for a covered cyber incident. As the term substantial cyber incident is not used in CIRCIA other than to help define a covered cyber incident, CISA does not see any benefit to having one set of requirements for what constitutes a substantial cyber incident and a separate set of requirements for which substantial cyber incidents experienced by a covered entity qualify as covered cyber incidents.

3. Substantial Cyber Incident

CISA is proposing to include within the rule a definition for the term substantial cyber incident. Given CISA's proposal to define a covered cyber incident as a substantial cyber incident experienced by a covered entity, the term substantial cyber incident is

essential to the CIRCIA regulation as it identifies the types of incidents that, when experienced by a covered entity, must be reported to CISA.

While CIRCIA does not define the term substantial cyber incident, it provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A). Consistent with these minimum requirements, CISA proposes the term substantial cyber incident to mean a cyber incident that leads to any of the following: (a) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (b) a serious impact on the safety and resiliency of a covered entity's operational systems and processes; (c) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or (d) unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise. CISA is further proposing that a substantial cyber incident resulting in one of the listed impacts include any cyber incident regardless of cause, including, but not limited to, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability. Finally, CISA is proposing the term substantial cyber incident does not include (a) any lawfully authorized activity of a United States Government entity or SLTT Government entity, including activities undertaken pursuant to a warrant or other judicial process; (b) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific

request by the owner or operator of the information system; or (c) the threat of disruption as extortion, as described in 6 U.S.C. 650(22).[136]

In developing this proposed definition, CISA examined how other Federal departments and agencies that regulate cyber incident reporting define similar terminology for their reporting regimes, reviewed the Model Definition for a Reportable Cyber Incident proposed by the Secretary of Homeland Security in the CIRC-informed DHS Report to Congress (the "CIRC Model Definition"), and considered the many comments received on this topic from stakeholders both at CIRCIA listening sessions and in written comments submitted in response to the CIRCIA RFI. CISA considered those various perspectives and approaches both within the constraints explicitly imposed by CIRCIA and in light of the purposes for which CISA believes CIRCIA was created as described in Section III.C in this document.

The proposed definition contains the following elements: (1) a set of four threshold impacts which, if one or more occur as the result of a cyber incident, would qualify that cyber incident as a substantial cyber incident; (2) an explicit acknowledgment that substantial cyber incidents can be caused through compromises of third-party service providers or supply chains, as well as various techniques and methods; and (3) three separate types of incidents that, even if they were to meet the other criteria contained within the substantial cyber incident definition, would be excluded from treatment as a substantial cyber incident. Each of these elements is addressed in turn below.

a. Minimum Requirements for a Cyber Incident to be a Substantial Cyber Incident

[136] The definition of ransomware attack contained in Section 2240(14)(A) was originally codified in 6 U.S.C. 681(14) but was moved from 6 U.S.C. 681(14) to 6 U.S.C 650(22) as part of the consolidation of definitions in the CISA Technical Corrections, *supra* note 135. The CISA Technical Corrections, however, did not update this cross-reference in CIRCIA. Nevertheless, pursuant to the rule of construction in Section (f)(2) of the CISA Technical Corrections, the cross reference in 6 U.S.C. 681b(c)(2)(C)(ii) to part of the definition of ransomware attack in 6 U.S.C. 681(14) is deemed a reference to the definition of ransomware attack now in 6 U.S.C. 650 (Section 2200 of the Homeland Security Act).

While Congress did not define the term substantial cyber incident in CIRCIA, Congress did include minimum requirements for the types of substantial cyber incidents that constitute covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A).[137] Because CISA is proposing that a covered cyber incident mean any substantial cyber incident experienced by a covered entity (see Section IV.A.ii.2 in this document), CISA interprets the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A) as the minimum requirements an incident must meet to be considered a substantial cyber incident (as opposed to a subset of substantial cyber incidents that constitute covered cyber incidents). Thus, while CISA has discretion to raise the threshold required for something to be a substantial cyber incident, resulting in a reduction of the number of incidents that would qualify as substantial, CISA may not lower the threshold below the requirements enumerated in 6 U.S.C. 681b(c)(2)(A).

CISA believes that the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A) create a sufficiently high threshold to prevent overreporting by making it clear that routine or minor cyber incidents do not need to be reported. Accordingly, CISA is proposing to use those requirements as the basis for the first part of the definition of substantial cyber incident, with minor modifications for clarity and for greater consistency with the CIRC Model Definition of a reportable cyber incident. Ultimately, CISA is proposing four types of impacts that, if experienced by a covered entity as a result of a cyber incident, would result in the incident being classified as a substantial

[137] 6 U.S.C. 681b(c)(2)(A) states that the types of substantial cyber incidents that constitute covered cyber incidents must, "at a minimum, require the occurrence of (i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes; (ii) a disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or (iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise."

cyber incident and therefore reportable under the CIRCIA regulation. Each of these impact types is described in its own prong of the substantial cyber incident definition.

i. Impact 1: Substantial Loss of Confidentiality, Integrity, or Availability

Under the first proposed threshold impact, a cyber incident would be considered a substantial cyber incident if it resulted in a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network. See § 226.1 of the proposed regulation. This impact reflects the substantive criteria contained in the first part of 6 U.S.C. 681b(c)(2)(A)(i), which states "a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network." Although this prong does not explicitly mention operational technology (OT)), CISA is using the term "information system," (which, per the proposed definition, as described in Section IV.A.iv.7 in this document, includes OT) in this threshold and proposes to interpret this aspect of the regulation to also specifically cover cyber incidents that lead to substantial loss of confidentiality, integrity, or availability of a covered entity's OT.

The concepts of confidentiality, integrity, and availability (CIA), often referred to as the "CIA triad," represent the three pillars of information security.[138] "Confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[139] "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity."[140] "Availability" refers to "ensuring timely and reliable access to and use of information."[141]

---

[138] See, e.g., NIST, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25 Vol. A at 1 (Dec. 2020), available at https://csrc.nist.gov/pubs/sp/1800/25/final.
[139] *Id.*
[140] *Id.*
[141] *Id.*

The loss of CIA of an information system, including OT, or network can occur in many ways. For example, if an unauthorized individual steals credentials or uses a brute force attack to gain access to a system, they have caused a loss of the confidentiality of a system. If that unauthorized individual uses that access to modify or destroy any information on the system, they have caused a loss of the integrity of the system and potentially a loss of the availability of the information contained therein. A denial-of-service attack that renders a system or network inaccessible is another example of an incident that leads to a loss of the availability of the system or network. These are just some of the many types of incidents that can lead to a loss of CIA and would be reportable if the impacts are "substantial."

Whether a loss of CIA constitutes a "substantial" loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss. One example of a cyber incident that typically would meet the "substantial" threshold for this impact type is a distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time. Similarly, a ransomware attack or other attack that encrypts one of a covered entity's core business or information systems substantially impacting the confidentiality, availability, or integrity of the entity's data or services likely also would meet the threshold of a substantial cyber incident under this first impact type and would need to be reported under the CIRCIA regulation. Persistent access to information systems by an unauthorized third party would typically be considered a substantial loss of confidentiality. By contrast, even time-limited access to certain high-value information systems, such as access to privileged credentials or to a domain controller, could also be considered a substantial loss of confidentiality. A large-scale data breach or otherwise meaningful exfiltration of data typically would also be considered a substantial cyber incident as it would reflect a substantial loss of the confidentiality of an information system. A theft of data that may

or may not itself meet the "substantial" impact threshold by nature of the data theft alone (based on the type or volume of data stolen) could become a substantial cyber incident if the theft is followed by a data leak or a credible threat to leak data. Conversely, CISA would not expect a denial-of-service attack or other incident that results in a covered entity's public-facing website being unavailable for a few minutes to typically rise to the level of a substantial cyber incident under this impact.[142]

ii. Impact 2: Serious Impact on Safety and Resiliency of Operational Systems and Processes

The second impact type of the proposed substantial cyber incident definition would require a covered entity to report a cyber incident that results in a serious impact on the safety and resiliency of a covered entity's operational systems and processes. This impact reflects the threshold enumerated in the second part of 6 U.S.C. 681b(c)(2)(A)(i), which states "a cyber incident that leads to . . . a serious impact on the safety and resiliency of operational systems and processes." Safety is a commonly understood term, which NIST defines as "[f]reedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."[143] NIST defines resilience as "[t]he ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption," and operational resilience as "[t]he ability of systems to resist, absorb, and recover from, or adapt to an

---

[142] The examples provided in this paragraph and elsewhere in this section of what typically might or might not be considered a substantial cyber incident are simply a few sample scenarios meant to provide context around this discussion. The examples are not meant as an exhaustive or definitive list of what is and is not a substantial cyber incident. Whether something is or is not a substantial cyber incident is fact-dependent and must be assessed on a case-by-case basis. For example, while, as noted, an incident resulting in a brief unavailability of a public-facing website would typically not qualify as a substantial loss of availability, such an incident may be significant for a covered entity whose public-facing website is a core part of its service offering (such as a webmail provider).

[143] NIST, *Developing Cyber-Resilient Systems*, NIST Special Publication 800-160 Vol. 2 Rev. 1, at 67 (Dec. 2021), available at https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final.

adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions."[144]

Similar to the interpretation of the word "substantial" in the first impact type, whether an impact on the safety and resiliency of an operational system or process is "serious" will likely depend on a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact. For example, a cyber incident that noticeably increases the potential for a release of a hazardous material used in chemical manufacturing or water purification likely would meet this definition. Similarly, a cyber incident that compromised or disrupted a BES cyber system that performs one or more reliability tasks would also likely meet this prong of the substantial cyber incident definition. Further, a cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls, would meet this definition. While CISA anticipates that the types of incidents that will actually lead to a serious impact to the safety and resilience of operational systems and processes may frequently involve OT, CISA does not interpret "operational systems and processes" to be a reference to OT. Congress used the specific phrase "operational technology" elsewhere in CIRCIA—including in the immediate next provision—and therefore certainly could have used it in this provision if that was the intent. Compare 6 U.S.C. 681b(c)(2)(A)(i) with 6 U.S.C. 681b(c)(2)(A)(ii)(II)). Accordingly, CISA interprets this prong broadly as not being limited to only incidents impacting OT, and covered entities should report incidents that are covered cyber incidents under this prong of the definition even if the impacts that meet the threshold are not to OT.

iii. Impact 3: Disruption of Ability to Engage in Business or Industrial Operations

[144] *Id.* at 65-66.

The third impact of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services. This prong reflects criteria enumerated by Congress in both 6 U.S.C. 681b(c)(2)(A)(ii) and (iii), which provides that one type of incident that could qualify as a substantial cyber incident that constitutes a covered cyber incident is a cyber incident that causes a disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a CSP, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

In drafting this prong, CISA has added two clauses to the statutory criteria relating to an entity's ability to engage in business operations or deliver goods or services. CISA proposes adding these clauses to this prong of the substantial cyber incident definition to clarify CISA's understanding of the statutory language. CISA understands that a disruption of business operations includes a disruption to an entity's ability to engage in business operations and the ability to deliver goods or services. CISA considers this language to be a clarification of the statutory language, and not an expansion.

NIST defines a disruption as "[a]n unplanned event that causes a . . . system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction)."[145] As opposed to the statutory source for the first two prongs of this definition, the portion of CIRCIA from

[145] NIST, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Rev. 1, Appendix G, (May 2010), available at https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final.

which this prong is drawn does not contain a qualifier such as "substantial" or "serious." Nevertheless, because this prong is part of the threshold for a "substantial" cyber incident, CISA believes it is appropriate to read into the prong some level of significance. Like the previous prongs, whether a disruption rises to the level of reportability may depend on a variety of factors and circumstances, such as the scope of the disruption and what was disrupted. A relatively minor disruption to a critical system or network could rise to a high level of substantiality, while a significant disruption to a non-critical system or network might not. Generally speaking, incidents that result in minimal or insignificant disruptions are unlikely to rise to the level of a substantial cyber incident reportable under this prong; however, the specific circumstances of the disruption should be taken into consideration.

While 6 U.S.C. 681b(c)(2)(A)(ii) provides that this category includes disruptions of business or industrial operations "due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability," CISA is not proposing to include this language in this third prong, as CISA reads this language as being illustrative of the types of incidents that might lead to a disruption of business or industrial operations, rather than a limitation on the types of incidents that can be reportable under this prong. To that end, examples of cyber incidents that would meet this prong include the exploitation of a zero-day vulnerability resulting in the extended downtime of a covered entity's information system or network, a ransomware attack that locks a covered entity out of its industrial control system, or a distributed denial-of-service attack that prevents customers from accessing their accounts with a covered entity for an extended period of time. Another example would be where a critical access hospital is unable to operate due to a ransomware attack on a third-party medical records software company on whom the critical access hospital relies; the critical access hospital, and perhaps the medical records software company as well if it also is a covered entity, would need to report the incident.

Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic, typically would not be considered substantial under this prong.

iv. Impact 4: Unauthorized Access Facilitated Through or Caused by a: (1) Compromise of a CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or (2) Supply Chain Compromise

The fourth prong of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a CSP, managed service provider, other third-party data hosting provider, or by a supply chain compromise. This prong reflects criteria enumerated in 6 U.S.C. 681b(c)(2)(A)(iii).

NIST defines unauthorized access as occurring when an individual "gains logical or physical access without permission to a network, system, application, data, or other resource."[146] Unauthorized access causes actual jeopardy to information systems and the information therein by compromising the first pillar of the CIA triad—confidentiality—and by providing an adversary with a launching off point for additional penetration of a system or network. Much like the third prong, the source language in CIRCIA does not contain any qualifier such as "substantial" or "serious." However, unlike that prong, CISA understands the absence of a qualifier here to be a reflection of the seriousness of unauthorized access through a third party (such as a managed service provider or CSP) or a supply chain compromise. Such cyber incidents uniquely have the ability to cause significant or substantial nation-level impacts, even if the impacts at many of the

[146] NIST, *Guide to Industrial Control Systems Security*, NIST Special Publication 800-82 Rev. 3, at 168 (Sept. 2023), available at https://csrc.nist.gov/pubs/sp/800/82/r3/final.

individual covered entities are relatively minor. The legislative intent makes clear that supply chain compromises such as the "SUNBURST" malware that compromised legitimate updates of customers using the SolarWinds Orion product, and third-party incidents like the compromise of the managed service provider Kaseya, were major drivers of the passage of CIRCIA.[147] CISA therefore understands that this prong reflects a recognition that CISA needs visibility into the breadth of a third-party incident or supply chain compromise to adequately meet its obligations under CIRCIA.

Examples of cyber incidents that CISA typically would consider meeting this prong include a detected, unauthorized intrusion into an information system or the exfiltration of information as a result of a supply chain compromise (see Section IV.A.iv.13 for further discussion on the meaning of supply chain compromise). Similarly, unauthorized access that was achieved through exploitation of a vulnerability in the cloud services provided to a covered entity by a CSP or by leveraging access to a covered entity's system through a managed service provider would meet this prong. Conversely, because the statute requires the unauthorized access to have been facilitated through or caused by a compromise of a third-party service provider or supply chain compromise, unauthorized access that results from a vulnerability within proprietary code developed by the covered entity or a gap in the covered entity's access control procedures that allows an unauthorized employee administrative access to the system would not

---

[147] See, e.g., *CHS Fact Sheet*, *supra* note 16, (referencing the SolarWinds supply chain compromise); Comm. on Homeland Security and Governmental Affairs, Staff Report: America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies, 25-27 (Mar. 2022) (discussing the Kaseya ransomware attacks), available at https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/; Business Meeting, Homeland Security and Governmental Affairs Committee, Opening Remarks by Ranking Member Rob Portman (Oct. 6, 2021), (citing SolarWinds as an example of an event that shows why greater transparency of these types of events through cyber incident reporting to CISA is needed), available at https://www.hsgac.senate.gov/hearings/10-06-2021-business-meeting/; *Stakeholder Perspectives Hearing*, *supra* note 17, at 55 (Statement of Rep. James Langevin) ("The SolarWinds breach has brought new attention to the issue of incident reporting, and for good reason."); 168 Cong. Rec. S1149 (daily ed. Mar. 14, 2022) (statement of Sen. Mark Warner) ("The SolarWinds breach demonstrated how broad the ripple effects of these attacks can be, affecting hundreds or even thousands of entities connected to the initial target.").

constitute a substantial cyber incident under this prong (though could still qualify as a substantial cyber incident under one of the first three prongs if it resulted in the requisite impact levels).

b. Guidance for Assessing Whether an Impact Threshold is Met

When evaluating whether a cyber incident meets one of the four proposed impact thresholds that would qualify it as a substantial cyber incident, a covered entity should keep in mind several principles. First, an incident needs to meet only one of the four prongs, not all four of the prongs, for it to be a substantial cyber incident. CISA believes Congress's use of the word "or" in 6 U.S.C. 681b(c)(2)(A) was intentional and was meant to confer the fact that for an incident to be a substantial cyber incident that meets the threshold of a covered cyber incident it only had to meet one of the enumerated criteria, not all the enumerated criteria. CISA's proposed definition for substantial cyber incident follows this example, using "or" intentionally to indicate that if an incident meets any of the enumerated criteria within the definition it is a substantial cyber incident. This approach is also consistent with the CIRC Model Definition, with which, for the reasons discussed below, CISA attempted to align to the extent practicable.

Second, for an incident to qualify as a substantial cyber incident, CISA interprets CIRCIA to require the incident to actually result in one or more of the impacts described above. A number of other cyber incident reporting regulations do not require actual impacts for an incident to have to be reported; rather, some require reporting if an incident results in imminent or potential harm, or identification of a vulnerability. While good policy rationales exist for both approaches in various contexts, CISA believes the phrase "require the occurrence of" in 6 U.S.C. 681b(c)(2)(A) limits reportable incidents under CIRCIA to those that have actually resulted in at least one of the impacts described in that section of CIRCIA. Likewise, CIRCIA's definition of cyber incident (of which substantial cyber incidents are a subset) specifically omits occurrences imminently, but

not actually, jeopardizing information systems or information on information systems. 6 U.S.C. 681(5). Consequently, if a cyber incident jeopardizes an entity or puts the entity at imminent risk of threshold impacts but does not actually result in any of the impacts included in the proposed definition, the cyber incident does not meet the definition of a substantial cyber incident. Similarly, if malicious cyber activity is thwarted by a firewall or other defensive or mitigative measure before causing the requisite level of impact, it would not meet the proposed definition of a substantial cyber incident and would not have to be reported. Consequently, blocked phishing attempts, failed attempts to gain access to systems, credentials reported missing but that have not been used to access the system and have since been rendered inactive, and routine scanning that presents no evidence of penetration are examples of events or incidents that typically would not be considered substantial cyber incidents. To both convey this intention and to more closely align with the language used in the CIRC Model Definition, CISA is proposing "a cyber incident that leads to" as the introductory language before the enumerated threshold prongs. CISA believes the phrase "leads to" satisfactorily conveys that a covered entity must have experienced one of the enumerated impacts for an incident to be considered a substantial cyber incident.

Third, the type of TTP used by an adversary to perpetrate the cyber incident and cause the requisite level of impact is typically irrelevant to the determination of whether an incident is a substantial cyber incident.[148] CISA believes that the specific attack vector or TTP used to perpetrate the incident (e.g., malware, denial-of-service, spoofing, phishing) should not be relevant to determining if an incident is a substantial cyber incident if one of the impact threshold prongs are met. One of the primary purposes of the

[148] The primary exception is the fourth prong, which is limited to instances where unauthorized access was facilitated through or caused by a compromise of a CSP, managed service provider, or another third-party data hosting provider, or by a supply chain compromise. However, even within this vector-specific prong, the specific TTPs used by the threat actor to compromise a third-party provider or the supply chain is not relevant to whether the incident is reportable.

CIRCIA regulation is to allow CISA the ability to identify TTPs being used by adversaries to cause cyber incidents. Limiting reporting to a specific list of TTPs that CISA currently is aware of would inhibit CISA's ability to fully understand the dynamic cyberthreat landscape as it evolves over time or be able to warn infrastructure owners and operators of novel or reemerging TTPs. (See further discussion in Section IV.A.ii.3.f of this document describing why CISA is proposing not to use the sophistication or novelty of the tactics used to narrow the definition of substantial cyber incidents.) This is also consistent with CIRCIA's statutory language, which references certain types of TTPs, such as denial-of-service attacks or exploitation of a zero-day vulnerability, as only examples, rather than a limitation on reportable covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A)(ii).

Fourth, for similar reasons, CISA has elected not to limit the definition of substantial cyber incident to impacts to specific types of systems, networks, or technologies. A number of commenters suggested that CISA should only require reporting of incidents that impact critical systems. CISA is proposing that under CIRCIA, if a cyber incident impacting a system, network, or technology that an entity may not believe is critical nonetheless results in actual impacts that meet the level of one or more of the threshold impact prongs, then the incident should be reported to CISA. In addition to helping ensure CISA receives reports on substantial cyber incidents even if they were perpetrated against a system, network, or technology deemed non-critical by the impacted covered entity, this approach also has the benefit of alleviating the need for a covered entity to proactively determine which systems, networks, or technologies it believes are "critical" and instead focus solely on the actual impacts of an incident as the primary determining factor as to whether a cyber incident is a reportable substantial cyber incident. For similar reasons, CISA is proposing to include, but not specifically distinguish, cyber incidents with impacts to OT. While it may be the case that cyber

incidents affecting OT are more likely to meet the impact thresholds in the definition of substantial cyber incident, CISA did not want to artificially scope out cyber incidents that primarily impact business systems but nevertheless result in many of the same type of impacts that could result from a cyber incident affecting OT.

Fifth, CISA is aware that in some cases, a covered entity will not know for certain the cause of the incident within the first few days following the occurrence of the incident. As is discussed in greater detail in Section IV.E.iv on the timing of submission of CIRCIA Reports, a covered entity does not need to know the cause of the incident with certainty for it to be a reportable substantial cyber incident. For incidents where the covered entity has not yet been able to confirm the cause of the incident, the covered entity must report the incident if it has a "reasonable belief" that a covered cyber incident occurred. If an incident meets any of the impact-based criteria, it would be reportable if the covered entity has a "reasonable belief" that the threshold impacts occurred as a result of activity without lawful authority, even if the specific cause is not confirmed. For the fourth prong, a reasonable belief that unauthorized access was caused by a third-party provider or a supply chain compromise would be sufficient to trigger a reporting obligation, even if the cause of the cyber incident was not yet confirmed. As discussed in Section III.C.ii on the purposes of the regulation, timely reporting is of the essence for CISA to be able to quickly analyze incident reports, identify trends, and provide early warnings to other entities before they can become victims. Accordingly, CISA believes its ability to achieve the regulatory purposes of CIRCIA would be greatly undermined if covered entities were allowed to delay reporting until an incident has been confirmed to have been perpetrated without lawful authority. Therefore, an incident whose cause is undetermined, but for which the covered entity has a reasonable belief that the incident may have been perpetrated without lawful authority, must be reported if the incident otherwise meets the reporting criteria. If, however, the covered entity knows with

certainty the cause of the incident, then the covered entity only needs to report the incident if the incident was perpetrated without lawful authority.

Finally, CISA expects a covered entity to exercise reasonable judgment in determining whether it has experienced a cyber incident that meets one of the substantiality thresholds. If a covered entity is unsure as to whether a cyber incident meets a particular threshold, CISA encourages the entity to either proactively report the incident or reach out to CISA to discuss whether the incident needs to be reported.

c. Reportability of Cyber Incidents Regardless of Cause

As noted in Section IV.A.ii.3.a.iv of this document, the CIRCIA statute limits which cyber incidents only involving unauthorized access can be considered a substantial cyber incident. Specifically, the statute states that to be considered a substantial cyber incident based on unauthorized access alone (without any of the impacts listed in the first three prongs, such as where the unauthorized access does not result in a "substantial" loss of confidentiality, integrity, or availability under the first prong), a cyber incident must be facilitated through or caused by a compromise of a CSP, managed service provider, another third-party data hosting provider, or by a supply chain compromise. See 6 U.S.C. 681b(c)(2)(A)(iii). Cyber incidents resulting in impacts other than unauthorized access and described in the first three impact prongs are not limited by the source or cause in the same manner. Similarly, as noted in Section IV.A.ii.3.a.iii of this document, CISA does not view the language in 6 U.S.C. 681b(c)(2)(A)(ii) regarding denial-of-service attacks, ransomware attacks, or exploitation of a zero-day vulnerability as suggesting a limitation on the vector or type of incidents in the third prong, or to suggest that denial-of-service attacks, ransomware attacks, or exploitation of a zero-day vulnerability that leads to the impacts described in the first two prongs would not be reportable if the impact thresholds are otherwise met. To ensure it is clear that cyber incidents resulting in threshold impacts other than unauthorized access should be reported regardless of cause or vector, including

whether they were or were not facilitated through or caused by a compromise of a third-party service provider or supply chain compromise, denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, CISA is proposing to include in the definition of substantial cyber incident explicit language to that effect. Specifically, CISA is proposing to include in the definition of substantial cyber incident the statement that a substantial cyber incident resulting in any of the threshold impacts identified in the first three prongs includes any cyber incident regardless of cause. See proposed § 226.1. As indicated in the proposed regulatory text, CISA interprets the phrase "regardless of cause" to include, but not be limited to, incidents caused by a compromise of a CSP, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

In today's complex cyber environment, entities frequently rely on third parties for various IT-related services, such as hosting, administering, managing, or securing networks, systems, applications, infrastructure, and digital information. Depending on what services are being provided, these third-party service providers—be they CSPs, managed service providers, or other third-party data hosting providers—via the systems and networks they manage, may provide an additional avenue through which nefarious individuals can seek to impact a service provider's customer's information systems or the information contained therein, which may also impact a covered entity. Similarly, adversaries may seek to impact covered entities by exploiting elements of the supply chain that a covered entity may rely upon.

This part of the substantial cyber incident definition is intended, in part, to ensure that a covered entity reports cyber incidents experienced by the covered entity that rise to the level of substantiality that warrants reporting even if the cyber incident in question was caused by a compromise of a product or service managed by someone other than the

covered entity. This clause is important to prevent the creation of a "blind spot" where the covered entity experiences a substantial cyber incident but escapes required reporting based on the manner in which the incident was initiated or perpetrated. Congress recognized the importance of this approach, and explicitly authorized it in CIRCIA for incidents that resulted in "unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." 6 U.S.C. 681b(c)(2)(A)(iii).

CISA believes the policy rationale for applying this provision to incidents resulting in unauthorized access or disruption of business or industrial operations (the third and fourth threshold prongs) applies equally to incidents resulting in a substantial loss of CIA, or a serious impact on the safety and resiliency of operational systems and processes (the first and second prongs). Accordingly, CISA proposes including this clause as a full part of the substantial cyber incident definition, so that it applies to cyber incidents that result in impacts meeting any of the four impact threshold prongs.

While a covered entity must report qualifying incidents that are the result of a compromise of a CSP, managed service provider, or other third-party data hosting provider, or by a supply chain compromise, it is important to note that this imposes reporting requirements solely on the covered entity that the incident impacts at a threshold level. Accordingly, a CSP, managed service provider, or other third-party service provider is not obligated, by virtue of this provision, to report an incident that causes threshold level impacts to one of its customers even if the impacts are the result of a compromise of the third-party's services, network, software, etc. A third-party service provider only needs to report a cyber incident if (a) the third-party service provider independently meets the definition of covered entity, and (b) the third-party service provider itself experiences impacts that rise to the level of a substantial cyber incident.

Note, however, a covered entity third-party provider could experience a reportable substantial cyber incident without the third-party service provider experiencing direct impacts from a cyber incident that exploits or compromises their information networks or systems. This would be the case where a cyber incident facilitated through or caused by a compromise of the third-party service provider meeting the definition of a covered entity caused enough impacts to one or more of the provider's customers that the cumulative effect of the incident resulted in a substantial disruption of the third-party service provider's business operations.

This part of the proposed substantial cyber incident definition is also intended to emphasize that the first three prongs of the definition of substantial cyber incident are also TTP, incident type, and vector agnostic. While denial-of-service attack, ransomware attack, and exploitation of a zero-day vulnerability are specifically listed in this part of the definition in light of their inclusion in 6 U.S.C. 681b(c)(2)(A)(ii), their inclusion in the statute and this part of the definition are as examples only. Any cyber incident experienced by a covered entity, regardless of cause, that meets the impact thresholds in the first three prongs of the definition of substantial cyber incident would be considered a substantial cyber incident. This includes, for example, exploitation of a previously known vulnerability, and not just exploitation of a zero-day vulnerability. For further examples of incidents that typically would and would not be considered a substantial cyber incident, see Section IV.A.ii.3.e of this document.

d. Exclusions

In 6 U.S.C. 681b(c)(2)(C), Congress identified two types of events that CISA must exclude from the types of incidents that constitute covered cyber incidents. Specifically, Congress stated that CISA was to "exclude (i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and (ii) the threat of disruption as extortion,

as described in section 2240(14)(A).” 6 U.S.C. 681b(c)(2)(C). In addition, CISA is proposing excluding any lawfully authorized U.S. Government or SLTT Government entity activity including activities undertaken pursuant to a warrant or other judicial process.

CISA is proposing to incorporate these exclusions into the definition of substantial cyber incident by proposing a statement reiterating these exclusions at the end of the definition itself. The statement added to the proposed definition of substantial cyber incident is taken almost verbatim from the CIRC Model Definition which itself includes both of the exclusions contained in 6 U.S.C. 681b(c)(2)(C). Additional information on each of the prongs of this exclusory statement are contained in the following three subsections.

i. Lawfully Authorized Activities of a United States Government Entity or SLTT Government Entity

CISA proposes excluding from the definition of substantial cyber incident any lawfully authorized United States Government entity or SLTT Government entity activity, including activities undertaken pursuant to a warrant or other judicial process. This exception, which is similar to an exception contained in the CIRC Model Definition, is intended to except from reporting any incident that occurs as the result of a lawful activity of a Federal or SLTT law enforcement agency, Federal intelligence agency, or other Federal or SLTT Government entity. This exception does not, however, allow a covered entity to delay or forgo reporting a covered cyber incident to CISA because it has reported a covered cyber incident to, or is otherwise working with, law enforcement. It simply says that a lawful activity conducted by a Federal or SLTT governmental entity, such as a search or seizure conducted pursuant to a warrant, is not itself a substantial cyber incident.

CISA believes this exception is warranted as reports on lawful Federal or SLTT government activity would in no meaningful way further the articulated purposes of the regulation, such as analyzing adversary TTPs and enabling a better understanding of the current cyber threat environment. This exception provides further clarity on the scope of cyber incident, which is defined as an occurrence "without lawful authority." Moreover, failure to exclude such incidents from required reporting could negatively impact a covered entity's willingness to work with Federal or SLTT law enforcement, intelligence, or other government agencies if such cooperation could result in new regulatory reporting obligations.

ii. Incidents Perpetrated in Good Faith by an Entity in Response to a Specific Request by the Owner or Operator of the Information System

Section 681b(c)(2)(C)(i) of title 6, United States Code, states that the description of the types of substantial cyber incidents that constitute covered cyber incidents shall exclude "any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system." CISA is proposing incorporating this exclusion verbatim into the proposed definition of substantial cyber incident.

There are a variety of situations in which a cyber incident could occur at a covered entity as the result of an entity acting in good faith to a request of the owner or operator of the information system through which the cyber incident was perpetrated. One example of this would be if a third-party service provider acting within the parameters of a contract with the covered entity unintentionally misconfigures one of the covered entity's devices leading to a service outage. Another example would be a properly authorized penetration test that inadvertently results in a cyber incident with actual impacts. Congress intended that such incidents, when the result of good faith

actions conducted pursuant to a specific request by the owner or operator of the information system at issue, be excluded from the CIRCIA reporting requirements.

In addition to the examples provided above, CISA interprets this exclusion to also exclude from reporting cyber incidents that result from security research testing conducted by security researchers who have been authorized by the covered entity or the owner or operator of the impacted information system to attempt to compromise the system, such as in accordance with a vulnerability disclosure policy or bug bounty programs published by the owner or operator. However, because the exception only applies to "cyber incident[s] perpetrated in good faith . . . in response to a specific request by" the information system owner or operator, this exception would only apply to this type of research where the bug bounty program, vulnerability disclosure policy, or other form of authorization preceded the discovery of the incident. That said, CISA anticipates that this example would occur rarely, as good faith security research should generally stop at the point the vulnerability can be demonstrated and should not typically engage in activity that would result in a covered cyber incident.[149]

Regarding this exclusion, the request that causes the incident need not necessarily come from the impacted covered entity itself, but rather from the owner or operator of the information system at issue. While the owner or operator of the information system through which the incident was caused will often be the covered entity, that may not always be the case. For example, in some situations involving a CSP or managed service provider, the service provider may duly authorize a penetration test on its own systems or software. If such testing inadvertently resulted in a cyber incident at the service provider, it could have downstream effects on one or more of the service provider's customers

[149] See, e.g., CISA, *Vulnerability Disclosure Policy Template* ("Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems."), available at https://www.cisa.gov/vulnerability-disclosure-policy-template-0.

(such as by taking out of operation a key cloud-based software that the customers rely upon for core operations). Such downstream effects could themselves constitute substantial cyber incidents, and, absent this exclusion, could be considered a covered cyber incident, subject to reporting under the proposed CIRCIA regulation if an impacted customer was a covered entity. However, because such a substantial cyber incident would have been perpetrated in good faith pursuant to a penetration test duly authorized by the information system's owner or operator (even if the owner or operator is not the sole impacted entity), neither the covered entity nor the service provider would be required to report the incident.

Conversely, circumstances could occur where a covered entity or the information system's owner or operator authorizes an action that results in a reportable impact despite the immediately precipitating action being approved by the covered entity or information system's owner or operator. For instance, if a covered entity, in response to a ransomware attack or other malicious incident, decides to take an action itself resulting in reportable level impacts, such as shutting down a portion of its system or operations, to prevent possibly more significant impacts, this would still be considered a reportable substantial cyber incident. In such a case, because the cyber incident itself was not perpetrated in good faith, and the threshold level impacts would not have occurred but for the initial cyber incident, CISA would not consider the covered entity's actions to meet the "good faith" exception even though the covered entity directed the immediately precipitating action in a good faith attempt to minimize the potential impacts of a cyber incident.

iii. The Threat of Disruption as Extortion, as Described in 6 U.S.C. 650(22)

Section 681b(c)(2)(C)(ii) of title 6, United States Code, provides that the description of the types of substantial cyber incidents that constitute covered cyber events shall exclude "the threat of disruption as extortion, as described in section 2240(14)(A)."

CISA is proposing incorporating this exclusion verbatim into the proposed definition of substantial cyber incident with a minor technical correction to include the updated citation to the definition for ransomware attack in CIRCIA.[150]

Section 650(22) of title 6, United States Code, defines "ransomware attack" as "an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment." While, as noted above, the definition of cyber incident excludes incidents where jeopardy is "imminent" but not "actual," the definition of ransomware attack includes threatened disruptions as a means of extortion. This exclusion clarifies that the threat of disruption of a system to extort a ransom payment that does not result in the actual disruption of a system is an "imminent," but not "actual," event, and is therefore not required to be reported as a covered cyber incident.

However, if a covered entity makes a ransom payment in response to such a threat, even if the disruption never materializes into a substantial cyber incident subject to covered cyber incident reporting required by this Part, the payment itself would still be subject to ransom payment reporting required by this Part. Only such a threat where no ransom payment is made and the disruption never materializes into a substantial cyber incident would remain excluded from mandatory reporting. Additionally, as noted in Section IV.A.ii.3.a.i above, this exclusion would not prevent a cyber incident involving a threat to disclose information obtained from an information system without authorization

[150] The definition of ransomware attack contained in Section 2240(14)(A) moved locations within the U.S. Code as part of the consolidation of definitions in the CISA Technical Corrections, *supra* note 135. While the CISA Technical Corrections did not update this cross-reference in CIRCIA, pursuant to the rule of construction in Section (f)(2) of the CISA Technical Corrections, CISA considers 6 U.S.C. 650 as the proper citation for the definition of "ransomware attack" for purposes of the proposed regulation.

from being a reportable substantial cyber incident if the cyber incident otherwise meets the threshold for being a substantial cyber incident, e.g., under prong (a)(1) of the substantial cyber incident definition due to the initial loss of confidentiality of the information system.

e. Examples of Cyber Incidents that Meet the Definition of Substantial Cyber Incident

To help covered entities determine what might and might not be considered a substantial cyber incident under the proposed definition, CISA is providing the following examples of (a) cyber incidents that are likely to be considered substantial cyber incidents, and (b) cyber incidents that are unlikely to be considered substantial cyber incidents. Both of these lists are for exemplary purposes only and are not intended to be exhaustive. Moreover, inclusion on either list is not a formal declaration that a similar incident would or would not be a substantial cyber incident if the agency were to finalize the definition as proposed. Inclusion here simply indicates the relative likelihood that such an incident would or would not rise to the level of a reportable substantial cyber incident. Determinations as to whether a cyber incident qualifies as a substantial cyber incident would need to be made on a case-by-case basis considering the specific factual circumstances surrounding the incident. Note, CISA continues to encourage reporting or sharing of information about all cyber incidents, even if it would not be required under the proposed regulations.

EXAMPLES OF INCIDENTS THAT LIKELY WOULD QUALIFY AS SUBSTANTIAL CYBER INCIDENTS

(1) A distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time.
(2) Any cyber incident that encrypts one of a covered entity's core business systems or information systems.
(3) A cyber incident that significantly increases the potential for a release of a hazardous material used in chemical manufacturing or water purification.
(4) A cyber incident that compromises or disrupts a BES cyber system that performs one or more reliability tasks.

(5) A cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls.
(6) The exploitation of a vulnerability resulting in the extended downtime of a covered entity's information system or network.
(7) A ransomware attack that locks a covered entity out of its industrial control system.
(8) Unauthorized access to a covered entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.
(9) Unauthorized access to a covered entity's business systems using compromised credentials from a managed service provider.
(10) The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage account.

EXAMPLES OF INCIDENTS THAT LIKELY WOULD NOT QUALIFY AS SUBSTANTIAL CYBER INCIDENTS

(1) A denial-of-service attack or other incident that only results in a brief period of unavailability of a covered entity's public-facing website that does not provide critical functions or services to customers or the public.
(2) Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic.
(3) The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems.
(4) Malicious software is downloaded to a covered entity's system, but anti-virus software successfully quarantines the software and precludes it from executing.
(5) A malicious actor exploits a known vulnerability, which a covered entity has not been able to patch but has instead deployed increased monitoring for TTPs associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.

f. Considerations

In 6 U.S.C. 681b(c)(2)(B), Congress identified three considerations for CISA in deciding what types of substantial cyber incidents constitute covered cyber incidents. Specifically, Congress instructed CISA to consider "(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue; (ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and (iii) potential impacts on

industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. 681b(c)(2)(B).

Throughout the process of analyzing what types of cyber incidents should constitute a substantial cyber incident, CISA kept in mind the considerations enumerated by Congress in 6 U.S.C. 681b(c)(2)(B). Some of the considerations are directly reflected in what CISA believes will be a substantial cyber incident under the proposed definition. For instance, as discussed above, factors such as the type, volume, and sensitivity of the data at issue, or the number of individuals directly or indirectly affected by an incident, will impact whether an incident should be considered a substantial cyber incident. Incidents where less data is impacted, the impacted data is not particularly sensitive, and/or the number of individuals directly or indirectly affected, are less likely to be considered substantial cyber incidents. Conversely, incidents involving large volumes of impacted data, sensitive data, or large numbers of impacted individuals are more likely to be considered substantial cyber incidents. Similarly, incidents that impact industrial control systems are much more likely to result in the second prong of the substantial cyber incident definition being met than incidents that solely impact business systems.

There is one consideration listed in 6 U.S.C. 681b(c)(2)(B), however, that CISA considered, but ultimately determined should not affect whether a cyber incident rises to the level of a substantial cyber incident in this proposed rule. That is the consideration listed in 6 U.S.C. 681b(c)(2)(B)(i), "the sophistication or novelty of the tactics used to perpetrate such a cyber incident." CISA believes there is value in receiving reports on all types of substantial cyber incidents, whether the tactics used are sophisticated or not, novel or not. If an unsophisticated TTP is being used to cause substantial impacts to covered entities, CISA believes there is value in knowing that so CISA and its Federal partners can warn other potential victims that this tactic is being used and can identify

and share new or previously identified methods to mitigate vulnerabilities that allow this tactic to be effective.

Similarly, if there is a resurgence in adversary use of a TTP that has previously been reported upon, there is value in CISA knowing that so it can alert entities to make sure they are maintaining effective defensive measures to counter that tactic. In fact, CISA routinely adds older vulnerabilities to the Known Exploited Vulnerability database that CISA publishes based on the fact that the previously identified vulnerabilities are actively being exploited. This allows CISA and others to emphasize with the public the importance of addressing those vulnerabilities.

Finally, it is possible that neither CISA nor the reporting entity might know the sophistication or novelty of the TTP at the time or reporting. CISA and/or the reporting entity may need time to assess the incident before being able to determine its sophistication and novelty, and CISA does not believe reporting should be delayed simply to evaluate the tactics used to perpetrate a cyber incident. For the aforementioned reasons, CISA is proposing that the relative sophistication or novelty of a TTP used in perpetrating a cyber incident should not influence whether that incident meets the definition of a substantial cyber incident.

g. Harmonization of Definition with the CIRC Model Definition and Other Regulatory Definitions

As discussed in Section III.B of this document, a number of different Federal departments and agencies oversee regulations, directives, or other programs that require certain entities to report cyber incidents. CISA has received many comments from stakeholders encouraging CISA to harmonize the CIRCIA reporting requirements with the requirements in other regulations, to include the definition of what is a reportable incident. See Section III.F.x of this document. CISA fully supports the harmonization of regulatory requirements where practicable and has been an active participant in the

CIRC's efforts to identify potential approaches to harmonizing Federal regulatory cyber incident reporting requirements. One of the specific recommendations made by the Department in its CIRC-informed Report to Congress is for departments and agencies to consider adopting a model definition for a reportable cyber incident where practicable.[151]

Cognizant of that recommendation and the value in seeking harmonization where practical, CISA considered the CIRC Model Definition for a reportable cyber incident during the development of the proposed CIRCIA definition for a substantial cyber incident. Ultimately, CISA did elect to incorporate many aspects of the CIRC Model Definition into the proposed CIRCIA definition for a substantial cyber incident, some verbatim. CISA did not propose using the CIRC Model Definition in its entirety, however, due in part to specific statutory requirements imposed within CIRCIA and the specific purposes CIRCIA is designed to achieve.

One example of where CISA's proposed definition differs from the CIRC Model Definition due to specific language contained in CIRCIA is in the sentence used to introduce the threshold criteria that elevate an incident to the level of a reportable or substantial cyber incident. Specifically, the first sentence of the CIRC Model Definition states "[a] reportable cyber incident is an incident that leads to, or, if still under the covered entity's investigation, could reasonably lead to any of the following [impacts]."[152] The section of CIRCIA related to substantial cyber incidents states that for a cyber incident to be a substantial cyber incident, it "requires the occurrence of" one of the enumerated impacts. 6 U.S.C. 681b(c)(2)(A). Because CIRCIA requires actual occurrence of the impacts, CISA does not propose including the phrase "or, if still under the covered entity's investigation, could reasonably lead to any of the following" in the

---

[151] *DHS Report*, *supra* note 4, at 25 ("Recommendation 1: The Federal Government should adopt a model definition of a reportable cyber incident wherever practicable. Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to a model definition of a reportable cyber incident.").
[152] *Id.* at 26.

initial sentence of the CIRCIA definition for substantial cyber incident. For similar reasons, CISA did not propose inclusion of the CIRC Model Definition's fourth threshold prong "*potential* operational disruption" (emphasis added), as CISA interprets CIRCIA to require actual impact, not potential impact, for an incident to be a substantial cyber incident.

Another substantive difference between the CIRC Model Definition and the CIRCIA proposed definition for substantial cyber incident is the inclusion in the CIRCIA proposed definition of a separate threshold prong based on a serious impact to safety and resiliency of a covered entity's operational systems and processes. While the CIRC Model Definition does not include a similar threshold prong, this threshold is specifically listed in CIRCIA as one of the minimum types of impacts that would qualify a cyber incident for inclusion as a covered cyber incident. 6 U.S.C. 681b(c)(2)(A)(i). Accordingly, CISA determined it was important to include that impact as a basis for coverage in its definition of substantial cyber incident despite its absence in the CIRC Model Definition.

CISA also occasionally modified the language used in the CIRC Model Definition to terminology that is consistent with CIRCIA and other portions of the proposed CIRCIA regulation. For example, CISA proposes using the term "covered entity's information system" instead of the CIRC Model Definition's construction "a covered information system" in the first threshold prong of the definition. Because CIRCIA does not distinguish between covered and not covered information systems, networks, or technologies, the use of the word "covered" in this manner would be inconsistent.

In addition to the CIRC Model Definition, CISA also considered how other Federal regulations defined reportable cyber incidents. While many of the regulations CISA reviewed have some similarities in how they define and interpret what is a reportable cyber incident, the specific language, structure, examples, and actual

requirements varied greatly based on the specific agency mission and purpose of the regulation. As the CIRC was established to make recommendations on how to harmonize these disparate regulations, and the DHS Report specifically recommends that agencies evaluate the feasibility of adapting current and future cyber incident reporting requirements to align with a model definition of a reportable cyber incident,[153] CISA ultimately felt that the path that would most effectively support harmonization across the various Federal cyber incident reporting requirements was to align the definition of covered cyber incident, to the extent practicable, with the CIRC Model Definition.

iii. CIRCIA Reports

1. CIRCIA Report

CISA is proposing to include in the regulation a definition of the term CIRCIA Report. CIRCIA requires a covered entity to submit (either directly or through a third party) a report to CISA when it reasonably believes a covered cyber incident occurred, makes a ransom payment, or experiences one of a number of circumstances that requires the covered entity to update or supplement a previously submitted Covered Cyber Incident Report. 6 U.S.C. 681b(a)(1)-(3). These reports are called Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports, respectively. CIRCIA additionally allows covered entities that make a ransom payment associated with a covered cyber incident to submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. 6 U.S.C. 681b(a)(5)(A). CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report.

CISA is proposing a term CIRCIA Report to be an umbrella term that encompasses all four types of covered entity reports collectively. Accordingly, CISA is proposing to define CIRCIA Report to mean a Covered Cyber Incident Report, Ransom

[153] *Id.* at 25-27.

Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report.

In some instances, CIRCIA refers to "reports," and at other times refers to "information" (either information contained in a CIRCIA Report or information about cyber incidents, covered cyber incidents, or ransom payments). CISA understands Congress' use of these different terms in different contexts within CIRCIA to be intentional, and therefore replicates these distinctions in the proposed rule. Specifically, references to a CIRCIA Report or any individual report (i.e., a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report) throughout this NPRM are intended to refer to the submission as a whole. By contrast, references to information (either in a CIRCIA Report or about cyber incidents, covered cyber incidents, or ransom payments) are intended to refer to discrete pieces of facts and ideas (which sometimes may be contained within a CIRCIA Report, perhaps along with other pieces of information), rather than the submission as a whole.

2. Covered Cyber Incident Report

CISA is proposing to include in the regulation a definition of the term Covered Cyber Incident Report. CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. 6 U.S.C. 681b(a)(1). CISA is proposing to refer to this type of report as a Covered Cyber Incident Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident as required by this Part. CISA is further proposing that a Covered Cyber Incident Report also includes any additional, optional information submitted as part of a Covered Cyber Incident Report.

As noted in the definition, a Covered Cyber Incident Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered

entity may voluntarily include within a Covered Cyber Incident Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will be considered part of the Covered Cyber Incident Report. Additional requirements related to the manner, form, content, and other aspects of a Covered Cyber Incident Report are described in Sections IV.E.i-iii of this document and §§ 226.6, 226.7, and 226.8 of the proposed regulation.

3. Ransom Payment Report

CISA is proposing to include in the regulation a definition of the term Ransom Payment Report. CIRCIA requires a covered entity that makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, to report that payment to CISA. 6 U.S.C. 681b(a)(2)(A). CISA is proposing to refer to this type of report as a Ransom Payment Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a ransom payment as required by this Part. CISA is further proposing for a Ransom Payment Report to also include any additional, optional information submitted as part of a Ransom Payment Report.

As noted in the definition, a Ransom Payment Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Ransom Payment Report additional information submitted pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will be considered part of the Ransom Payment Report. Additional requirements related to the manner, form, content, and other aspects of a Ransom Payment Report are described in Sections IV.E.i-iii of this document and §§ 226.6, 226.7, and 226.9 of the proposed regulation. If the ransom payment being reported is the result of a covered cyber incident that the covered entity or a third party acting on its behalf has already reported to CISA,

then the Ransom Payment Report also would be considered a Supplemental Report and must meet any requirements associated with Supplemental Reports as well.

4. Joint Covered Cyber Incident and Ransom Payment Report

CISA is proposing to include in the regulation a definition of the term Joint Covered Cyber Incident and Ransom Payment Report. Pursuant to 6 U.S.C. 681b(a)(5)(A), covered entities that make a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting timeframe for reporting the covered cyber incident may submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to simultaneously report both a covered cyber incident and ransom payment related to the covered cyber incident being reported. CISA is proposing that a Joint Covered Cyber Incident and Ransom Payment Report also include any additional, optional information submitted as part of the report.

As noted in the definition, a Joint Covered Cyber Incident and Ransom Payment Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Joint Covered Cyber Incident and Ransom Payment Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will be considered part of the Joint Covered Cyber Incident and Ransom Payment Report. Additional requirements related to the manner, form, and content of a Joint Covered Cyber Incident and Ransom Payment Report are described in Sections IV.E.i-iii of this document and §§ 226.6, 226.7, and 226.10 of the proposed regulation.

5. Supplemental Report

CISA is proposing to include in the regulation a definition of the term Supplemental Report. CIRCIA requires a covered entity to promptly submit an update or supplement to a previously submitted Covered Cyber Incident Report under certain circumstances. 6 U.S.C. 681b(a)(3). CISA is proposing to refer to this type of report as a Supplemental Report. CISA is proposing that the term Supplemental Report be used to describe a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required by this Part. CISA is further proposing that a Supplemental Report also include any additional, optional information submitted as part of a Supplemental Report.

As noted in the definition, a Supplemental Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Supplemental Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information is considered part of the Supplemental Report. Additional requirements related to the manner, form, content, and other aspects of a Supplemental Report are described in Sections IV.E.i-iii of this document and §§ 226.6, 226.7, and 226.11 of the proposed regulation.

iv. Other Definitions

1. CIRCIA

CISA is proposing to define the term CIRCIA to mean the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended. This will simplify the regulatory text by allowing CISA to refer to CIRCIA without having to use the full title of the statute or full legal citation throughout the regulation.

2. CIRCIA Agreement

CISA is proposing to create the term CIRCIA Agreement and define it as an agreement between CISA and another Federal agency that meets the requirements of § 226.4(a)(2), that has not expired or been terminated, and which, when publicly posted in accordance with § 226.4(a)(5), indicates the availability of a substantially similar reporting exception. CISA believes the establishment and defining of this term will allow covered entities to better identify circumstances where they can leverage the substantially similar reporting exception and avoid potentially duplicative reporting to another Federal department or agency and CISA. Additional details on both the CIRCIA Agreement and the substantially similar reporting exception can be found in Section IV.D.i of this document.

3. Cloud Service Provider

CISA is proposing to include a definition for the term cloud service provider. CISA believes defining this term is important to ensure that covered entities understand the meaning of an unauthorized access or disruption of business or industrial operations due to a loss of service facilitated through, or caused by, a compromise of a CSP, as that is one example of a substantial cyber incident provided in CIRCIA. 6 U.S.C. 681b(c)(2)(A)(iii). Section 650 of title 6, United States Code, defines the term CSP as "an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto." 6 U.S.C. 650(3). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this definition in the regulation.

4. Cybersecurity and Infrastructure Security Agency (CISA)

CISA is proposing to include a definition for the term Cybersecurity and Infrastructure Security Agency or CISA. This term is used repeatedly throughout the proposed regulation to describe the Federal entity responsible for the oversight of the

proposed CIRCIA regulation and with whom covered entities and other stakeholders will engage on various activities required under the regulation. CISA is proposing to define Cybersecurity and Infrastructure Security Agency or CISA as the Cybersecurity and Infrastructure Security Agency as established under section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 and subsequent laws, or any successor organization.

5. Cybersecurity Threat

CISA is proposing to include a definition for the term cybersecurity threat. Defining the term cybersecurity threat is a streamlined approach that provides needed context for the requirement in 6 U.S.C. 681b(c)(8)(D) that CISA include in the final rule procedures for, among other things, protecting privacy and civil liberties, for certain personal information received in CIRCIA Reports that is not directly related to a cyber threat. For the reasons explained below, CISA is proposing to use and define the term cybersecurity threat instead of "cyber threat."

CIRCIA defines the term "cyber threat" as "ha[ving] the meaning given the term 'cybersecurity threat' in section 2200 [6 U.S.C. 650]" of the Homeland Security Act of 2002, as amended. Section 650 of title 6, United States Code, defines "cybersecurity threat" as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system," other than "any action that solely involves a violation of a consumer term of service or a consumer licensing agreement." 6 U.S.C. 650(8). Rather than using the term "cyber threat," CISA is proposing to use the term "cybersecurity threat," with this definition effectively verbatim, because CISA believes it is most consistent with CIRCIA.

6. Director

CISA is proposing to include a definition for the term Director and to define it as the Director of CISA, any successors to that position, or any designee. CISA is proposing to include this definition as CIRCIA assigns the Director specific responsibilities related to implementation of the CIRCIA regulation.

7. Information System

CISA is proposing to include a definition for the term information system. This term is a key term for the proposed regulation as, among other things, it is used within the definition of ransomware attack and substantial cyber incident as well as to help identify the types of information that a covered entity must provide in reports required under the regulation.

The Paperwork Reduction Act of 1980 (PRA), 44 U.S.C. 3502, defines information system as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[154] Section 650 of title 6, United States Code, defines information system as having the meaning given the term in the PRA, 44 U.S.C. 3502, specifically including "industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. 650(14).

Because the 6 U.S.C. 650 definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing defining Information using the language contained in the definition in 6 U.S.C. 650(14) with the addition of an explicit acknowledgment that OT is included within the definition of information system. CISA believes OT is encompassed in the definition of information system contained within 6 U.S.C. 650(14) by reference to industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and

[154] 44 U.S.C. 3502(8).

programmable logic controllers; however, CISA is proposing to explicitly include the words "operational technology systems" within the definition in light of the common industry use of this term to avoid any potential misinterpretations about whether OT is encompassed by the proposed CIRCIA definition of information systems.

8. Managed Service Provider

CISA is proposing to include a definition for the term managed service provider. CISA believes it is important to define this term to ensure that covered entities understand the meaning of an unauthorized access or disruption of business or industrial operations due to a loss of service facilitated through, or caused by, a compromise of a managed service provider, as that is one example of a substantial cyber incident provided in CIRCIA. 6 U.S.C. 681b(c)(2)(A)(iii). The term managed service provider is defined in 6 U.S.C. 650(18) and sets out three criteria that must be met to qualify as a managed service provider. The definition reads, "an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center." 6 U.S.C. 650(18). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this same definition of managed service provider in the regulation.

9. Personal Information

CISA is proposing to include a definition for the term personal information. Personal information is a key term in the proposed regulation as CIRCIA requires CISA to undertake certain steps to protect personal information. See e.g., 6 U.S.C. 681e(a)(3). CISA is proposing to define the term personal information to mean information that identifies a specific individual or information associated with an identified or identifiable individual. Under this definition, personal information would include, but are not limited

to, both identifying information such as photographs, names, home addresses, direct telephone numbers, and Social Security numbers as well as information that does not directly identify an individual but is nonetheless personal, nonpublic, and specific to an identified or identifiable individual. Examples would include medical information, personal financial information (e.g., an individual's wage or earnings information; income tax withholding records; credit score; banking information), contents of personal communications, and personal web browsing history. This proposed definition would include "personally identifiable information," as defined in OMB Memorandum M-17-12 as referring to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, but also proposes to include information that might not be clearly linkable to an individual but would nonetheless relate to a specific individual and be considered personal and nonpublic, such as an individual's web browsing history or the content of an email. CISA is proposing this definition to encompass the broad range of personally sensitive information that a cybersecurity incident might implicate, including the content of personal communications, which might not be able to be used on its own to identify an individual, to ensure that all personally sensitive information is handled appropriately.

CISA is not proposing to include in this definition information that does not relate to a specific individual. Therefore, information such as general business telephone numbers or business financial information would generally not be considered personal information under this definition.

This proposed definition of "personal information" would be different and broader than the approach taken by the Cybersecurity Information Sharing Act of 2015, (6 U.S.C. 1501 *et seq*.). 6 U.S.C. 1503(d)(2) more narrowly requires removal of information that is "known at the time of sharing" to be "personal information" that

identifies a specific person or belongs to a specific person rather than information that is linked or linkable to a specific person. CISA welcomes public comment on this proposed definition of "personal information" and whether CISA should instead adopt the approach taken by the Cybersecurity Information Sharing Act of 2015 to defining personal information.

10. Ransom Payment

CISA is proposing to include a definition for the term ransom payment. Ransom payment is a key term in the proposed regulation as CIRCIA requires that covered entities report ransom payments to CISA within 24 hours of the payment being made. 6 U.S.C. 681b(a)(2). CISA is proposing to use the definition of the term ransom payment from CIRCIA in the regulation verbatim.

11. Ransomware Attack

CISA is proposing to include a definition for the term ransomware attack. CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack to report the ransom payment to CISA within 24 hours of making the payment. 6 U.S.C. 681b(a)(2). CISA believes including a definition for the term ransomware attack will help covered entities determine whether they are required to submit a Ransom Payment Report to CISA.

Section 650(22) of title 6, United States Code, defines the term ransomware attack as "(A) [] an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and (B) does not include any such event where the demand for payment is (i) not genuine; or (ii) made in good faith by an entity in response to a specific request

by the owner or operator of the information system." 6 U.S.C. 650(22). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this definition with a few minor modifications described below.

First, in defining the term ransomware attack, CISA is proposing to replace the term "incident" (which is used in the statutory definition of ransomware attack) with the full definition of "incident" as found in section 2200(12) of the Homeland Security Act of 2002, as amended (6 U.S.C. 650(12)) (i.e., "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system"). The definition of "incident" in 6 U.S.C. 650(12) applies to the term "incident" throughout Title XXII of the Homeland Security Act of 2002, as amended, including to the term "incident" within the statutory definition of ransomware attack at 6 U.S.C. 650(22).[155]

Using this definition of "incident" is not only consistent with the statute, but it also avoids CISA specifically defining the term "incident" in the regulation, which CISA believes could create confusion in light of the inclusion in the proposed regulation of a definition for the term cyber incident.

CISA considered, but ultimately decided against, proposing the use of the term "cyber incident" in place of "incident" in the definition of ransomware attack. As noted earlier in the discussion of the proposed definition for cyber incident, CIRCIA removed the "imminently jeopardizes" clause found in the Homeland Security Act's definition of

---

[155] As originally enacted, CIRCIA explicitly included a definition of both "cyber incident" and "incident." See Pub. L. 117-103. However, when the definition of "incident" was moved as part of the consolidation of definitions in the CISA Technical Corrections to the beginning of Title XXII of the Homeland Security Act (6 U.S.C. 650(12)), the definition of "incident" in CIRCIA was struck as a conforming edit to remove the redundancy. See CISA Technical Corrections, *supra* note 135, Section (b)(2)(N)(v). Further, in the original as-enacted version of CIRCIA, both uses of the term "incident" (as opposed to the CIRCIA term "cyber incident") were in definitions that were moved to 6 U.S.C. 650 as part of the CISA Technical Corrections, namely the definitions of ransomware attack and supply chain compromise. See 6 U.S.C. 650(22) and (28).

"incident" from CIRCIA's definition of cyber incident, instead opting to require "actual jeopardy" for an event to qualify as a cyber incident under CIRCIA. Consequently, using the term "cyber incident" in lieu of "incident" in the definition of ransomware attack would have a substantive impact on the definition. CISA believes that Congress intentionally used the term "incident" (in lieu of the term "cyber incident") in the definition of ransomware attack to account for the fact that a ransomware attack may involve a threat of disruption (i.e., imminent jeopardy) and that such a threat—without the disruption ever occurring—may be sufficient to extort a ransom payment. Moreover, Congress specifically included incidents where jeopardy is "imminent" but not "actual" in its definition of ransomware attack, including both threatened and realized interruptions as means of extortion. Therefore, to avoid a substantive change to the meaning of the term ransomware attack (which would also narrow the scope of reportable ransom payments), while also avoiding the confusion that could be caused by similarly defining both "cyber incident" and "incident" in the proposed rule, the proposed rule relies on 6 U.S.C. 650(12)'s definition of the word "incident" in lieu of the word "incident" within the definition of the term ransomware attack.

Second, the NPRM replaces the word "includes" with "involves, but need not be limited to, the following." This change was made to avoid the implication that the term ransomware attack includes some other category of incidents not otherwise described here (i.e., that "includes" means "includes, but is not limited to"). At the same time, the definition is not intended to suggest that any occurrence that includes more than the three listed elements is no longer considered a ransomware attack. The "need not be limited to" clause is intended to convey that, as long as the three listed elements are involved in the occurrence in question, any additional facts about the occurrence would not cause it to be outside of the definition of a ransomware attack.

Third, CISA is proposing to delete the phrase "a demand" from the third prong of the statutory definition, thus modifying it from "to extort a demand for a ransom payment" to "to extort a ransom payment." This is intended to clarify that this prong requires that the threat actor extort the ransom payment itself from the victim (consistent with the common understanding of a typical ransomware attack), and not a process where the extortion is a demand for the victim entity to demand a ransom payment from a third entity. This interpretation is supported by the legislative history of CIRCIA showing that Congress understood this term to encompass the traditional ransomware attacks that the country was experiencing at a significantly increasing frequency in the months and years prior to CIRCIA's passage[156] and not a novel two-step extortion of a demand that, to CISA's knowledge, has never occurred. Numerous canons of statutory interpretation, to include the Absurdity Doctrine, the Harmonious-Reading Canon, and the canon of Purposive Construction, further support this interpretation.

CISA's proposed definition also includes two minor, non-substantive changes to improve the readability of the definition. First, CISA is proposing to separate the statutory description of the type of incident that constitutes a ransomware attack into three subparts, one for each of the three prongs of the definition. Second, in the portion of the statutory definition contained in the newly delineated paragraph (1), CISA is

---

[156] See, e.g., *Stakeholder Perspectives Hearing, supra* note 17, at 12-13 (statement of Rep. Andrew Garbino, Ranking Member, Subcomm. on Cybersecurity, Infrastructure Protection, and innovation of the H. Comm. on Homeland Security) ("Everyone here remembers the ransomware attacks on Colonial Pipeline and JBS Meats . . . We must ensure that CISA has the visibility it needs to help defend our Federal networks and to help our critical infrastructure owners and operators protect themselves."), (statement of Rep. John Katko, Ranking Member, H. Comm. on Homeland Security) ("Every single day, entities, large and small, are affected by the scourge of ransomware . . . ."); 168 Cong. Rec. S1149-50 (daily ed. Mar. 14, 2022) (statement of Sen. Mark Warner) ("[R]ansomware attacks are a serious national security threat that have affected everything from our energy sector to the Federal Government and Americans' own sensitive information. . . As . . . ransomware attacks continue to increase, the Federal Government must be able to quickly coordinate a response and hold bad actors accountable."); HSGAC Minority Staff Report, *America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies* at iii ("Ransomware is a type of malware that encrypts victims' computer systems and data, rendering the systems unusable and the data unreadable. Perpetrators then issue a ransom demand . . . If the victim pays, hackers *may* provide the victim with a key to decrypt their systems and data . . . ." (italics in original)), available at https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/.

proposing to eliminate the second instance of the phrase "use or threat of use" and instead insert roman numerals and the conjunction "or" to make clear that the "use or threat of use" phrase applies to both (i) unauthorized or malicious code on an information system or (ii) another digital mechanism such as a denial-of-service attack.

The proposed definition of ransomware attack contains language mirroring language in the CIRCIA authorizing legislation that excludes from the definition any event where the demand for a ransom payment is "not genuine" or is "made in good faith by an entity in response to a specific request by the owner or operator of the information system." Circumstances in which an entity may determine a ransom demand is "not genuine" include if the demand is a known hoax or the demand lacks necessary information for the receiving entity to comply, such as an amount demanded or payment instructions. Ransom demands "made in good faith by an entity in response to a specific request by the owner or operator of the information system" typically would include those that are part of red teaming, penetration testing, vulnerability analysis, training exercises, or other authorized activities designed to test prevention, detection, response, or other capabilities of the requesting entity. In both exclusions, while there may facially be a demand that would otherwise meet the definition of ransomware attack, the demand is made without expectation or desire to actually receive a ransom payment from the covered entity. Similar to the parallel "good faith" exclusion in the definition of substantial cyber incident (as discussed in Section IV.A.ii.3.d.ii of this document), because the exception only applies to instances where the demand for ransom payment was made "in response to a specific request by" the information system owner or operator, this exception would only apply to situations where the request or authorization preceded the demand for ransom payment.

It is noteworthy that, though the definition of a ransomware attack specifically addresses cyber incidents involving interruption or disruption of operations and threats to

do the same, it does not include other forms of extortionate cyber incidents that are similar to ransomware attacks; specifically, extortionate demands for payment based on threats to leak sensitive information obtained without authorization from an information system. While such incidents (without more) do not fall within the definition of a ransomware attack, they would still be reportable under CIRCIA, if the incident otherwise qualifies as a covered cyber incident, as proposed to be defined in § 226.1, e.g., if the underlying incident (including any actual disclosure in line with those threats) leads to the substantial loss of confidentiality of an information system or network.

12. State, Local, Tribal, or Territorial Government Entity

CISA is proposing to include a definition for the term State, Local, Tribal, or Territorial Government entity. This term has significance in the regulation for two primary reasons. First, the term is used within the proposed definition of covered entity to describe certain entities that would be subject to CIRCIA's reporting requirements. Second, pursuant to 6 U.S.C. 681d(f), the section of CIRCIA on noncompliance with required reporting does not apply to a SLTT Government entity.

The U.S. Census Bureau defines a government entity as "an organized entity which, in addition to having governmental character, has sufficient discretion in the management of its own affairs to distinguish it as separate from the administrative structure of any other governmental unit."[157] The Homeland Security Act definition for the term "State" includes both States and territories, defining the term "State" to mean "any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." 6 U.S.C 101(17). The Homeland Security Act definition for the term "Local Government" includes both local

[157] U.S. Bureau of the Census, *Classification Manual* (Oct. 2006), available at https://www.census.gov/programs-surveys/gov-finances/technical-documentation/classification-manuals.html.

and tribal government entities, defining the term "Local Government" to mean "(a) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a Local government; (b) An Indian tribe or authorized tribal organization, or in Alaska, a Native village or Alaska Regional Native Corporation; and (c) A rural community, unincorporated town or village, or other public entity." 6 U.S.C 101(13).

To create its proposed definition for the term SLTT Government entity, CISA is proposing to create an umbrella term that merges the three definitions referenced in the previous paragraph, and include the definition of Indian tribe that is referenced in the Homeland Security Act. This approach will allow CISA to leverage existing, accepted definitions for each element that composes the term SLTT Government entity—i.e., State, local, territorial, tribal, and government entity—within a single, consolidated definition. CISA believes this is also appropriate because SLTT Government Entities are treated the same throughout the proposed regulation, and this umbrella term simplifies this task.

13. Supply Chain Compromise

CISA is proposing to include a definition for the term supply chain compromise. This term has significance in the regulation as CIRCIA explicitly states that unauthorized access facilitated through or caused by a supply chain compromise can be a substantial cyber incident. See 6 U.S.C. 681b(c)(2)(A)(iii).

Section 650 of title 6, United States Code defines "supply chain compromise" as "an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and

can occur at any point during the life cycle." 6 U.S.C. 650(28). NIST defines a "supply chain" as the "linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle."[158] The supply chain for an information system is typically considered to be the multiple layers of software and hardware that are integrated to perform the various functions of the information system. Examples of items in the supply chain of an information system, which are acquired often from multiple vendors, include hardware items like microchips (and the components that comprise the microchips), operating systems (and the code libraries that comprise the operating systems), and other types of software (and the code libraries that compromise the software). information systems—including both ICT and OT—"rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem that . . . consists of multiple levels of outsourcing. This ecosystem is comprised of public and private sector entities (e.g., acquirers, suppliers, developers, system integrators, external service providers, and other ICT/OT-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage ICT/OT products and services."[159]

CISA is proposing to use the definition of the term supply chain compromise contained in 6 U.S.C. 650 verbatim for the definition of the term in the regulation with one exception: the definition in the proposed regulation replaces the term "incident" with the term "cyber incident." As noted in the earlier discussion on the term cyber incident, Congress narrowed the types of incidents CISA could require reporting on under CIRCIA by explicitly stating the term cyber incident did not include an incident that imminently

---

[158] NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication 800-161 Rev.1, at 1 (May 2022), available at https://csrc.nist.gov/pubs/sp/800/161/r1/final.
[159] See *id.*

jeopardizes, but does not actually jeopardize, an information system or the information contained therein. As the use of the term supply chain compromise in the regulation is limited to the definition of certain substantial cyber incidents, the actual (versus imminent) jeopardy requirement is built into the broader requirements already, thus making the end result the same regardless of whether the definition of supply chain compromise uses the term incident or cyber incident. Rather than introducing potential confusion into the regulation by defining incident and cyber incident, CISA is proposing to use the term cyber incident in the definition of supply chain compromise.

As noted in the definition, a supply chain compromise can occur anywhere in the lifecycle of an information system. This can include design, development and production, distribution, acquisition and deployment, maintenance, or disposal.[160] For example, a supply chain compromise can occur when a cyber threat actor infiltrates a software vendor's network and deploys malicious code to compromise the software before the vendor sends it to their customers, which then compromises the customer's data or systems.[161] Newly acquired software or hardware may be compromised from the outset, or a compromise may occur through other means like a patch or a hotfix.[162] Common techniques for software supply chain compromises include hijacking updates, undermining code signing, and compromising open source code.[163]

14. Virtual Currency

CISA is proposing to include a definition for the term virtual currency. CISA is proposing to define this term because CIRCIA requires covered entities to include in any Ransom Payment Report "the type of virtual currency or other commodity requested" as

---

[160] CISA, *Defending Against Software Supply Chain Attacks* at 3, available at https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks-0 (Apr. 2021).
[161] *Id.* at 2.
[162] See *id.*
[163] *Id.* at 4.

part of the ransom demand. 6 U.S.C. 681b(c)(5)(G). CISA wants to ensure that covered entities understand this requirement.

CIRCIA defines virtual currency as "the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value." 6 U.S.C. 681(10). CISA understands this definition as equivalent to a "value that substitutes for currency or funds" in 31 U.S.C. 5312(a)(2)(J), and "virtual currency" as defined in guidance from the Financial Crimes Enforcement Network (FinCEN).[164] Therefore, CISA is proposing to clarify the relationship between these terms by adding a sentence to the definition in CIRCIA noting that virtual currency includes any form of value that substitutes for currency or funds.

v. Request for Comments on Proposed Definitions

CISA seeks comments on all the proposed definitions. In addition, CISA seeks specific comments on the following questions:

3. The proposed definitions of cyber incident, covered cyber incident, and substantial cyber incident, to include the appropriateness and clarity of the thresholds contained in the proposed definition of substantial cyber incident, the three exclusions to the proposed definition of substantial cyber incident, and the guiding principles described in Section IV.A.ii.b of this document regarding how to determine if an incident was a substantial cyber incident.
4. Whether CISA should specifically add the term "significant," "substantial," or any other appropriate word at the beginning of subparagraph 3 of the definition of substantial cyber incident to clarify the impact level required.

---

[164] FinCEN Guidance, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* at 7 (May 9, 2019), available at https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

5. The proposed examples of incidents that likely would or would not qualify as a substantial cyber incident, to include whether the examples provided by CISA are accurate and whether there are other types of incidents that it would be useful to include in the list of examples to incidents that likely would or would not qualify as a substantial cyber incident.
6. Anticipated challenges for covered entities related to understanding or reporting a covered cyber incident if such incident stemmed from a disruption of a third-party vendor or service provider that is itself not a covered entity.
7. As noted in the preamble, CISA believes there is value in CISA receiving reports on all types of cyber incidents that meet the substantial cyber incident impact thresholds, regardless of whether the TTPs used are sophisticated or not, or novel or not. Therefore, CISA proposes that the "sophistication or novelty of the tactics" should not influence whether an individual incident or category of incidents qualifies as a substantial cyber incident. Do you agree with this proposal, or should the sophistication or novelty of a tactic influence whether an individual incident or category of incidents meets one of the substantial cyber incident thresholds? Similarly, should CISA use sophistication or novelty of a tactic as a justification for including or excluding any specific categories of incidents from the population of cyber incidents required to be reported? How does this intersect with the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A)?
8. Should exploitation of a zero-day vulnerability as a general matter be considered to meet one of the threshold impacts in the definition of substantial cyber incident? Please provide data or information specifically regarding (1) whether exploitation of a zero-day vulnerability provides an indication of a malicious actor's sophistication, (2) whether exploitation of a zero-day vulnerability results in a different level of risk to a victim entity than exploitation of a known

vulnerability, and (3) benefits that reporting on the exploitation of zero-day vulnerabilities might provide to CISA's understanding of the cyber threat landscape, CISA's ability to warn entities about emerging threats, and the federal government's awareness of victim entities targeted in cyber incidents utilizing zero-day vulnerabilities.

9. Whether there are any terms for which CISA did not propose a definition but should consider including to improve the clarity of the regulation.

B. Applicability

As noted in Section IV.A.i. above, due to the operative significance and impact of the term, CISA proposes to define covered entity to mean any entity that meets the criteria established in the Applicability Section, § 226.2. CISA believes that § 226.2 also satisfies the statutory requirement that CISA include in the final rule a "clear description of the types of entities that constitute covered entities." See 6 U.S.C. 681b(c)(1).

The proposed Applicability section includes two primary means by which an entity in a critical infrastructure sector qualifies as a covered entity, the first based on the size of the entity and the second based on whether the entity meets any of the enumerated sector-based criteria. An entity in a critical infrastructure sector only needs to meet one of the criteria to be considered a covered entity. For example, an entity in a critical infrastructure sector that exceeds the size standard and meets none of the § 226.2(b) sector-based criteria will be considered a covered entity. Conversely, an entity that meets one or more of the sector-based criteria will be a covered entity regardless of whether it exceeds the § 226.2(a) size standard. An entity in a critical infrastructure sector does not have to meet both the size-based criterion and one of the sector-based criteria to be considered a covered entity.

i. Interpreting the CIRCIA Statutory Definition of Covered Entity

In developing this proposed Applicability section, CISA first looked at the parameters imposed by CIRCIA. See 6 U.S.C. 681(4). Specifically, in the definition of covered entity provided by CIRCIA, Congress limits what may be a covered entity to "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21." See 6 U.S.C. 681(4).

PPD-21 does not define the word "entity" but instead adopts a systems and assets approach when referring to critical infrastructure. However, this does not fit within the regulatory scheme required by CIRCIA. Therefore, CISA interprets the word "entity" to be a broad term, generally including any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government) regardless of governance model that has legal standing and is uniquely identifiable from other entities.[165] The organizational structure or nomenclature chosen by the entity does not matter as long as it is a structure that imports legal presence or standing in the United States. CISA does not, therefore, interpret or understand the word "entity" to mean a system or asset, and some of the things that would not be considered entities include software, hardware, and other equipment; buildings and facilities; and systems. CISA believes this interpretation is both consistent with the plain language meaning of the term "entity" and appropriate given the purposes of CIRCIA, which require CISA to collect sufficient reports to develop analysis and understand cyber threat trends across the entire critical infrastructure landscape.

The second limitation contained in the statutory definition is that the entity must be "in a critical infrastructure sector, as defined in Presidential Policy Directive 21."

---

[165] Black's Law Dictionary defines "entity" as "[a] generic term inclusive of person, partnership, organization, or business [that] can be legally bound [and] is uniquely identifiable from any other entity." See Black's Law Dictionary, 2nd Ed., as found on www.thelawdictionary.org. Black's also contains a separate definition for "legal entity," defining it as "[a] lawful or legally standing association, corporation, partnership, proprietorship, trust, or individual [that h]as legal capacity to (1) enter into agreements or contracts, (2) assume obligations, (3) incur and pay debts, (4) sue and be sued in its own right, and (5) to be accountable for illegal activities." *Id.*

Presidential Policy Directive 21 (PPD-21) does not actually contain a definition for "critical infrastructure sector," but it does specifically enumerate 16 critical infrastructure sectors.[166] PPD-21 also does not specifically define the composition of the individual critical infrastructure sectors; however, PPD-21 required the Secretary of Homeland Security to update the National Infrastructure Protection Plan (NIPP), which is intended to guide the national effort to manage risks to the Nation's critical infrastructure. The NIPP included a "Call to Action" which required each critical infrastructure sector to update its Sector-Specific Plan (SSP) as part of an overall joint planning effort and to update the SSP every four years thereafter.[167] The SSPs are developed jointly by representatives of the private sector, referred to as Sector Coordinating Councils (SCCs),[168] and representatives of the government, referred to as Government Coordinating Councils (GCCs).[169] Each SSP[170] includes a "sector profile," which describes entities that are in the respective critical infrastructure sector. These profiles do not limit the descriptions of the entities that comprise each critical infrastructure sector identified in PPD-21 to entities that own systems and assets that meet the statutory

---

[166] The 16 critical infrastructure sectors enumerated in PPD-21 are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

[167] The NIPP states that SSPs are supposed to be updated every four years, but to date, none of these plans have been updated. See *National Infrastructure Protection Plan* (2013), available at https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan.

[168] The SCCs are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SCCs coordinate and collaborate with SRMAs and related Government Coordinating Councils to address the entire range of critical infrastructure security and resilience policies and efforts for that sector. See https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils (last visited Nov. 28, 2023).

[169] GCCs are formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCCs are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector. See https://www.cisa.gov/resources-tools/groups/government-coordinating-councils (last visited Nov. 28, 2023).

[170] CISA's website has a webpage for each critical infrastructure sector, each of which includes a link to the sector's respective SSP. These webpages are available at https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Nov. 28, 2023). The current versions of the SSPs are also collectively located at https://www.cisa.gov/2015-sector-specific-plans (last visited Nov. 28, 2023).

definition of "critical infrastructure" set forth by 42 U.S.C. 5195c(e).[171] Rather, in implementing PPD-21, the SSPs make clear that a wide variety of entities, including at least some entities that do not own or operate systems or assets that meet the definition of critical infrastructure in PPD-21 but are active participants in critical infrastructure sectors and communities, are considered "in a critical infrastructure sector."

For example, according to the 2015 Food and Agriculture SSP, among the variety of entities that composed the Food and Agriculture Sector in 2014 were more than 935,000 restaurants and institutional food service establishments; an estimated 114,000 supermarkets, grocery stores, and other food outlets; over 81,000 domestic food facilities (e.g., warehouses; manufacturers; processors); and roughly 2.1 million farms.[172] Similarly, according to the 2015 Healthcare and Public Health SSP, the array of entities that composed the Healthcare and Public Health Sector included entities that provide direct patient care (e.g., hospitals, urgent care clinics, doctor and dentist offices); medical research institutions; medical record system vendors; health insurance companies; local and State health departments; cemeteries, crematoriums, morgues, and funeral homes; pharmaceutical and other medical supply manufacturers and distributors; medical laboratories; drug store chains; and blood banks.[173] As a third example, the 2015 Commercial Facilities SSP defines the Commercial Facilities Sector to include a mix of entities, such as the nation's 1.1 million malls, shopping centers, and other retail establishments; over 52,000 hotel-based properties; nearly 1,400 casinos and associated resorts; 1 million office buildings; 5.6 million multi-family rental buildings, and nearly

---

[171] PPD-21 defines "critical infrastructure" as "having the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[172] DHS, *Food and Agriculture SSP* at 3 (2015), available at https://www.cisa.gov/publication/nipp-ssp-food-ag-2015.

[173] DHS, *Healthcare and Public Health SSP* at 5 (May 2016), available at https://www.cisa.gov/resources-tools/resources/healthcare-and-public-health-sector-specific-plan-2015 (hereinafter "*Healthcare and Public Health SSP*").

125,000 establishments designed for public assembly, such as stadiums, arenas, movie theaters, museums, zoos, libraries, and other performance venues.[174] CISA considered the variety of entities described in the sector profiles in the SSPs when determining the scope of the Applicability section.

CISA has determined it is appropriate to define entities within a critical infrastructure sector consistently with SSP sector profiles that were developed through a collaborative public-private partnership, as these sector profiles reflect a mutual understanding of what types of entities are in a critical infrastructure sector. This interpretation was supported by many commenters whose comments reflected the breadth of entities that are within a critical infrastructure sector.[175] Accordingly, CISA proposes to include an equivalently wide variety of types of entities within the scope of the CIRCIA regulatory description of "covered entity" to reflect the same diversity of entities that are in a critical infrastructure sector within the context of PPD-21, the NIPP, and each sector's SSP. This is also why CISA is not proposing to limit the scope of the Applicability section to owners and operators of critical infrastructure.

A number of commenters have recommended that CISA limit the definition of covered entity to critical infrastructure or a subset thereof. CISA believes that interpretation is neither consistent with the authorization granted to CISA by Congress in CIRCIA, nor would it enable CISA to achieve the intended purposes of the regulation. To the first point, a plain language reading of CIRCIA's statutory definition of covered entity indicates that CISA has the authority to include within the scope of the regulation

---

[174] DHS, *Commercial Facilities SSP: An Annex to the NIPP 2013*, at 3 (2015), available at https://www.cisa.gov/publication/nipp-ssp-commercial-facilities-2015.

[175] See, e.g., Comments submitted by the National Retail Federation, CISA-2022-0010-0092-0001 (stating that food and beverage retailers and restaurants fall within the definitions of the Commercial Facilities Sector and/or the Food and Agriculture Sector); National Electrical Manufacturers Association, CISA-2022-0010-0026-0001 (noting in an example that shopping malls are part of the Commercial Facilities Sector); Rural Wireless Association, CISA-2022-0010-0093-0001 (acknowledging the entire communications sector may be included in the covered entity definition"); Center for Democracy and Technology, CISA-2022-0010-0068-0001 (citing the NIPP and Education Facilities SSP to show that all K-12 schools could be included as covered entities).

more than just entities that own or operate critical infrastructure. As demonstrated by the broad sector profiles in SSPs described above, CISA views the language used by Congress in CIRCIA bounding the scope of who could be a covered entity as simply "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21" as representative of a much broader set of entities than just owners and operators of critical infrastructure. Had Congress wanted to limit CISA's regulatory authority to critical infrastructure owners and operators, it could have easily done so, as PPD-21 includes a definition for the term "critical infrastructure" itself that could have been used for this purpose.[176]

More importantly, such a narrowing scope of the term covered entity would severely hinder CISA's ability to achieve CIRCIA's regulatory purposes. As discussed earlier, CISA identified a number of purposes that the regulation is designed to facilitate. See Section III.C.i. Many of these purposes require a sufficient amount of data to achieve. These purposes include the identification of commonly exploited vulnerabilities and effective countermeasures; trend analysis and threat tracking, both generally and in relation to specific sectors, industries, or geographic regions; and the issuance of cybersecurity alerts and early warnings. See Section III.C.ii. Reporting from a broad range of entities is necessary to provide adequate visibility of the cyber landscape across critical infrastructure sectors, which CIRCIA is meant to facilitate. 6 U.S.C. 681a(a)(1). Furthermore, the products and analysis CISA is able to produce in support of these goals are likely to significantly improve in quality in proportion with increases in the amount of data available to CISA to support its analytical activities.

To receive a sufficient number of reports to achieve these regulatory goals, CISA believes a broad interpretation of the term covered entity is essential. See Section III.C.ii.

---

[176] See PPD-21, "Definitions" at 12, available at https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and.

This is particularly necessary in light of the limitations Congress imposed on the term covered cyber incident which defines the types of incidents that must be reported under the proposed rule. As discussed later in this document, CISA interprets the Congressional language related to substantial cyber incident and, by proxy, the definition of covered cyber incident, to limit the types of incidents for which CISA can mandate reporting. As the number of CIRCIA Reports CISA will receive is a function of both whether an entity meets the description of a covered entity and whether the incident experienced meets the definition of covered cyber incident, narrowly interpreting both would severely restrict the number of incidents about which CISA receives information. Because CISA's discretion to define a covered cyber incident is more limited by CIRCIA itself, CISA believes it is important to scope covered entity, where it has greater discretion under CIRCIA, more broadly.

CISA is not, however, proposing to scope the term covered entity so broadly as to include virtually every entity within one of the critical infrastructure sectors within the description of covered entity. CISA believes that this is just the starting threshold at which Congress intended that CISA consider describing the contours of entities that should be included as covered entities. Rather, CISA's proposed Applicability section is designed to focus the reporting requirements primarily on entities that own or operate systems or assets considered critical infrastructure under the PPD-21 definition, while still requiring reporting from a small subset of entities that might not own or operate critical infrastructure but that could impact critical infrastructure to help ensure CISA receives an adequate number of reports overall, including reports of substantial cyber incidents from entities that are most likely to own or operate critical infrastructure. To achieve this, CISA is proposing a description for covered entity that would capture both entities of a sufficient size (based on number of employees or annual revenue) as well as smaller entities that meet specific sector-based criteria.

ii. Determining if an Entity is in a Critical Infrastructure Sector

As a threshold matter, to be a covered entity, an entity must be "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21." 6 U.S.C. 681. As noted above, PPD-21 does not actually include a definition for "critical infrastructure sector," but rather provides a list of the sixteen critical infrastructure sectors and directed updates to the NIPP and the public-private partnership model (i.e., SSPs).[177]

CISA anticipates that the process for an entity to determine if it is within a critical infrastructure sector will usually be a relatively straightforward exercise. CISA has strong public-private partnerships with the critical infrastructure community, and will be leveraging these relationships as part of the outreach and education campaign that is required by CIRCIA to inform entities that are likely covered entities of the regulatory reporting requirements associated with this proposed rule.[178] CISA expects that entities will be able to obtain informational materials as part of this outreach and education campaign that will simplify the process of determining whether an entity is a covered entity. However, CISA has attempted to propose a population of entities in a critical infrastructure sector that would typically expect themselves to be included in a critical infrastructure sector, which will enable an entity to easily self-identify whether or not it is a covered entity. For example, entities engaged in or facilitating transportation, such as airplane or car manufacturers, airport and train station operators, and trucking companies, can readily self-identify as in the Transportation Services Sector. Similarly, entities engaged in the production, storage, and distribution of food, such as farms, food packagers and distributers, and grocery stores can readily self-identify as in the Food and

---

[177] *Id.* at 10-11.

[178] See 6 U.S.C. 681b(e)(1); see also CISA's Critical Infrastructure Partnership Advisory Council (CIPAC) website describing CISA's partnership and forum with the critical infrastructure community at https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac (last visited Nov. 28, 2023).

Agriculture Sector. Banks, credit unions, credit card companies, registered broker-dealers, and other entities providing financial services can similarly self-identify as in the Financial Services Sector, while drinking water and wastewater treatment facilities can also readily identify as in the Water and Wastewater Systems Sector. Moreover, many of these same entities are members of the SCC for their respective critical infrastructure sectors and on this basis would be able to accurately self-identify which critical infrastructure sector(s) they would fall within.[179]

In some cases, however, it may be less obvious to an entity whether it falls into one or more of the critical infrastructure sectors. Examples include mine tailings and navigation locks (Dams Sector); nursing homes and cemeteries (Healthcare and Public Health Sector); and schools and elections infrastructure (Government Facilities Sector). The scope of types of entities that are considered part of a sector are described in the sector profiles in each sector's SSP. As noted above in Section IV.B.i, SSPs are documents developed jointly by each sector's SCC and GCC to help implement PPD-21 and the NIPP. The current versions of SSPs for all 16 sectors can be found on the CISA website at https://www.cisa.gov/2015-sector-specific-plans. The overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors. Illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups.

If an entity is unsure as to whether or not it is part of a critical infrastructure sector, CISA recommends the entity review the SSP for the sector or sectors that most closely align with the line of activities in which the entity is engaged. Once the final rule has issued, entities will also be able to reference informational materials that will be

---

[179] See CISA's Sector Coordinating Councils website for information on SCCs and membership for each sector's SCC at https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils (last visited Nov. 28, 2023).

published as part of CISA's outreach and education campaign. If after taking these steps, an entity still is unsure as to whether it is in a critical infrastructure sector, CISA recommends the entity contact CISA so that CISA can assist the entity in determining if it is in a critical infrastructure sector.

iii. Clear Description of the Types of Entities that Constitute Covered Entities Based on Statutory Factors

Section 681b(c)(1) of title 6, United States Code, requires CISA to include in the final rule "A clear description of the types of entities that constitute covered entities, based on—(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure."

The first part of this requirement is that CISA must provide "[a] clear description of the types of entities that constitute covered entities..." For the reasons described in this section, CISA believes that the criteria contained within the proposed Applicability section are easily understandable and clearly explain the types of entities that constitute covered entities. Accordingly, CISA believes that the Applicability section satisfies CIRCIA's "clear description" requirement.

In developing this clear description of what is a covered entity, 6 U.S.C. 681b(c)(1) requires CISA to base this clear description on the three factors enumerated within that section. CISA understands 6 U.S.C. 681b(c)(1) not as imposing minimum requirements on what may be a covered entity, but rather simply as providing lenses through which CISA is to consider what entities it should seek to include in the

description of covered entity. For example, CISA is to consider "the likelihood" an entity will be targeted, but 6 U.S.C. 681b(c)(1) does not require that entities be included in the description of covered entity only if they have a "high likelihood" or "very high likelihood" of being targeted.

Further, while 6 U.S.C. 681b(c)(1) uses the word "and," CISA does not interpret 6 U.S.C. 681b(c)(1) as requiring that all three factors be relevant to each entity or category of entities included in the description of covered entity; rather, CISA reads the "and" as indicating that CISA must consider, as part of its process of determining the description of covered entity, all three factors. For example, an entity could be considered a covered entity if it maintains sensitive intellectual property, the compromise of which could cause significant national security or economic security consequences (factor A), even if unauthorized access to that information would not likely enable the disruption of reliable operation of critical infrastructure (factor C).

This interpretation is also consistent with the specifics of the 6 U.S.C. 681b(c)(1) factors themselves, which, collectively, address different aspects of risk. "Risk" is generally understood to be a measure of the extent to which an entity is threatened by a potential circumstance or event, determined based on a function of (1) the consequences, or adverse impacts, that could arise if the circumstances or event occurs, and (2) the threat or vulnerabilities, or the likelihood of occurrence.[180] In the cybersecurity context specifically, risk is often understood to refer to those consequences and threats or vulnerabilities caused by or resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. See 6 U.S.C. 650(7). This risk "equation" is often summarized as Risk = Consequence x Threat x Vulnerability. Viewed through this framing, CISA interprets the three factors listed in 6

[180] See, e.g., NIST, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (March 2006) at 48, https://doi.org/10.6028/NIST.FIPS.200 (last visited Mar. 12, 2024).

U.S.C. 681b(c)(1) to each represent a different aspect of the risk equation: factor A (the consequence of disruption or compromise) addresses the "consequence" prong of the equation; factor B (the likelihood that such an entity may be targeted) addresses the "threat" prong; and factor C (the extent to which compromise of an entity could enable the disruption of reliable operation of critical infrastructure) speaks, albeit indirectly, to vulnerability, i.e., the extent to which compromise of this entity could increase the vulnerability of critical infrastructure. Read through this lens, CISA understands the 6 U.S.C. 681b(c)(1) factors to be direction to CISA to consider specific aspects of the three prongs of cybersecurity risk—consequence, threat, and vulnerability—in assessing who should be deemed a covered entity. While the risk equation recognizes that an extremely low consequence can balance out a moderate threat to result in a generally low overall risk, a very high threat combined with even a moderate consequence, or a very high consequence combined with a moderately low threat can still lead to a moderate to high cybersecurity risk. With this understanding in mind, CISA interprets these factors not to limit the possible scope of covered entities to those entities that achieve high scores on each prong of the risk equation, but rather to use these factors to consider the various identified aspects of cybersecurity risk in determining which entities in a critical infrastructure sector should be covered entities. Moreover, if CISA were to interpret these three factors as requiring CISA only to deem entities that meet all three as covered entities, this could result in CISA not receiving sufficient reporting across any given critical infrastructure sector to competently fulfill its statutory responsibilities under CIRCIA to aggregate and analyze information. As reflected in the discussion throughout this section, CISA considered all three factors enumerated in 6 U.S.C. 681b(c)(1) as it analyzed how to describe covered entity.

All three factors—i.e., (A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and

safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure—were particularly central to the determination of the sector-based criteria being proposed by CISA to augment the group of entities that would be considered covered entities under the first prong of the criteria contained in the Applicability section based on their size. These factors also drove CISA's proposal to exclude entities in a critical infrastructure sector that fall below the size standards (unless they meet a sector-based criteria) while including entities in a critical infrastructure sector that are larger (even if not otherwise a covered entity based on the sector-based criteria).

While the discussion below is focused largely on the reasons why CISA is proposing to include entities in the description of covered entity based on the extent to which these factors apply in the context of covered cyber incident reporting requirements, the rationale generally holds true for ransom payment reporting requirements as well. CIRCIA provides one term—"covered entity"—to describe the scope of entities subject to both reporting requirements, and, consistent with this framing, CISA is proposing to apply the covered cyber incident reporting requirements and the ransom payment reporting requirements to the same universe of covered entities. This is also consistent with the three statutory factors described above, the current threat landscape related to ransomware attacks, and CISA's responsibilities under CIRCIA. If a covered entity pays a ransom payment, it is likely that it has experienced a ransomware attack from which it has not been able to recover quickly (e.g., through the use of backup systems and data). To the extent a covered cyber incident against a particular entity would justify its inclusion in the description of covered entity due to the factors above (e.g., the

consequences that disruption to or compromise of such an entity could cause), so too would a ransomware attack from which an entity cannot quickly recover, as this would likely involve the very disruption or compromise envisioned by these factors. Further, in light of the rise of ransomware attacks as a proportion of cyber incidents,[181] the rise of ransomware attacks targeting entities in critical infrastructure sectors specifically,[182] and CISA's statutory charge under CIRCIA to "coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments," 6 U.S.C. 681a(a)(2), it is critical that CISA receive a sufficient number of Ransom Payment Reports from a breadth of entities in critical infrastructure sectors.

iv. Explanation of Specific Proposed Applicability Criteria

1. Size-Based Criterion

a. Overview

The first group of entities that CISA is proposing to include as covered entities are entities within a critical infrastructure sector that exceed the U.S. Small Business Administration's (SBA) small business size standard based on either number of employees or annual revenue, depending on the industry. For a number of reasons CISA believes a sensible approach is to require larger entities within a critical infrastructure

---

[181] See, e.g., Verizon, *Data Breach Investigations Report* at 7 (2022) (hereinafter, "*Verizon 2022 DBIR*"), available at https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report.

[182] See, e.g., CISA, FBI, NSA, Australian Cyber Security Centre, and United Kingdom National Cyber Security Centre, *Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat of Ransomware, AA22-040A* (Feb. 9, 2022), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a ("The [FBI], [CISA], and [NSA] observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The United Kingdom's National Cyber Security Centre (NCSC-UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC-UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors."); FBI Internet Crime Complaint Center, *Internet Crime Report* at 14 (2022), available at https://www.ic3.gov/Home/AnnualReports (noting that the Internet Crime Complaint Center received 870 voluntary complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack, including at least 1 member of every critical infrastructure sector except Dams and Nuclear Reactors, Materials, and Waste Sectors).

sector to report cyber incidents while generally excluding smaller entities from those same reporting requirements.

In assessing whether to propose a size-based criterion as a basis for scoping which entities in a critical infrastructure sector should be considered covered entities, CISA took into consideration the three factors described in 6 U.S.C. 681b(c)(1). CISA believes that each of these factors support the inclusion of the very small percentage of businesses in the United States that exceed the small business size standards in the description of "covered entity."

The first factor Congress identified in 6 U.S.C. 681b(c)(1) is the consequences that disruption to or compromise of an entity could cause to national security, economic security, or public health and safety. While size is not alone indicative of criticality, larger entities' larger customer bases, market shares, number of employees, and other similar size-based characteristics mean that cyber incidents affecting them typically have greater potential to result in consequences impacting national security, economic security, or public health and safety than cyber incidents affecting smaller companies. For example, a successful cyber incident affecting a national drug store chain is much likelier to have significant national security, economic security, or public health and safety impacts than a similar incident affecting a "mom-and-pop" drug store. Similarly, there is a substantially higher likelihood of significant impacts resulting from a successful cyber incident affecting a large industrial food conglomerate, a multinational hotel chain, or a large hospital system than one affecting a small independent farm, a single-location bed and breakfast, or a small doctor's office, respectively. Countless other similar examples exist.

At least one other regulator has used the likelihood of greater consequences at larger facilities to justify imposing regulatory requirements based on company size. Specifically, the Food and Drug Administration's Mitigation Strategies to Protect Food

Against Intentional Adulteration regulations at 21 CFR part 121 imposes less stringent regulatory requirements on small and very small businesses, stating that larger, more well-known businesses "are likely to have larger batch sizes, [with attacks on them] potentially resulting in greater human morbidity and mortality. Further, an attack on a well-recognized, trusted brand is likely to result in greater loss of consumer confidence in the food supply and in the government's ability to ensure its safety and, consequently, cause greater economic disruption than a relatively unknown brand that is distributed regionally."[183] By requiring reporting from large entities, CISA is more likely to rapidly be informed about incidents impacting the largest number of people and creating the most significant national security, economic security, or public health and safety impacts.

The second factor Congress identified in 6 U.S.C. 681b(c)(1) for CISA to consider as part of scoping the description of covered entity is the likelihood that an entity may be targeted by a malicious cyber actor. Recent studies show that large entities disproportionately experience cyber incidents. Per the 2022 Verizon DBIR, from November 2021 through October 2022, entities with more than 1,000 employees experienced 23.5%, of the cyber security incidents analyzed by Verizon for which the size of the organization was known,[184] despite entities with more than 1,000 employees accounting for less than 1% of U.S. businesses.[185] That percentage actually increased the following year, with the 2023 Verizon DBIR stating that entities with more than 1,000 employees experienced 41% of the cybersecurity incidents analyzed by Verizon for which the size of the organization was known during the relevant timeframe.[186] This is

---

[183] 78 FR 78033 (Dec. 24, 2013).
[184] *Verizon 2022 DBIR*, *supra* note 181, at 50 (for the 2,701 incidents analyzed by Verizon that occurred between November 1, 2021 and October 31, 2022 and for which Verizon knew the impacted organization's size, 636 had more than 1,000 employees).
[185] According to the U.S. Census Bureau, in 2021, only 8,365 out of 8,148,606 (or .1%) of companies with one or more employees had 1,000 or more employees. See U.S. Census Bureau, 2021 County Business Patterns, available at https://www.census.gov/programs-surveys/cbp/data.html.
[186] Verizon, *Data Breach Investigations Report* at 50 (2023) (for the 1,183 incidents analyzed by Verizon that occurred between November 1, 2021 and October 31, 2022 and for which Verizon knew the impacted

consistent with the belief that terrorist organizations and other bad actors frequently target larger, more well-known entities.[187] The desire to target large entities has been noted specifically in regards to cyber incidents as well. For instance, per the 2024 Homeland Security Threat Assessment, based on trends from the first half of the year, the year 2023 was expected to be the second most profitable year ever for ransomware attackers due in part to "big game hunting," i.e., the targeting of large organizations.[188]

The third and final factor Congress identified in 6 U.S.C. 681b(c)(1) for CISA to consider as part of scoping the description of covered entity is the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure. The majority of critical infrastructure is owned and operated by the private sector.[189] Although the percentage of critical infrastructure owned and operated by larger entities versus small businesses is unknown, given that the less than 1% of businesses in America that are not considered small businesses account for 56% of the United States' gross domestic product and employ nearly 54% of all private sector employees,[190] these entities are likely to own or

---

organization's size, 489 had more than 1,000 employees) (hereinafter, "*Verizon 2023 DBIR*"), available at https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/.

[187] See, e.g., *Focused Mitigation Strategies To Protect Food Against Intentional Adulteration*, 78 FR 78014, 78033 (Dec. 24, 2013) ("It is our assessment that [a desire to maximize public health harm and, to a lesser extent, economic disruption] are likely to drive terrorist organizations to target the product of relatively large facilities, especially those for which the brand is nationally or internationally recognizable. An attack on such a target would potentially provide the widescale consequences desired by a terrorist organization and the significant public attention that would accompany an attack on a recognizable brand.").

[188] Department of Homeland Security, *2024 Homeland Security Threat Assessment* at 26 ("Ransomware attackers extorted at least $449.1 million globally during the first half of 2023 and are expected to have their second most profitable year. This is due to the return of 'big game hunting'—the targeting of large organizations—as well as cyber criminals' continued attacks against smaller organizations."), available at https://www.dhs.gov/publication/homeland-threat-assessment (hereinafter, "*2024 Homeland Security Threat Assessment*"); see also Dimitry Dontov, *What Businesses are the Most Vulnerable to Cyberattacks*, Forbes.com (Jan. 19, 2021) ("[M]ature hacking groups like Evil Corp are going after large businesses, including Fortune 500 companies. Cybercriminals have their sights set on 'big fish' in various industries, as seen with attacks on Garmin, Blackbaud, Magellan Health and others."), available at https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=331f38bf3534.

[189] See, e.g., U.S. Government Accountability Office (GAO), *GAO-22-104279: CRITICAL INFRASTRUCTURE PROTECTION: CISA Should Improve Priority Setting, Stakeholder Involvement, and threat Information Sharing* at 1 (Mar. 2022) ("The majority of critical infrastructure is owned and operated by the private sector."), available at https://www.gao.gov/products/gao-22-104279.

operate a disproportionate percentage of the nation's critical infrastructure. Moreover, in light of the interconnectedness of the world today, incidents at entities in critical infrastructure sectors that are not themselves owners and operators of critical infrastructure can have cascading effects that end up impacting critical infrastructure. Based on this, CISA believes that substantial cyber incidents (which, as described below, are the types of incidents that covered entities are required to report) at larger entities routinely will have a high likelihood of disrupting the reliable operation of critical infrastructure.

In addition to the rationales provided based on CISA's consideration of the 6 U.S.C. 681b(c)(1) factors, CISA believes there are additional reasons justifying the proposed sized-based criteria to scope covered entity. For instance, larger entities also are likely to have more mature cybersecurity capabilities or be better situated to bring in outside experts to assist during an incident.[191] These capabilities make larger entities more likely to identify early signs of compromise than smaller entities. By including large entities in the description of covered entity, the likelihood that an incident is noticed and reported is increased, while the timeframe between initiation of an incident and its reporting is likely to be decreased.

For similar reasons, CISA believes larger entities also frequently will be better situated to simultaneously report and respond to or mitigate an incident, which is a situation many, if not most, reporting entities will be faced with given the statutorily mandated 72-hour reporting requirement for Covered Cyber Incident Reports and 24-

---

[190] U.S. Small Business Administration Office of Advocacy, *Frequently Asked Questions* (Mar. 2023), available at https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/ (last visited Nov. 28, 2023).

[191] *Verizon 2023 DBIR*, *supra* note 186, at 65 ("In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.").

hour reporting requirement for Ransom Payment Reports. Finally, larger entities generally will be better situated to absorb costs associated with reporting, even if per-report costs are relatively minimal, which CISA believes they will be. Given this, to the extent that CISA is offering regulatory relief to a portion of the community that Congress included in the statutory definition of covered entity (the regulatory relief being not including certain entities as covered entities in the proposed Applicability section in § 226.2), CISA believes that relief should be provided to smaller businesses that may be less capable of absorbing costs associated with incident reporting to the extent they do not fit within the sector-based criteria described below. Such an approach is also consistent with the goals of the Small Business Regulatory Enforcement Fairness Act, which Congress enacted in large part to ensure departments and agencies explore options for reducing any significant economic impact on small businesses that, based on their more limited resources, may have greater difficulty understanding and complying with regulations.[192]

CISA believes that this proposed approach has ancillary benefits as well. First, employee- and revenue-based criteria have a long history of use for other purposes, including regulatory purposes.[193] CISA additionally believes that most entities should be able to relatively easily determine if they meet the size-based requirements for inclusion as a covered entity. The desire for definitional clarity was a common refrain raised by stakeholders during CIRCIA listening sessions and in comments submitted in response to the RFI. CISA believes this aspect of the Applicability Section (as well as the Applicability section as a whole) achieves that clarity. Second, while CISA believes the costs incurred by an individual entity associated with reporting an incident under the

[192] See 5 U.S.C. 601 et seq.

[193] See, e.g., 7 CFR 205.236(d)(1) (provides certain exceptions to small businesses as determined by 13 CFR part 121 for requirements applicable to foods labeled as organic); 40 CFR 86.1801-12(j) (exempts small businesses meeting the SBA size standards from certain vehicle greenhouse gas emission standards); 40 CFR part 1033 (provides different locomotive emissions standards for "small railroads" which, among other things, must meet the SBA size standards to qualify).

proposed regulation are relatively low, by removing small businesses from the description of covered entity unless they meet a specific sector-based reason for inclusion, CISA will significantly lower the aggregated costs associated with this regulatory program.

In response to the CIRCIA RFI, several commenters advocated for CISA to use a size-based threshold that would allow CISA to broadly capture entities above a certain size. Multiple commenters recommended the definition of covered entity include all entities with 50 or more employees,[194] with some also recommending it include entities with more than 1,000 customers or $5 million in revenue.[195] One commenter suggested exempting from coverage entities that meet the SBA definition of a small business for certain North American Industry Classification System (NAICS) codes.[196]

Contrarily, a number of stakeholders recommended against using a size threshold for identifying covered entities because the size of an entity does not necessarily equate to criticality.[197] These stakeholders argued that using a size threshold would: (a) cause CISA to miss reports from entities that own, or provide products or services to, critical infrastructure that fell below the chosen threshold; and (b) require reporting of incidents from entities that do not own or operate systems or assets that are critical infrastructure, which a number of the commenters asserted is not in line with the purposes of the

---

[194] See e.g., Comments submitted by the Computing Technology Industry Association, CISA-2022-0010-0122, Cyber Threat Alliance, CISA-2022-0010-0019, and SolarWinds, CISA-2022-0010-0027.
[195] See Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; SolarWinds, CISA-2022-0010-0027.
[196] See Comment submitted by the National Grain and Feed Association, CISA-2022-0010-0104.
[197] See, e.g., Comments submitted by the Information Technology-ISAC, CISA-2022-0010-0048 ("Focusing on the incident's impact on critical infrastructure might also provide a path to defining the term 'covered entity.' For example, if the goal of the program is to manage risks and disruptions to critical infrastructure, CISA could define "covered entities" based on the products or services companies provide to critical infrastructure. In this way, a covered entity is not determined by its size, but by the criticality of the products or services it provides to other critical infrastructure."); (ISC)2, CISA-2022-0010-0112 ("Each of the 16 critical infrastructure sectors has varying risk profiles which should be considered when considering this definition. We suggest basing the definition on the nature of those services and the effect it could have on customers instead of employees and revenue."); NCTA – The Internet & Television Association, CISA-2022-0010-0102 ("Covered entity eligibility criteria that are size- and sector-neutral are critical because the online ecosystem consists of a broad range of interdependent entities, including communications networks, cloud services, CDN providers, software and security vendors, and e-commerce platforms and applications.").

regulation. While CISA agrees with commenters that the size of an entity does not necessarily equate to that entity's criticality, it does not believe the two outcomes the commenters suggest will occur or have the negative impact suggested based on how CISA has proposed to scope the description of covered entity.

Regarding the first concern, that using a size-based standard would cause CISA to miss reports from critical infrastructure entities that fall below the size standard, CISA would agree with this if a size-based standard was the only way in which an entity could become a covered entity. To address this concern and ensure that most entities that own or operate critical infrastructure are included within the covered entity description regardless of size, CISA has included additional sector-based criteria in the Applicability section which, if met by an entity in a critical infrastructure sector, would make that entity a covered entity, even if the entity's size is below the applicable size standard. Many of the sector-based criteria are specifically designed to target entities that own or operate critical infrastructure, and these criteria are independent of the size standard for determining applicability of the proposed regulations. In other words, an entity in a critical infrastructure sector is a covered entity if it meets any of the criteria included in the Applicability section, be it the size-based standard or one of the sector-based criteria. As noted earlier, an entity in a critical infrastructure sector does not have to meet both the size-based standard and one of the sector-based criteria for inclusion as a covered entity.

As to the second concern, that size-based thresholds will result in reporting of incidents from entities that do not own or operate systems or assets that constitute critical infrastructure and that those reports would not advance the purposes of the regulation, CISA agrees with the first part of the comment, but not the latter. CISA agrees that size is not always indicative of criticality, and thus, including all entities of a certain size that are within a critical infrastructure sector as covered entities will result in CISA receiving some reporting from entities that are in critical infrastructure sectors, but do not own or

operate systems or assets that constitute critical infrastructure. CISA, however, disagrees that CISA requiring reporting from those entities that do not own or operate critical infrastructure would not support the purposes of this regulation. Incidents that occur at entities in critical infrastructure sectors reveal valuable information on TTPs and trends that can be used to help better protect other entities in those specific sectors and others, regardless of whether the reporting entities own or operate systems or assets that constitute critical infrastructure. If CISA were to require reporting on only significant incidents from entities that own or operate critical infrastructure, CISA's ability to identify adversary trends and campaigns, identify vulnerabilities that are being exploited, and issue early warnings would be significantly more limited. It is much more in line with the purpose of the regulation for CISA to learn about new or novel vulnerabilities, trends, or tactics sooner and be able to share early warnings before additional entities within a critical infrastructure sector, whether or not they own or operate critical infrastructure, can fall victim to them.

Additionally, in light of the interconnectedness of the world today, incidents at entities in a critical infrastructure sector, even if that the entity does not own or operate critical infrastructure, can have unexpected, cascading effects that end up impacting critical infrastructure.[198] Requiring reporting from entities in critical infrastructure sectors, whether or not they own or operate systems or assets that are critical infrastructure, can enable response and mitigation activities that may help prevent incidents from causing cascading impacts to critical infrastructure or hamper the delivery of NCFs.

b. Proposed Size-Based Criterion

[198] See, e.g., CISA, *A Guide to Critical Infrastructure Security and Resilience* at 6 (Nov. 2019) ("Connections and interdependencies between infrastructure elements and sectors means that damage, disruption, or destruction to one infrastructure element can cause cascading effects, impacting continued operation of another."), available at https://www.cisa.gov/resources-tools/resources/guide-critical-infrastructure-security-and-resilience (hereinafter "*Guide to Critical Infrastructure Security and Resilience*").

CISA is proposing that the description of covered entity include any entity in a critical infrastructure sector that exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the SBA Size Standards, which are codified in 13 CFR part 121. These standards "define whether a business is small and, thus, eligible for Government programs and preferences reserved for 'small business' concerns."[199] While designed in large part for determining eligibility to participate in certain Federal government contracts, procurements, grants, and other similar purposes, the Small Business Size Regulations indicate that the SBA Size Standards are for general use by Federal departments and agencies promulgating regulations that include size criteria.[200] If a Federal department or agency wants to use different size criteria, it is required to consult with the SBA in writing during the rulemaking process and explain why the SBA's existing size standards would not satisfy program requirements.[201]

SBA Size Standards vary by industry (as designated by NAICS[202] code) and are generally based on the number of employees or the amount of annual receipts (i.e., annual revenue) the business has. SBA reviews and updates the Size Standards every five years via rulemaking. The current SBA Size Standards are contained in the SBA's Table of Small Business Size Standards, effective January 1, 2022, which can be found at both 13 CFR 121.201 and https://www.sba.gov/document/support-table-size-standards. Currently, the threshold for those industries where small business status is determined by number of employees is between 100 and 1,500 employees depending on the industry. The threshold for those industries where small business status is determined by annual

---

[199] See 13 CFR 121.101(a).
[200] See 13 CFR 121.903(a).
[201] *Id.*
[202] NAICS is the standard used by Federal statistical departments and agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. Additional information on NAICS, to include a listing of current NAICS codes, can be found at https://www.census.gov/naics/ (last visited Nov. 28, 2023).

revenue is between $2.25 million and $47 million depending on the industry. It is estimated that, as of 2022, there are more than 32 million small businesses in the United States, and that small businesses comprise 99.9% of all American businesses.[203]

In establishing its Size Standards, the SBA considers economic characteristics comprising the structure of an industry, such as degree of competition, average firm size, and distribution of firms by size, as well as competition from other industries, growth trends, historical activity within an industry, and unique factors occurring in the industry which may distinguish small firms from other firms.[204] As the establishment of the SBA Size Standards is done via regulation, the public is afforded the opportunity to review and provide comments on any proposed modifications to existing SBA Size Standards before they go into effect. In light of the comprehensive and transparent process through which the SBA establishes its Size Standards, and the successful use of these standards as size-based thresholds for various Federal programs, CISA believes the SBA Size Standards are well-suited for use as the size-based threshold aspect of the CIRCIA Applicability section.

In determining the approach to propose for the covered entity description's size threshold, CISA also considered working with the SBA to establish a size standard for entities in critical infrastructure sectors tailored to the CIRCIA program. In exploring this option, CISA assessed whether a clear justification existed for using higher or lower thresholds than those established by the SBA Size Standards. CISA also considered whether a single threshold for all entities, rather than industry-specific thresholds, might be warranted. Ultimately, CISA, based in part on conversations with SBA, did not

---

[203] See, e.g., Kelly Main, *Small Business Statistics of 2023*, Forbes (Dec. 7, 2022), available at https://www.forbes.com/advisor/business/small-business-statistics/); U.S. Chamber of Commerce, *Small Business Statistics*, https://www.chamberofcommerce.org/small-business-statistics/ (last visited Nov. 28, 2023).

[204] 13 CFR 121.102(a).

believe sufficient justification existed to deviate from the existing SBA Size Standards in any of these manners.

The first alternative CISA considered was the use of higher thresholds than those established in the SBA Size Standards. By raising the threshold—i.e., increasing the minimum number of employees or amount of annual receipts an entity has to have before qualifying as a covered entity—CISA would be further reducing the number of entities that would qualify as covered entities. Considering the significant number of entities for whom using the SBA Size Standards as the threshold would provide regulatory relief, CISA believes that there is no need to generally exclude additional entities. Conversely, for the reasons discussed earlier supporting the need for broad collection of reports, CISA is concerned that any further reduction in the number of covered entities could make it difficult for CISA to achieve the goals of the regulation. See Section III.C.ii.

The second alternative CISA considered was the use of lower thresholds than those established in the SBA Size Standards. By lowering the threshold—i.e., decreasing the minimum number of employees or amount of annual receipts an entity has to have before qualifying as a covered entity—CISA would be expanding the number of entities that would qualify as covered entities under this threshold. For the reasons discussed above, CISA believes it does not need to collect reports from the entire possible universe of covered entities allowed under the statutory language and that it is prudent to provide regulatory relief to smaller entities where possible. To the extent that some categories of entities from whom CISA believes reporting is important fall below the size threshold, CISA will be able to include those entities in the description of covered entity using the proposed sector-based criteria.

Finally, CISA explored whether there might be some benefit to using a single size-based threshold (or two—i.e., one each for number of employees and annual receipts), as opposed to the SBA Size Standards approach that establishes bespoke

thresholds for more than 1,000 individual industries based on their NAICS codes. CISA does believe that using a single size-based threshold (or two) that would be consistent across all industries would be a simpler, clearer approach; however, the SBA has consistently determined that using size thresholds tailored by industry is important to respecting relevant and significant distinctions across different industries. Not only does the SBA use that approach in its own Size Standards, the Small Business Size Regulations require the SBA Administrator to ensure that any size standard approved by the SBA for use by other Federal regulators under the 13 CFR 121.903 process "varies from industry to industry to the extent necessary to reflect the differing characteristics of the various industries, and consider other relevant factors."[205] In light of this, CISA believes the best approach would be to use the SBA Size Standards as the basis for the CIRCIA size threshold.

c. How to Determine Whether an Entity Meets the Size Threshold

To determine if an entity in a critical infrastructure sector meets the proposed size threshold, an entity will need to determine which NAICS code should be applied to the entity and whether the entity meets the applicable employee-based or annual receipts-based threshold. The SBA's Small Business Size Regulations provide requirements for how to determine if an entity qualifies as a small business under SBA regulations.[206] This includes, among other things, requirements for determining which NAICS code applies to a given entity (13 CFR 121.101), how to calculate number of employees (13 CFR 121.106), and how to calculate annual receipts (i.e., annual revenue) (13 CFR 121.104). CISA does not see any reason to deviate from this well-established approach to determining an entity's size and thus is proposing to use the instructions found in the SBA's Small Business Size Regulations as the methodology to be used to determine if an

[205] 13 CFR 121.903(b).
[206] See 13 CFR 121.103 – 121.107.

entity meets the CIRCIA covered entity size threshold. Accordingly, CISA is proposing that when an entity is determining whether it meets the size threshold provided in the Applicability section, the entity should follow the instructions contained in the Small Business Size Regulations, 13 CFR part 121, or any successor thereto.

CISA recognizes that entity size and other characteristics can be dynamic, and whether an entity meets the size-based threshold or other criteria for being a covered entity may vary depending on when the entity assesses if they meet the criteria set forth in § 226.2. See discussion on reporting requirements in Section IV.C.i in this document for more information.

2. Sector-Based Criteria

CISA is also proposing to include as part of the description of covered entity in the Applicability section a series of criteria that are based on characteristics typically associated with entities in one or more specific critical infrastructure sectors or subsectors. Specifically, CISA is proposing to include in the scope of covered entity any entity that meets one or more of a set of specified sector-based criteria, each of which is described below. These criteria apply regardless of the specific critical infrastructure sector of which the entity considers itself to be part.

CISA is proposing these additional, sector-based criteria for a variety of reasons. First, as noted in the discussion regarding the size-based criterion, an entity's size does not necessarily reflect its criticality. Some entities in a critical infrastructure sector that fall below the proposed size-based thresholds own or operate systems or assets that would be likely to meet the definition of critical infrastructure set forth by 42 U.S.C. 5195c(e). One of the main purposes of this regulatory program authorized by CIRCIA is to enhance the security and resiliency of critical infrastructure, and therefore receiving Covered Cyber Incident Reports and Ransom Payment Reports from as many entities that own or operate critical infrastructure as possible is imperative to meet this directive.

Another designated purpose of the CIRCIA regulation is for CISA to develop and share information on cybersecurity trends and threats. CISA believes that in addition to cross-sector cybersecurity threat and trend analysis, there is great value to being able to produce sector-specific threat and trend analysis. To achieve the latter, it is essential for the Federal government to have sufficient reporting from each critical infrastructure sector. For some sectors or subsectors, such as the Water and Wastewater Systems Sector, there currently is little or no required reporting of cyber incidents to the Federal government, making it very difficult for CISA or other Federal partners to provide reliable, incident-based, sector-specific trend and threat analysis. CISA believes the proposed sector-based criteria will help ensure the Federal government has sufficient reporting within each sector to support this type of analysis.

Third, consistent with the factors in 6 U.S.C. 681b(c)(1), CISA believes that broader coverage may be warranted for those sectors, subsectors, or industries that have historically been inordinately targeted by malicious cyber actors, including by foreign countries, or for which there is a greater likelihood of significant national security, economic security, or public health and safety consequences or disruption to the reliable operation of critical infrastructure. By ensuring CISA receives CIRCIA Reports from entities, regardless of size, in these more frequently or likely targeted sectors, subsectors, or industries, and entities against whom a covered cyber incident is more likely to result in significant consequences or disruptions to critical infrastructure, CISA and its partners will be better situated to identify new TTPs, campaigns, and vulnerabilities and share early warnings and prevention measures to help entities in those communities address the potential heightened threat for them of cyber incidents.

Based on the above rationales, CISA is proposing sector-based criteria for entities operating in each of the critical infrastructure sectors listed below. During the development of these proposed criteria, CISA engaged each of the SRMAs to consult on

potential criteria for their respective sector, as well as other Federal agencies with cybersecurity-related regulatory authorities focused on specific sectors. CISA also considered the inputs received from the public through both the CIRCIA listening sessions and in response to the CIRCIA RFI.

For the proposed sector-based criteria, CISA proposes to cover entities that own or operate certain types of facilities or entities that perform certain functions as covered entities. For example, the Chemical Sector sector-based criteria proposes capturing within the description of covered entity any entity that owns or operates a CFATS-covered chemical facility, and the Healthcare and Public Health sector-based criteria would include, among others, entities that manufacture any Class II or III medical device. See Section IV.B.iv.2.a and i in this document. While these criteria are focused on certain facility types or functions as the basis of determining whether an entity is a covered entity, CISA is proposing that the entire entity (e.g., corporation, organization), and not the individual facility or function, is the covered entity. Thus, for example, if an entity owns 20 chemical distribution facilities, only five of which are CFATS-regulated facilities, the entire entity is the covered entity, and not simply the five CFATS-regulated facilities. Accordingly, if that entity experiences a substantial cyber incident or makes a ransom payment, the entity would need to report that incident or payment to CISA regardless of whether the underlying incident impacted any of the five CFATS-regulated facilities. Similarly, if an entity manufactures Class II or III medical devices, in addition to other functions that do not meet one of the sector-based criteria, the entire entity is the covered entity, and any substantial cyber incident experienced by any part of the entity would need to be reported, regardless of whether the underlying incident impacted the manufacturing of Class II or III medical devices. CISA believes this is consistent with CIRCIA's entity-based approach, and will ensure that adequate reporting is provided to CISA to perform sector-specific cybersecurity threat and trend analysis, which might not

be possible if reporting was limited only to incidents that actually impact the specific facilities or functions identified in the sector-based criteria. Considering the entire entity (e.g., corporation, organization), and not an individual facility or function, as the covered entity will also avoid delays in reporting that could be caused if entities had to wait to specifically determine whether particular facilities or functions were impacted by a substantial cyber incident.

a. Chemical Sector

CISA is proposing to include in the description of covered entity any entity in a critical infrastructure sector that owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards.[207] CISA proposes including this criterion to ensure that entities that own or operate a covered chemical facility that presents a high risk of significant adverse consequences for human life or health, national security, and/or critical economic assets if subjected to terrorist attack, compromise, infiltration, or exploitation are required to report substantial cyber incidents to CISA.

Under CFATS, any facility that possesses a threshold quantity of one of more than 300 chemicals of interest must provide information to CISA to enable CISA to conduct a risk assessment of the facility. See 6 CFR 27.200. If CISA determines that the facility is high-risk based on this assessment, the facility is required to develop and implement a site security plan, which must include appropriate cybersecurity measures. See 6 CFR 27.210(a)(3). These facilities are referred to under the CFATS regulations as covered chemical facilities.

---

[207] See 6 CFR part 27. CISA is aware that, at the time of publication of this NPRM, Congress has allowed statutory authority for the CFATS program to expire. CISA believes that by the time the CIRCIA final rule is issued, CFATS will be reauthorized by Congress. Should CFATS not be reauthorized by the time the CIRCIA final rule is ready for publication, CISA proposes to replace the proposed CFATS-based Chemical Sector criterion in this NPRM with an alternate Chemical Sector criterion focused on owners and operators of facilities regulated by the Environmental Protection Agency (EPA) under its Risk Management Program (RMP) regulations. That alternative is discussed at the end of this subsection.

Consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) also supports the inclusion of entities that own or operate CFATS covered chemical facilities within the description of covered entity. To determine if a chemical facility is high-risk and thus subject to CFATS, CISA conducts a risk assessment on the facility that considers the potential consequences of a successful attack on the facility, the level of threat facing the facility, and the vulnerability of the facility to an attack.[208] Only chemical facilities that have the potential to cause significant consequences to public health and safety if compromised by terrorism (i.e., the first factor identified in 6 U.S.C. 681b(c)(1), which relates to consequence) and face a high potential threat (i.e., the second factor identified in 6 U.S.C. 681b(c)(1), which relates to likelihood of threat) will meet the criteria to be designated a CFATS covered chemical facility. As such, CISA believes that the first two factors enumerated in 6 U.S.C. 681b(c)(1) support the inclusion of entities that own or operate CFATS covered chemical facilities within the description of covered entity. The third factor enumerated in 6 U.S.C. 681b(c)(1), which refers to the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure, similarly supports inclusion of these entities, as most, if not all, CFATS covered chemical facilities would meet the definition of critical infrastructure based on the potential national security or public health and safety consequences associated with a successful attack on the facility.

As noted in the previous section of this document, while CFATS security requirements apply only to the covered chemical facilities themselves, CISA is proposing in this NPRM that the CIRCIA cyber incident reporting requirements apply to the entire corporate entity that owns or operates the CFATS-covered chemical facility and are not limited to substantial cyber incidents that impact a CFATS-covered chemical facility.

---

[208] See CISA, *CFATS Tiering Methodology Fact Sheet*, available at https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-tiering-methodology) (last visited Oct. 15, 2023).

CISA believes this is consistent with CIRCIA's entity-based approach and will ensure that adequate reporting is provided to CISA to perform chemical sector cyber threat and trend analysis, which might not be possible if reporting were limited only to incidents that actually impact CFATS-covered chemical facilities.

Because CFATS currently requires covered chemical facilities to report certain incidents, including potential cyber incidents, to CISA, CISA recognizes that this proposed criteria likely will result in two different legal obligations for certain entities to report cyber incidents to CISA under certain circumstances, depending on whether it is reporting a covered cyber incident or not. To avoid the same entity having to report the same incident to CISA twice, CISA is proposing that submission of a cyber incident report to CISA under either one of these authorities will satisfy the incident reporting obligations for both regulations for the incident, assuming the single submission includes all the information required to comply with both CFATS and CIRCIA, independently. However, if a covered entity reports an incident to CISA per CFATS requirements and intends for this report to also meet its reporting obligations under CIRCIA, it would need to indicate that intent in the submission. Otherwise, a separate CIRCIA Report would need to be filed to meet the entity's reporting obligations.

Finally, CISA also is aware that a number of high-risk chemical facilities may not be subject to CFATS under one of the statutory exemptions in the legislation authorizing CFATS. Specifically, CFATS does not apply to facilities regulated under MTSA; public water systems, as that term is defined in 42 U.S.C. 300f; Treatment Works, as that term is defined in 33 U.S.C. 1292; or facilities subject to regulation by the NRC. 6 CFR 27.110(b). As a result, many entities that own high-risk chemical facilities would not be required to report cyber incidents to CISA either under CFATS or under this proposed sector-based criteria. CISA is proposing to require each of these categories of entities to file a CIRCIA Report under various other sector-based criteria, however, so CISA

ultimately is proposing that all entities that own or operate a high-risk chemical facility must report covered cyber incidents and ransom payments under one of the sector-based criteria.

As noted in an earlier footnote, CISA is aware that, at the time of publication of this NPRM, Congress allowed the statutory authority for CFATS to expire. CISA believes that by the time the CIRCIA final rule is issued, CFATS will be reauthorized, but also recognizes that it is prudent to include for public consideration a proposed alternative Chemical Sector sector-based criterion should CFATS not be reauthorized. Accordingly, CISA proposes that if CFATS is not reauthorized by the time the CIRCIA final rule is ready for publication, CISA instead would replace the CFATS-based Chemical Sector criterion with a Chemical Sector sector-based criterion that description identifies owners and operators of facilities subject to the EPA RMP rule as covered entities.

The EPA RMP rule, which is authorized by Section 112(r) of the Clean Air Act,[209] requires facilities that use certain extremely hazardous substances to develop a risk management plan for chemical accident prevention purposes.[210] For similar reasons as those provided above in relation to the proposed CFATS-focused Chemical Sector sector-based criterion, a consideration of the 6 U.S.C. 681b(c)(1) factors would also support the inclusion of entities that own or operate facilities that are required to comply with EPA RMP requirements in the description of covered entity. According to the EPA, such chemical accidents that occur at such facilities can pose significant consequence and potential threat to national security and public health and safety because "[f]acilities subject to the RMP regulation pose significant risks to the public and the environment. These risks stem from potential accidental chemical releases that can cause fires,

---

[209] See 40 CFR part 68.

[210] See EPA, *Risk Management Program (RMP) Rule Overview*, https://www.epa.gov/rmp/risk-management-program-rmp-rule-overview (last visited Nov. 28, 2023).

explosions, and harmful vapor clouds."[211] Furthermore, according to the U.S. GAO, "[t]housands of high-risk chemical facilities may be subject to the risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass causalities to surrounding populations."[212] Moreover, as part of the development of the CFATS program's regulations, DHS drew from information and sources available through EPA RMP, including the list of substances used by EPA RMP to regulate facilities, due to the overlapping safety and security concerns associated with many chemicals.[213]

For the reasons described above, CISA believes entities owning facilities subject to EPA RMP would be a satisfactory alternate criterion for ensuring CISA receives reporting under CIRCIA from entities within the Chemical Sector, and is supported by the three factors in 6 U.S.C. 681b(c)(1); however, CISA believes the CFATS-targeted criterion would be a better criterion for the Chemical Sector, if permissible, for a few reasons. First, regulation under the EPA RMP rule is limited to facilities that only present toxic or flammable release concerns because they impact public health and safety, whereas CFATS regulates facilities that are high risk due to other chemical security related concerns. Additional security concerns posed by CFATS includes coverage of chemicals that pose risks related to theft or diversion of explosives or weapons of mass effect, in addition to toxic and flammable release hazards. Second, whereas EPA RMP determines coverage primarily based on the potential consequences of a chemical release, CFATS additionally is required to take into account threat when determining if a facility

---

[211] Reconsideration of the 2017 Amendments to the Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act, Section 112(r)(7), *Regulatory Impact Analysis* at 76 (Nov. 18, 2019), available at https://www.regulations.gov/document/EPA-HQ-OEM-2015-0725-2089.
[212] U.S. GAO, *GAO-20-453: CRITICAL INFRASTRUCTURE PROTECTION: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities* (May 2020), available at https://www.gao.gov/products/gao-20-453.
[213] See 72 FR 17688 (Apr. 9, 2007).

is a CFATS covered chemical facility. Finally, because CFATS imposes cyber incident reporting requirements, using CFATS as a basis for the CIRCIA cyber incident reporting requirements coverage promotes harmonization of Federal cyber incident reporting regulations by aligning reporting requirements for the same population of entities. For these reasons, CISA is proposing to include a criterion capturing entities that own or operate facilities regulated under EPA RMP within the description of covered entity only if CFATS is not authorized at the time of the issuance of the CIRCIA final rule.

CISA is interested in receiving comments on these two alternatives, to include:

10. The decision to solely use the CFATS-based criterion if CFATS is in effect at the time of the issuance of the CIRCIA final rule.
11. Other possible alternatives that CISA should consider as a sector-based criterion for the Chemical Sector if CFATS is not reauthorized by Congress.

b. Communications Sector

CISA is proposing to include in the description of covered entity any entity that provides communications services by wire or radio communications, as defined in 47 U.S.C. 153(40), 153(59), to the public, business, or government. This criterion would also require reporting from both one-way communications service providers (e.g., radio and television broadcasters, cable television and satellite operators) and two-way communications service providers (e.g., telecommunications carriers; submarine cable licensees; fixed and mobile wireless service providers; VoIP providers; internet service providers), irrespective of whether they are subject to FCC regulatory reporting or other FCC requirements.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of both one-way and two-way communications service providers within the description of covered entity. First, the disruption or compromise of either one-way or two-way communications systems could significantly impact national security, economic

security, and public health and safety. As noted in the 2015 Communications SSP, "[v]irtually every element of modern life is now dependent on cyber infrastructure. As a result, our Nation's economic and national security relies on the security of the assets and operations of critical communications infrastructure."[214] Executive Order 13618 – Assignment of National Security and Emergency Preparedness Communications Functions reinforces the importance of these entities to national security, stating that "[t]he Federal Government must have the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions. . . . Such communications must be possible under all circumstances to ensure national security, effectively manage emergencies, and improve national resilience."[215]

One-way communications services providers are the primary providers of information, including emergency alerts, to the public. Therefore, a covered cyber incident affecting one-way communications service providers has the potential to significantly jeopardize public health and national security by crippling the government's ability to distribute important information quickly. Two-way communications services are essential to the operation of the nation's public safety answering points and 911 emergency call system for transmission of both voice and data.[216] These risks exist regardless of a provider's size, as small service providers may serve critical infrastructure operators, and wireless service providers, broadcasters, and cable providers of all sizes are responsible for providing emergency alerts.

Second, Communications Sector assets historically have been targeted by malicious cyber actors. Per the 2023 IBM Security X Force Threat Intelligence Index, "Media and Telecom" entities have consistently experienced cyber incidents over the

---

[214] See *Communications SSP: An Annex to the NIPP 2013* at 3 (2015), available at https://www.cisa.gov/2015-sector-specific-plans (hereinafter "*Communications SSP*").
[215] *EO 13618 – Assignment of National Security and Emergency Preparedness Communications Functions*, 77 FR 40779 (July 6, 2012).
[216] Public safety answering points are required to report outages to the FCC pursuant to 47 CFR part 4, which the FCC then shares with CISA.

years, with the industry peaking as the industry experiencing the fourth most incidents in 2019.[217] Additionally, per the 2024 Homeland Security Threat Assessment, the telecommunications industry is likely to remain a target of foreign government-affiliated cyber actors from foreign countries such as Russia and China.[218]

Finally, communications services also are essential to the operations of every other critical infrastructure sector. As noted in the Communications SSP, "the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the Communications Sector to support its operations…."[219] Damage, disruption, or unauthorized access to these communications providers has a high likelihood of disrupting the reliable operation of other critical infrastructure assets, which can cause potentially cascading impacts to NCFs. This criticality to other sectors is reinforced by the fact that communications is one of four designated lifeline functions, indicating that the reliable operations of this sector is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.[220]

c. Critical Manufacturing Sector

CISA is proposing to include in the description of a covered entity any entity that owns or has business operations that engage in one or more of the listed categories of manufacturing, which are the four manufacturing industries that together currently constitute the Critical Manufacturing Sector. The Critical Manufacturing Sector

---

[217] IBM, *2023 IBM Security X-Force Threat Intelligence Index* at 42, available at https://www.ibm.com/reports/threat-intelligence (hereinafter, "*IBM 2023 Threat Index*").
[218] *2024 Homeland Security Threat Assessment* at 20, *supra* note 188, at 20 ("Russian government-affiliated cyber espionage likely will remain a persistent threat to federal, state, and local governments, as well as entities in the defense, energy, nuclear, aviation, transportation, healthcare, education, media, and telecommunications industries. Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including healthcare and public health, financial services, the defense industrial base, government facilities, and communications.").
[219] *Communications SSP*, *supra* note 214, at 9.
[220] See *Guide to Critical Infrastructure Security and Resilience*, *supra* note 198, at 4 ("There are four designated lifeline functions—transportation, water, energy, and communications, which means that their reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors.").

subsectors, which were identified by DHS after a study of the manufacturing sector, are Primary Metal Manufacturing (NAICS Subsector 331); Machinery Manufacturing (NAICS Subsector 333); Electrical Equipment, Appliance, and Component Manufacturing (NAICS Subsector 335); and Transportation Equipment Manufacturing (NAICS Subsector 336).[221] In 2008, DHS combined these four subsectors into a new Critical Manufacturing Sector based largely on the fact that the failure or disruption of any of these industries could cause, among other things, a large number of fatalities, significant national economic impact, or an inability of the government to provide necessary services to the public.[222]

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of the entities comprising the Critical Manufacturing Sector within the description of covered entity. First, as noted in the previous paragraph, the President designated entities within these NAICS codes as the Critical Manufacturing Sector due in large part to the potential that disruption or compromise of such entities could impact national security, economic security, or public health and safety.[223] Moreover, the entities within this sector often focus on efficiency, not redundancy, with lean inventories and just-in-time practices that can increase vulnerability to cascading disruptions and decrease agility in response with potentially damaging financial implications,[224] increasing the likelihood that a cyber incident could negatively impact economic security.

Second, the manufacturing industry historically have been targeted by malicious cyber actors, and the expectation is for that targeting to continue. According to the IBM

---

[221] See 73 FR 23476 (Apr. 30, 2008).
[222] *Id.*
[223] *Id.*
[224] See *Critical Manufacturing SSP: An Annex to the NIPP 2013* at 4 (2015), available at https://www.cisa.gov/2015-sector-specific-plans (hereinafter "*Critical Manufacturing SSP*").

Security X-Force Threat Intelligence Index for 2023 (IBM 2023 Threat Index), the manufacturing industry experienced the most cyber incidents in both 2021 and 2022.[225]

Third, damage or disruption to a Critical Manufacturing Sector entity has the potential to disrupt the reliable operation of critical infrastructure. As noted in the *Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector*, "[b]ecause of the importance of the manufacturing industry in sustaining cross-sector interdependencies, the Critical Manufacturing Sector also includes systems and operations that, if attacked or disrupted, would cause major interruptions to the essential functions of one or more other [critical infrastructure] sectors and result in national-level impacts."[226] Moreover, local or regional disruptions to entities within the Critical Manufacturing Sector can have cascading impacts across wide geographic regions and industries.[227]

Given the overall criticality of the entities within this sector, the reliance of NCFs on the items manufactured by entities within this sector, the relative lack of substitutability of many of the products produced by the sector, and the history of cyber incidents impacting manufacturing entities, CISA believes it is appropriate for all entities operating in any of the four Critical Manufacturing Sector subsectors to be required to report covered cyber incidents and ransom payments to CISA.

d. Defense Industrial Base Sector

CISA proposes including within the description of covered entity any entity that is a contractor or subcontractor required to report cyber incidents to DOD pursuant to the definitions and requirements of the DFARS *Safeguarding Covered Defense Information and Cyber Incident Reporting* clause located at 48 CFR 252.204-7012. This proposed

---

[225] See *IBM 2023 Threat Index*, *supra* note 217, at 42; see also *Verizon 2022 DBIR*, *supra* note 181, at 50 (listing Manufacturing as experiencing the fifth most cyber incidents of any industry in 2022).
[226] 73 FR 23476, 23477 (Apr. 30, 2008).
[227] See *Critical Manufacturing SSP*, *supra* note 224, at v.

sector-based criteria would require reporting from DOD contractors and subcontractors that provide operationally critical support to DOD, as well as DOD contractors and subcontractors that utilize unclassified information systems that are owned, or operated by or for, the contractor to process, store, or transmit covered defense information.[228]

DOD's contractor cyber incident reporting requirements apply to the subset of contractors that process, store, or transmit "covered defense information" or that DOD has determined provide "operationally critical support." "Covered defense information" includes things such as controlled technical information, critical information related to operations security, and information concerning certain items, commodities, technology, or software whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.[229] Contractors that provide "operationally critical support" include those that provide "supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."[230] CISA acknowledges that contractors that provide operationally critical support also includes entities in one or more critical infrastructure sectors, and are not generally considered as part of the Defense Industrial Base, as described in the Defense Industrial Base SSP.[231] For the purposes of the CIRCIA rule, CISA proposes grouping these entities under the Defense Industrial Base Sector sector-based criteria to provide these entities an easier means of identifying whether they are a covered entity. CISA also recognizes that certain

---

[228] See 48 CFR 252.204-7012.
[229] 48 CFR 204.7301.
[230] 48 CFR 252.204-7012(a).
[231] The Defense Industrial Base Sector "consists of government and private sector organizations that can support military operations directly; perform R&D; design, manufacture, and integrate systems; and maintain depots and service military weapons systems, subsystems, components, subcomponents, or parts – all of which are intended to satisfy U.S. military national defense requirements." *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* at 15 (2015), available https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector.

contractors that provide operationally critical support may fall under other proposed Applicability criteria, including other sector-based criteria (*e.g.* for the Transportation Sector).

As both DOD and their prime contractors frequently contract with small businesses to meet small business contracting and subcontracting goals and requirements, many of the entities covered under these criteria would not be captured by the size threshold contained in the proposed Applicability section. In developing the final rule requiring these contractors to report cyber incidents to DOD, DOD specifically addressed the need to include small businesses in the regulated population, stating in part that the costs to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than the costs of implementation of the regulation and that "[t]he value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small)."[232]

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. First, cyber incidents perpetrated against contractors covered under the DFARS regulation "may cause harm to the Government through the compromise of covered defense information or other Government data, or the loss of operationally critical support capabilities, which could directly impact national security."[233] Second, members of the U.S. intelligence community have concluded that malicious cyber actors, to include foreign countries, are likely to continue to target members of the Defense Industrial Base Sector.[234] Finally, damage, disruption, or unauthorized access to these entities, including the accessing of sensitive cybersecurity vulnerability information, may enable the disruption of the

---

[232] 81 FR 72986, 72987 (Oct. 21, 2016).
[233] See 80 FR 51739 (Aug. 26, 2015).
[234] See *2024 Homeland Security Threat Assessment* at 20, *supra* note 188, at 20 ("Russian government-affiliated cyber espionage likely will remain a persistent threat to . . . entities in the defense . . . industr[y]. Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including . . . the defense industrial base . . . .").

reliable operation of critical infrastructure because of its interdependency with critical defense infrastructure. As noted earlier, the entities proposed for inclusion under this sector-based criterion are regulated under the DFARS because they provide "operationally critical support" or process, store, or transmit "covered defense information." Disruption of operationally critical support definitionally disrupts the reliable operation of critical defense infrastructure, and the compromise of covered defense information could be used to enable the disruption of the reliable operation of critical infrastructure.

CISA recognizes that entities required to report under these criteria are, by definition, already required to report certain cyber incidents to DOD. Given their criticality to national security, however, CISA nevertheless is proposing to include them within the CIRCIA Applicability section. This will ensure that the Federal government receives information necessary to identify cyber threats, exploited vulnerabilities, and TTPs that affect entities in this community and in other interdependent critical infrastructure sectors, even if changes are made to what must be reported pursuant to the DFARS regulation, over which CISA has no authority. CISA acknowledges the potential this creates for duplicative reporting and is committed to working with DOD to explore the applicability of the substantially similar reporting exception to enable entities subject to both CIRCIA and DFARS cyber incident reporting requirements to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government to the extent practicable. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

e. Emergency Services Sector

CISA proposes including within the description of covered entity any entity that provides one or more of five listed emergency services or functions to a population equal to or greater than 50,000 individuals. These five disciplines—law enforcement, fire and

rescue services, emergency medical services, emergency management, and public works that contribute to public health and safety—and the types of entities that provide these services are described in the 2015 Emergency Services SSP.[235]

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. Regarding the first and third enumerated factors (consequence and disruption of reliable operation of critical infrastructure), as noted in the Emergency Services SSP, this sector's operations provide the first line of support for nearly all critical infrastructure, and a failure or disruption in these services could result in significant harm or loss of life, major public health impacts, long term economic loss, and cascading disruptions to other critical infrastructure.[236] Similarly, members of the broader public rely on these entities to provide assistance in the times of greatest need.

Regarding the second factor enumerated in 6 U.S.C. 681b(c)(1), which relates to threat, Emergency Services Sector entities routinely are targeted by malicious cyber actors. As noted in the 2012 Emergency Services Sector Cyber Risk Assessment Fact Sheet, Emergency Services Sector entities "face[] threats from criminals, hackers, terrorists, and nation-states, all of whom have demonstrated varying degrees of capability and intention to attack [Emergency Services Sector] cyber infrastructure."[237] Malicious cyber activity targeting law enforcement and other Emergency Services Sector entities has continued to be a problem in more recent years.[238] Given Emergency Services Sector

---

[235] DHS, *Emergency Services SSP: An Annex to the NIPP 2013* (2015), available at https://www.cisa.gov/resources-tools/resources/emergency-services-sector-specific-plan-2015.
[236] See *id.* at 3-7.
[237] DHS, *2012 Emergency Services Sector Cyber Risk Assessment Fact Sheet*, available at https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cyber-risk-assessment.
[238] See, e.g., Resecurity, *Cybercriminals Are Targeting Law Enforcement Agencies Worldwide* (Aug. 19, 2022) ("Resecurity registered an increase in malicious activity targeting law enforcement agencies at the beginning of Q2 2022."), available at https://www.resecurity.com/blog/article/cybercriminals-are-targeting-law-enforcement-agencies-worldwide; J.J. Green, *Cyberterrorists Targeting First Responders* (Sept. 6, 2017) ("A U.S. intelligence community collaborative warned first responders in late July about escalating efforts to target them and their missions by cyberterrorists."), available at https://wtop.com/national-security/2017/09/cyber-terrorists-targeting-first-responders/.

entities' critical role in the nation's public health and security and their continued targeting by malicious cyber actors, it is essential that CISA, as the SRMA for this sector, have an adequate understanding of emerging cyber threats and trends impacting this sector.

Generally speaking, entities within the Emergency Services Sector are not subject to any Federal cyber incident reporting requirements. While most of the entities within this sector are SLTT entities likely to be captured by the SLTT Government Facilities Sector sector-based criterion (see Section IV.B.iv.2.h in this document), without this sector-based criterion, CISA would not receive reports from those Emergency Services Sector entities within the private sector that fall under the SBA Size Standards referenced in the sized-based standard in the Applicability section. Accordingly, to ensure CISA has both visibility into cyber incidents impacting privately owned Emergency Services Sector entities as well sufficient reporting from this sector overall, CISA is proposing this sector-based criteria.

Much like any other sector, entities within the Emergency Services Sector can vary greatly in size and resources. For the same reasons provided above as support for the proposal to use a size-based threshold, CISA believes that it makes sense to focus CIRCIA covered cyber incident and ransom payment reporting requirements on the larger, better-resourced entities within the Emergency Services Sector. To achieve that, CISA is proposing that the reporting requirements only apply to those entities that support populations equal to or greater than 50,000 individuals. CISA based its decision to propose 50,000 individuals as the threshold as that is consistent with the definition of a "small government jurisdiction" under the Regulatory Flexibility Act, which is the primary law requiring Federal departments and agencies to consider the effects of their regulations on small businesses and other small entities. 5 U.S.C. 601(5). CISA believes

this is an appropriate basis for reporting under CIRCIA for the same reasons described in Section IV.B.iv.1.a as support for the size-based criterion.

f. Energy Sector

CISA proposes including within the description of covered entity any entity that is required to report cybersecurity incidents under NERC's CIP Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to DOE. This criterion proposes to require reporting from entities registered with NERC who are part of the BES and identified as "Responsible Entities" under CIP-003-8 (Cyber Security – Security Management Controls) or CIP-008-6 (Cyber Security – Incident Reporting and Response Planning) and any successor standards. The goal of the CIP Cyber Security Standards is to mitigate the risk to the reliable operation of the BES as the result of a cybersecurity incident. This criterion would also require reporting from Electric Utilities, Balancing Authorities, Reliability Coordinators, and Generating Entities that are subject to electric emergency incident and disturbance reporting requirements via Form OE-417. DOE uses Form OE-417 to collect information from the electric power industry relevant to DOE's overall national security and National Response Framework responsibilities. CISA is proposing to include this specific criterion in light of the importance of these Energy Sector assets and the frequency with which the energy industry is impacted by cyber incidents.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. Regarding the first and third enumerated factors (consequence and disruption of reliable operation of critical infrastructure), the reliable operation of the U.S. electric energy supply systems and BES is essential, as infrastructure within all 16 critical infrastructure sectors relies on electricity to function. As noted in the 2015 Energy SSP, "[t]he energy infrastructure provides essential fuel to all critical infrastructure sectors, and without energy, none of

them can operate properly. Thus the Energy Sector serves one of the four lifeline functions, which means that its reliable operation is so critical that a disruption or loss of energy function will directly affect the security and resilience of other critical infrastructure sectors."[239] Cyber incidents affecting entities that own or operate the Energy Sector assets identified in the proposed criterion could result in cascading impacts affecting the nation's ability to carry out a multitude of NCFs, with significant consequences to economic security and public health and safety.

Regarding the second factor enumerated in 6 U.S.C. 681b(c)(1) relating to threat, Energy Sector entities routinely are targeted by malicious cyber actors, including foreign actors. According to the IBM 2023 Threat Index, the energy industry experienced the fourth most cyber incidents between 2018 and 2022.[240] The energy industry also is one of the industries noted in the 2024 Homeland Security Threat Assessment as likely to remain a target of Russian government-affiliated cyber espionage.[241]

The criterion proposed captures a wide variety of Energy Sector entities, to include both energy generators and distributors across the spectrum of coal, natural gas, hydroelectric, wind, and solar. Many additional Energy Sector entities would be required to report under the proposed size-based threshold or other proposed sector-based criteria, such as the criteria requiring reporting from owners and operators of commercial nuclear power reactors and certain pipelines (see Sections IV.B.iv.2.k and l in this document).

CISA acknowledges the potential for the inclusion of this criterion to create an additional reporting obligation on entities already required to report cyber incidents to the Federal government. CISA is committed to working with DOE, FERC, and NERC to explore the applicability of the substantially similar reporting exception to enable, to the extent practicable, entities subject to both CIRCIA and CIP Reliability Standards or Form

---

[239] *Energy SSP* at 19 (2015), available at https://www.cisa.gov/2015-sector-specific-plans.
[240] *IBM 2023 Threat Index*, *supra* note 217, at 42.
[241] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

OE-417 reporting requirements to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

When developing the sector-based criteria for the Energy Sector, CISA also considered developing a criterion focused on entities within the Energy Sector's Oil and Natural Gas Subsector. The Oil and Natural Gas Subsector includes entities engaged in the production, gathering, processing, transmission, distribution, and storage of oil and gas, such as wells, processing plants and refineries, gathering and boosting stations, and natural or manmade storage facilities.[242] CISA anticipates that many Oil and Natural Gas Subsector entities will be considered covered entities through the size-based threshold, and that many others will be captured under any of a number of other proposed sector-based criteria, such as the Chemical Sector sector-based criterion covering entities that own or operate CFATS facilities, the Transportation Systems Sector sector-based criterion covering entities that own or operate MTSA facilities, and the Transportation Systems Sector sector-based criterion covering entities that own or operate certain designated pipelines (see Sections IV.B.iv.2.a and l in this document). In light of the number of Oil and Natural Gas Subsector entities that CISA anticipates will be covered through these other criteria, CISA is not proposing a specific sector-based criterion for this subsector. However, if as a result of public comment, CISA determines that it must modify or eliminate any aspect of the description of covered entity through which Oil and Natural Gas Subsector entities currently would be included as part of this proposed rule, including the size-based criterion, CISA may incorporate a sector specific criterion or

[242] See EPA, *Overview of the Oil and Natural Gas Industry*, https://www.epa.gov/natural-gas-star-program/overview-oil-and-natural-gas-industry (last visited on Nov. 28, 2023).

multiple criteria focused on Oil and Natural Gas Subsector entities in the final rule to ensure these entities remain covered entities.

If CISA were to include a specific Oil and Natural Gas Subsector sector-based criterion, it would likely set a threshold for Oil and Natural Gas Subsector entities and only those entities that exceed a specific size threshold would be considered a covered entity. Such a threshold would be set by CISA to ensure that the largest Subsector entities would be required to report, similar to the scope of entities that would be required to report under the proposed SBA size-based criterion, and could likely leverage the SBA Table of Size Standards employee or annual revenue thresholds using NAICS codes applicable to the Subsector to create an average that would become the threshold. CISA may also consider creating a threshold based on metrics specific to entities that are part of the Oil and Natural Gas Subsector, such as those entities exceeding specified refinery production capacity or liquefied natural gas terminal storage capacity.

CISA is interested in receiving comments from the public on the following topics:

12. CISA's proposal to incorporate Oil and Natural Gas Subsector entities primarily through the size-based threshold instead of developing one or more criteria specifically targeting Oil and Natural Gas Subsector entities—and whether this size threshold will capture the correct population of entities in this subsector.
13. The potential alternative criteria that could be included if any of the current proposed criteria that would otherwise capture Oil and Natural Gas Subsector entities were modified or not included in the final rule.

g. Financial Services Sector

CISA proposes to include in the description of covered entity various Financial Services Sector entities that, if victimized in a covered cyber incident, have the potential to impact the economic security of the nation. Specifically, CISA is proposing to include in the description of covered entity (1) all of the Financial Services Sector entities that are

required to report cybersecurity incidents to their respective primary Federal regulator (e.g., national banks; savings and loans holding companies; FICUs), (2) Financial Services Sector entities for whom the primary Federal regulator has indicated an intention to require cybersecurity incident reporting (e.g., futures commission merchants;[243] security-based swap data repositories), and (3) Financial Services Sector entities encouraged or expected to report cybersecurity incidents to their primary Federal regulator pursuant to an Advisory Bulletin (e.g., Fannie Mae and Freddie Mac;[244] money services businesses[245]).

CISA believes the inclusion of these entities in the description of covered entity is supported by consideration of the factors enumerated in 6 U.S.C. 681b(c)(1). As noted by many of the regulatory agencies currently requiring cyber incident reporting from Financial Services Sector entities, requiring the proposed entities to report helps promote early awareness of emerging threats to the financial system, and allows entities and their primary regulators to react to any such threats before they become systemic and threaten the nation's economic security.[246] This is especially important given the continued targeting of Financial Services Sector entities by malicious cyber actors, as relevant to the

---

[243] See Testimony of CFTC Chairman Rostin Behnam on the "State of the CFTC," U.S. House of Representatives Committee on Agriculture (Mar. 31, 2022), available at https://agriculture.house.gov/uploadedfiles/behnam_testimony_house_ag_3-31-2022.pdf.

[244] Pursuant to *Advisory Bulletin 2020-05*, Fannie Mae and Freddie Mac are expected to report certain cybersecurity incidents to the FHFA. See *AB 2020-05: Enterprise Cybersecurity Incident Reporting* (Aug. 21, 2020), available at https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Enterprise-Cybersecurity-Incident-Reporting.aspx.

[245] Pursuant to *Advisory Bulletin FIN-2016-A005*, money services businesses are expected to report certain cybersecurity incidents to the Department of the Treasury's Financial Crimes Enforcement Network. See FIN-2016-A005, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* (Oct. 25, 2016), available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.

[246] See, e.g., 86 FR 66424, 66424 (Nov. 23, 2021) ("This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic."); 88 FR 12811, 12811 (Mar. 1, 2023) ("[G]iven the growing frequency and severity of cyber incidents within the financial services industry, it is important that the NCUA receive timely notice of cyber incidents that disrupt a FICU's operations, lead to unauthorized access to sensitive data, or disrupt members' access to accounts or services."); 88 FR 23146, 23147 (Apr. 14, 2023) ("[T]he regulation requires that SCI entities have policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain their operational capability and promote the maintenance of fair and orderly markets . . . .").

second factor enumerated in 6 U.S.C. 681b(c)(1) related to threat. According to the IBM 2023 Threat Index, Financial Services Sector entities have experienced either the most or second most cyber incidents for each of the past five years,[247] while the 2024 Homeland Security Threat Assessment highlights financial services as one of the sectors Chinese government cyber actors are likely to continue targeting.[248] As to the third factor, i.e., the extent to which damage, disruption, or unauthorized access will likely enable the disruption of the reliable operation of critical infrastructure, systemic impacts to the Financial Services Sector has the potential to disrupt the reliable operation of critical infrastructure in light of virtually every critical infrastructure sectors' reliance on financial services entities for the conduct of day-to-day business operations.

As with several other proposed sector-based criteria, CISA recognizes that entities that would be required to report under these criteria are, for the most part, already required to report to another Federal regulatory agency. Given their importance to the nation's economy and the frequency with which they are targeted, CISA nevertheless is proposing to include them within the CIRCIA Applicability section ensure that the Federal government is able to receive information necessary to identify cyber threats against, exploited vulnerabilities of, and TTPs used to effect entities in this community without reliance on other authorities whose primary focus may not be security, and who might not currently or in the future require the submission of information necessary for CISA to achieve the purposes for which CIRCIA was enacted. CISA acknowledges the potential this creates for duplicative reporting and is committed to working with the respective Financial Services Sector Federal regulatory agencies to explore the applicability of the substantially similar reporting exception to enable, to the extent practicable, entities subject to both CIRCIA and another reporting requirement to be able

---

[247] *IBM 2023 Threat Index*, supra note 217, at 42; see also Verizon 2022 DBIR, supra note 181, at 50 (noting the Finance industry had the third highest number of incidents in 2022).
[248] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

to comply with both regulatory reporting regimes through the submission of a single report to the Federal government. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

h. Government Facilities Sector

CISA proposes to include three different sector-based criteria for entities in the Government Facilities Sector, one focused on SLTT Government Entities, one focused on Education Subsector entities, and one focused on Elections Infrastructure Subsector entities. First, CISA proposes to include in the description of covered entity any SLTT Government entity for a jurisdiction with a population equal to or greater than 50,000 individuals. Second, CISA proposes to include in the description of covered entity any entity that qualifies as either (A) a local educational agency (LEA), educational service agency (ESA), or state educational agency (SEA), as defined under 20 U.S.C. 7801, with a student population of 1,000 or more students; or (B) an institute of higher education (IHE) that receives funding under Title IV of the Higher Education Act. Third, CISA is proposing to include in the description of covered entity any entity that manufactures, sells, or provides managed service for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments, including but not limited to voter registration databases; voting systems; and information and communication technologies (ICT) used to report, display, validate, or finalize election results. As discussed in greater detail in Section IV.D.iii in this document, CISA is proposing to except from required reporting Federal agencies already required to report incidents to CISA under FISMA, such that these sector-based criteria are focused on SLTT and private sector members of the Government Facilities sector.

With the first of these three criteria, CISA is seeking reporting from SLTT Government Entities from jurisdictions over a certain size. Consideration of the factors

enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of larger SLTT Government Entities in the description of covered entity. Regarding the first factor, it is likely that the disruption or compromise of only some of the largest SLTT Government Entities have the potential to cause significant consequences on a large enough scale to impact national security, economic security, and, especially, public health and safety. SLTT Government Entities are responsible for numerous NCFs within their jurisdictions, overseeing functions such as developing and maintaining public works and services, preparing for and managing emergencies, and preserving constitutional rights. Similarly, along with their Federal counterparts, SLTT Government Entities like State Departments of Health provide a wide variety of services that are critical to the public health and well-being of their citizenry.

As to the second factor CISA is to consider, i.e., the likelihood that such an entity will be targeted by a malicious cyber actor, SLTT Government Entities are frequently impacted by cyber incidents.[249] Furthermore, the 2024 Homeland Security Threat Assessment indicates that SLTT Government Entities are likely to remain the targets of foreign governments, such as Russia and China.[250]

Third, damage or disruption to various SLTT Government Entities have the potential to disrupt the reliable operation of critical infrastructure. SLTT Government Entities own or operate critical infrastructure across various sectors, to include energy, water, transportation, and emergency services among others. Damage or disruption of these entities has potential to directly impact the reliable operation of critical

---

[249] See, e.g., *Verizon 2022 DBIR*, *supra* note 181, at 50 (public administration entities experienced the second largest number of reported incidents); *IBM 2023 Threat Index*, *supra* note 217, at 42 (listing Government as the eighth most impacted industry).

[250] See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20 ("Russian government-affiliated cyber espionage likely will remain a persistent threat to federal, state, and local governments [and] Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including . . . government facilities.").

infrastructure and to create the potential for cascading impacts affecting the reliable operations of other critical infrastructure as well.

For the same reasons that CISA is proposing to limit the Emergency Services Sector sector-based criteria to entities that serve populations equal to or greater than 50,000 individuals (see Section IV.B.iv.2.e), CISA is proposing to use the same small government jurisdiction threshold to demark which SLTT jurisdictions' government entities will be required to report. CISA believes that this line of demarcation, which would provide regulatory relief to more than two-thirds of counties and over 95% of cities from which CISA could require reporting under the statutory definition of covered entity, should cover enough entities to provide sufficient data for CISA to perform cyber incident trend and threat analysis for this vital community.

With the second of these criteria—covering LEAs, ESAs, and SEAs with student populations of 1,000 or more students, as well as IHE that receive funding under Title IV of the Higher Education Act—CISA seeks to ensure reporting from a sufficient cross-sector of entities to understand and be able to share information on threats to our nation's education facilities. Consideration of the factors enumerated in 6 U.S.C 681b(c)(1) supports the inclusion of these entities within the description of covered entity, especially the second factor related to threat.

As noted in the 2024 Homeland Security Threat Assessment, "[Kindergarten through 12th grade (K-12)] school districts have been a near constant ransomware target due to school systems' IT budget constraints and lack of dedicated resources, as well as ransomware actors' success at extracting payment from some schools that are required to function within certain dates and hours."[251] The Verizon 2022 DBIR and the IBM 2023 Threat Index both identified education facilities as the sixth most frequently impacted

[251] See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 18.

industry in 2022.[252] A recent U.S. GAO report on cybersecurity at K-12 schools echoed this conclusion, stating that "research from several federal and private sector sources indicate that cyber threats [against K-12 schools] have escalated over time, and are becoming more sophisticated and pervasive."[253] Many Education Subsector entities, primarily IHE, also own infrastructure or perform activities that support national security, public health and safety, and the reliable operations of critical infrastructure, such as hospitals, first responder organizations, water and wastewater treatment facilities, energy facilities, and research facilities.

To obtain reporting from a representative cross-section of Education Subsector entities, CISA proposes two prongs to the criterion for this subsector, one focused on the K-12 community and one focused on IHE. For the K-12 community, CISA proposes to require reporting from LEAs, ESAs, and SEAs, as defined in 20 U.S.C. 7801 (part of the Elementary and Secondary Education Act, as amended (20 U.S.C. 6301 *et seq*.)), with a student population of 1,000 or more students. LEAs, more commonly referred to as school districts, are the public authorities legally constituted within a State for administrative control or direction of public schools in a city, county, township, school district, or other political subdivision of a State.[254] SEAs are the Statewide board of education or other agency or officer primarily responsible for the supervision of schools within a state.[255] ESAs are state-authorized regional service centers that often provide direct education service delivery to schools and districts in their respective regions.

CISA proposes to require reporting from LEAs, SEAs, and ESAs with student populations of 1,000 or more students. This threshold would capture in the description of

---

[252] *Verizon 2022 DBIR*, *supra* note 181, at 50; *IBM 2023 Threat Index*, *supra* note 217, at 42.
[253] U.S. GAO, *GAO-23-105480, Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity* at 12 (2022), available at https://www.gao.gov/products/gao-23-105480.
[254] 34 CFR 303.23.
[255] 34 CFR 300.41.

covered entities all SEAs, approximately half of all LEAs, and some percentage of ESAs, with smaller LEAs and ESAs excluded from the reporting population.[256]

CISA is proposing this threshold, which is limited to LEAs, SEAs, and ESAs, with larger student populations, for three primary reasons. First, studies show that "larger school districts (as defined by student enrollment) appear to be at a significantly greater risk for experiencing a cyber incident than small school districts."[257] Second, covered cyber incidents impacting education agencies with larger student populations will, on average, have a greater likelihood of impacting more individuals, thus potentially causing more substantial impacts than incidents perpetrated against education agencies with smaller student populations. Finally, similar to the use of the small government jurisdiction definition as a threshold line of demarcation for other SLTT Government Entities, CISA believes this approach will afford regulatory relief to smaller entities that are likely to have fewer resources with which to comply with CIRCIA's incident reporting requirements, while still requiring reporting from a broad enough population to provide sufficient data for CISA to perform cyber incident trend and threat analysis for this community.

In developing this criterion and threshold, CISA considered various alternatives, including (1) covering LEAs, SEAs, and ESAs with student populations of 2,500 students or more; (2) using the same small government jurisdiction threshold CISA is proposing to use for other SLTT Government Entities and entities required to report under the Emergency Services Sector sector-based criteria (i.e., entities serving jurisdictions with a

---

[256] All SEAs (56 of 56) and approximately 52% of LEAs (6,911 of 13,318) have student populations of 1,000 or more students. See National Center for Education Statistics, 2022 Digest of Education Statistics, Table 214.20, available at https://nces.ed.gov/programs/digest/d22/tables/dt22_214.20.asp. As the student population covered by each ESA is not readily available, to be conservative, for purposes of the CIRCIA RIA, CISA is assuming all 553 ESAs serve student populations of 1,000 or more students.

[257] Douglas Levin, *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report* at 15, available at https://www.k12six.org/the-report.

population of 50,000 or more individuals); and (3) requiring reporting from all LEAs, SEAs, and ESAs.

The first alternative CISA considered was establishing a higher threshold based on student population, specifically one that would require reporting from LEAs, SEAs, and ESAs with 2,500 or more students. Setting the threshold at 2,500 students would result in approximately 30% of all LEAs, SEAs, and ESAs collectively qualifying as covered entities.[258] The primary benefit of this threshold, in comparison to the proposed 1,000 student threshold, would be the lower costs to the K-12 community resulting from having fewer entities qualify as covered entities. However, an analysis conducted by the Department of Education based on cyber incidents impacting the K-12 community that were voluntarily reported to CISA in 2023 showed that the greatest percentage of incidents impacting the K-12 community impacted school districts with between 1,000 and 2,500 students (around approximately 30% of all incidents). This represents the largest percentage of incidents experienced by any of the size-based segments of the K-12 community analyzed by the Department of Education.[259] Given the large percentage of cyber incidents impacting school districts with between 1,000 and 2,500 students, CISA believes the small additional burden imposed on the sector by requiring reporting from education agencies with between 1,000 and 2,500 students that experience a substantial cyber incident or make a ransom payment is outweighed by the benefit of the additional insight into cybersecurity threats targeting the K-12 community that this

---

[258] All SEAs (56 of 56) and approximately 28% of LEAs (3,726 of 13,318) have student populations of 2,500 or more students. See National Center for Education Statistics, 2022 Digest of Education Statistics, Table 214.20, available at https://nces.ed.gov/programs/digest/d22/tables/dt22_214.20.asp. As the student population covered by each ESA is not readily available, to be conservative, for purposes of the CIRCIA RIA, CISA is assuming all 553 ESAs serve student populations of 2,500 or more students.

[259] Department of Education analyzed the incidents experienced by K-12 school districts with the following size-based segments: 25,000 or more students; 10,000-24,999 students; 5,000-9,999 students; 2,500-4,999 students; 1,000-2,499 students; 600-999 students; 300-599 students; 1-299 students; and no size reported. Even combining some of the other segments, the 1,000-2,499 students segment still experienced a greater percentage of the analyzed incidents than other segments (e.g., more than all of the smaller segments combined, more than the 2,500-4,999 and 5,000-9,999 students segments combined, and more than the 10,000-24,999 and 25,000 or more students segments combined).

additional coverage would provide. Thus, CISA has elected to propose setting the student population threshold at 1,000 students, and not 2,500 students. CISA acknowledges that it may be possible to set this threshold at 2,500 students and get some reporting that would be informative to the overall subsector; however, CISA does not believe this will result in representative or adequate reporting for the subsector because it would not include the population that is most likely to be targeted by malicious actors based on the Department of Education's analysis. Nonetheless, CISA is interested in receiving comments on the proposal to set the threshold at 1,000 students versus 2,500 students for this subsector, and what benefits or disadvantages may exist for selecting one threshold over another.

Regarding the second alternative considered—i.e., using the same jurisdiction-based threshold that CISA is proposing for other SLTT Government Entities—CISA sees value in using the same threshold across all SLTT Government Entities, which includes LEAs, SEAs, and ESAs. Doing so would avoid potential confusion resulting from having different thresholds for different types of SLTT Government Entities. However, based on consultations with the Department of Education, CISA understands that school districts frequently do not follow typical county, city, or other jurisdictional lines, with many LEAs and ESAs covering schools that are located in multiple jurisdictions. As a result, the number of individuals within a given LEA's or ESA's "jurisdiction" may not be readily available or discernable, causing many LEAs and ESAs to have difficulties in determining if they meet a criterion based on the number of individuals located within their "jurisdiction." Conversely, student population is a standard metric used within the K-12 community for various purposes and is a metric with which every LEA, SEA, and ESA should be very familiar. As an entity's ability to determine whether it is a covered entity is crucial to implementation of the proposed regulation, CISA believes it is preferable to use a student population-based metric for the K-12 community rather than

the jurisdictional population-based metric CISA is proposing for the sector-based criteria for other SLTT Government Entities.

Regarding the final alternative considered—i.e., covering all LEAs, SEAs, and ESAs—there are some arguments in favor of broader reporting requirements, such as the frequency with which educational entities are subjected to cyber incidents and the absence of any other nationwide cyber incident reporting requirements for this community. Ultimately, however, CISA decided that, for the same reasons CISA is proposing a size threshold for the sector-based criteria for other SLTT Government Entities and several other sectors and subsectors, proposing a size threshold for the sector-based criteria for the K-12 community is the most well-supported approach. Doing so not only supports general consistency in approach across the SLTT Government Entities' community, but also promotes the correct balance between burden and ensuring sufficient reporting from this community.

CISA is interested in receiving comments on this prong of the proposed sector-based criteria, to include:

14. Whether CISA should include a size threshold for education agencies that would be required to report and, if so, what metric (e.g., student population; number of individuals within the jurisdiction) should be used as the unit or measurement for the threshold.
15. If CISA were to include a criterion for education agencies using a size threshold based on student population, whether 1,000 students, 2,500 students, or another number of students would be the optimal threshold for this subsector criterion and why.
16. Whether CISA should include a criterion to require reporting from some or all private schools operating in the K-12 space, as cyber incidents impacting K-12 private schools would not be subject to reporting under the current proposal

(unless they qualify as a covered entity under the general size-based threshold) since LEAs, SEAs, and ESAs do not have authority over private schools.

The Government Facilities Education Subsector sector-based criteria would also include in the description of covered entity those IHE that receive funding under Title IV of the Higher Education Act (Title IV). In addition to being part of a routinely targeted subsector, given the diverse roles IHE can play in various NCFs, the consequences of a covered cyber incident impacting an IHE could be significant. For example, some IHE provide research or other support to national security entities such as DOD and DHS, others are high-risk chemical facilities regulated under CFATS. While some IHE might be covered by the Applicability section based on other sector-based criteria, CISA believes it is important to require reporting from IHE more broadly.

IHE that receive funding under Title IV include any IHE—be it a college or university that offers a 2-year or 4-year degree, a trade school, or other type of IHE—that offers Federal financial aid to its students. This includes the majority of IHE, ensuring that CISA will receive adequate reporting to identify cybersecurity trends for the entire IHE community. Title IV-funded IHE also already are subject to cybersecurity incident reporting requirements under the Gramm-Leach-Bliley Act, but that is limited to reporting to the Department of Education cybersecurity incidents resulting in unauthorized access to student information. This proposal will expand the scope of reporting required of these IHE to reporting on a broader range of cybersecurity incidents and any ransom payments made by these entities.

With the third proposed Government Facilities Sector sector-based criteria—entities that manufacture, sell, or provide managed service for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments, including but not limited to voter registration databases; voting systems; and ICT used to report, display, validate, or

finalize election results—CISA is seeking to ensure sufficient reporting to understand cyberthreats to our nation's elections infrastructure and assist SLTT election officials and their private sector partners to prevent, respond to, and mitigate impacts of cyber incidents impacting elections infrastructure. In January 2017, DHS officially designated election infrastructure as a critical infrastructure subsector of the Government Facilities Sector.[260] In this designation, the Department stated that the United States' election infrastructure is vital to our national interest and must be a priority for cybersecurity assistance and protections provided by the Department.[261]

Election infrastructure refers to storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and ICT systems used to manage the election process and report and display results on behalf of SLTT governments. Such ICT systems include, but are not limited to, voter registration databases and other systems used to manage the voter registration process and maintain voter registration data; electronic poll books; voting systems, election management systems, and other systems used to create, print, facilitate the voting of, and tabulate ballots, including electronic ballot delivery, marking, and return systems, as well as systems used to validate, audit, certify, or otherwise finalize election results; and public information systems used to display election information and results to the public, including SLTT election websites and election night reporting systems. These and other types of technologies used to manage the election process are described in greater detail in the Election Infrastructure SSP.[262]

---

[260] See Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), available at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (hereinafter "Statement by Secretary Jeh Johnson").

[261] *Id.*

[262] *Election Infrastructure Subsector-Specific Plan: An Annex to the NIPP 2013* (2020), available at https://www.cisa.gov/sites/default/files/publications/election_infrastructure_subsector_specific_plan.pdf.

Currently, entities that manufacture, sell, or provide managed services for ICT specifically used to support election processes are not subject to any Federal cyber incident reporting requirements. Consequently, in conjunction with the first Government Facilities Sector sector-based criterion, which would require reporting from SLTT election entities for jurisdictions with populations greater than 50,000 individuals, CISA believes this third Government Facilities Sector sector-based criterion focused on private sector members of the Election Infrastructure Subsector is necessary to ensure CISA and its Federal partners receive sufficient reporting from both public and private sector entities within the Elections Infrastructure Subsector to understand the cyber threats to elections infrastructure.

CISA believes that including these entities in the description of covered entity is supported by a consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) (i.e., consequence, threat, and disruption of reliable operation of critical infrastructure). While damage or disruption of election infrastructure may not directly produce national security, economic security, or public health and safety consequences, the impact of eroded public confidence in our election system may indirectly lead to such consequences.[263] Damage, destruction, or unauthorized access to elections infrastructure would impact the reliable operation of critical infrastructure as certain systems and assets of election infrastructure themselves are critical infrastructure.[264] Finally, malicious cyber actors have targeted and are expected to continue to target elections infrastructure.[265]

---

[263] See *Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol* (Dec. 22, 2022), available at https://www.govinfo.gov/app/details/GPO-J6-REPORT/.

[264] Statement by Secretary Jeh Johnson, *supra* note 260 ("Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.").

[265] See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 19 ("Our electoral processes remain an attractive target for many adversaries, and we expect many of them will seek to influence or interfere with the 2024 election . . . Cyber actors likely will seek to exploit election-related networks and data, including state, local, and political parties' networks and election officials' personal devices and e-mail accounts. . . . Though we continue to strengthen the integrity of our elections infrastructure, cyber actors, both government-affiliated and cyber criminals, likely will remain opportunistic in their targeting of

CISA recognizes that many standard ICT, such as laptops, cell phones, email, staff management and payroll software, and business and data management software may be used by entities responsible for the conduct and management of elections. CISA does not intend for this sector-based criterion to capture entities that manufacture, sell, or provide managed services related to those types of ICT, except to the extent that they are specifically used for election processes. Thus, for example, while an entity that develops, sells, or provides managed services related to software specifically designed to facilitate the management of temporary election workers would be considered a covered entity under this proposed criterion, a standard staff management and payroll software provider would not be considered a covered entity simply because an SLTT election office uses the software to conduct routine business.

i. Healthcare and Public Health Sector

CISA proposes to include in the description of covered entity[266] multiple sector-based criteria related to the Healthcare and Public Health Sector. As its name implies, entities within the Healthcare and Public Health Sector, along with Federal and SLTT Departments of Health and similar government entities that are part of the Government Facilities Sector, are essential to the maintenance of the public health of the nation, providing goods and services that are integral to maintaining local, national, and global health security. Entities within the sector provide various services, to include direct patient care, medical equipment and materials, laboratory support, health IT, health plans, and mass fatality management services.[267]

---

election-related networks and data, routinely attempting to exploit misconfigured or vulnerable public-facing websites, webservers, and election-related information technology systems.").

[266] CISA is aware that covered entity also is a defined term in the HIPAA regulations. As noted in the proposed § 226.1, the definitions included in this proposed rule are "[f]or the purposes of this Part." Whenever the term covered entity is used in this document, it is referring to the statutory term in CIRCIA and/or the proposed definition of covered entity in the CIRCIA proposed rule, and not to entities that meet the existing HIPAA regulatory definition of covered entity or any other existing definition of the term covered entity.

[267] See *Healthcare and Public Health SSP*, *supra* note 173.

Unfortunately, entities within this sector routinely experience cyber incidents, with U.S. healthcare entities experiencing the seventh most cyber incidents of any industry in 2022.[268] Many entities within the sector currently are required to report certain cyber incidents to HHS under the HIPAA Breach Notification Rule (45 CFR 164.400-414) and to the Federal Trade Commission under the HITECH Act Health Breach Notification Rule (16 CFR 318); however, those requirements are generally focused solely on data breaches and do not require reporting of other types of cyber incidents that do not involve unauthorized acquisition of or access to personal health information. Device manufacturers, importers, distributors, and user facilities must establish and maintain records, make such reports, and provide such information, as the Secretary of Health and Human Services may by regulation reasonably require to assure that such device is not adulterated or misbranded and to otherwise assure its safety and effectiveness. 21 U.S.C. 360i(a). FDA's regulations at 21 CFR Part 803 require device manufacturers and importers, to report certain device-related adverse events and product problems, including those caused by cyber incidents, to the FDA, but that reporting requirement is limited to situations where a device is likely to or has caused or contributed to a death or serious injury or for medical device manufacturers and importers when they initiate a correction or removal of a medical device to reduce a risk to health posed by the device. In light of the sector's broad importance to public health, the diverse nature of the entities that compose the sector, the historical targeting of the sector, and the current lack of required reporting unrelated to data breaches or medical devices, CISA proposes requiring reporting from multiple parts of this sector.

The first criterion CISA proposes related to this sector will mean that certain entities providing direct patient care will be considered covered entities. Specifically, CISA proposes including in the description of covered entity any entity that owns or

[268] See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.

operates (1) a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or (2) a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1). Many different types of entities provide direct care to patients, such as hospitals, clinics, urgent care facilities, medical offices, surgical centers, rehabilitation centers, nursing homes, and hospices. The size of the facilities, the number of patients cared for daily, and the types of services provided can vary dramatically across these entities. While all of these various types of entities contribute to the nation's public health and well-being, CISA does not believe it is prudent or cost-effective to require covered cyber incident and ransom payment reporting from every individual provider of patient care. Rather, CISA is proposing to focus on hospitals, as they routinely provide the most critical care of these various types of entities, and patients and communities rely on them to remain operational, including in the face of cyber incidents affecting their devices, systems, and networks to keep them functioning.

Currently, there are approximately 6,000 hospitals in the United States.[269] CISA is proposing requiring reporting from larger hospitals (i.e., those with more than 100 beds) and critical access hospitals. CISA believes it is worthwhile to focus on larger hospitals for required reporting, as they are more likely than smaller hospitals to experience substantial impacts if they fall victim to a covered cyber incident given their size and the correspondingly greater number of patients they are caring for on any given day. Additionally, focusing on larger hospitals is supported by much of the same rationale behind CISA's decision to propose an overall size-based criterion based on the SBA small business size standards in the Applicability section (e.g., larger hospitals are more likely to have in-house or access to cyber expertise; larger hospitals are likely to be better equipped to simultaneously respond to and report a cyber incident).

---

[269] See American Hospital Association, *Fast Facts on U.S. Hospitals*, https://www.aha.org/statistics/fast-facts-us-hospitals (last visited July 31, 2023).

While CISA is not generally proposing to require reporting from smaller hospitals, CISA is proposing to require reporting from critical access hospitals. Critical access hospitals are facilities that have been certified by the Centers for Medicare & Medicaid Services as meeting certain criteria, including that they are located in a state that has established a Medicare rural hospital flexibility program, and that they are designated as a critical access hospital by the State in which they are located, among other requirements.[270] CISA is proposing to include these in the reporting requirements as they typically are the only source of emergency medical care for individuals living within certain rural areas. As a result, a substantial cyber incident at a critical access hospital may have disproportionate impacts to its size given the limited alternative emergency health care options for individuals within its service area.

The second public health and healthcare sector sector-based criterion CISA is proposing would require reporting from manufacturers of drugs listed in Appendix A of the report *Essential Medicines Supply Chain and Manufacturing Resilience Assessment,* sponsored by the U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR).[271] In this report, ASPR, in collaboration with governmental and non-governmental entities, prioritized 86 essential medicines identified as either critical for minimum patient care in acute settings or important for acute care or important for acute care of respiratory illnesses/conditions, with no comparable alternative available. The report was published in response to a commitment by the Biden Administration, in its June 2021 100-day review of the pharmaceutical supply chain as tasked in Executive Order 14017, to "assemble a consortium of public health experts (including emergency medicine and critical care) in

---

[270] See section 1820(e) of the Social Security Act and 42 CFR 485.601 et seq.
[271] ARMI, *Essential Medicines Supply Chain and Manufacturing Resilience Assessment* (May 2022), available at https://www.armiusa.org/wp-content/uploads/2022/07/ARMI_Essential-Medicines_Supply-Chain-Report_508.pdf; see also ASPR, *Essential Medicines Report Now Available* (May 23, 2022), available at https://aspr.hhs.gov/newsroom/Pages/Essential-Medicines-May22.aspx.

the government, non-profit, and private sector to review [a previous list of Essential Medicines, Medical Countermeasures, Critical Inputs developed by FDA in response to Executive Order 13944], and recommend 50-100 drugs that are most critical to have available at all times for U.S. patients because of their clinical need and lack of therapeutic redundancy."[272] Given the importance of these products, CISA believes it is appropriate to include manufacturers of these products among the CIRCIA covered entity population in order to enable the Federal government to more quickly identify any emerging cyberthreats against them.

Third, CISA is proposing to require reporting from manufacturers of Class II (moderate risk) and Class III (high risk) devices, as defined in 21 U.S.C. 360c. FDA has established classifications for approximately 1,700 different generic types of devices, each of which is assigned to one of three regulatory classes based on the level of control necessary to provide reasonable assurance of the safety and effectiveness of the device.[273] These classifications are risk-based, with Class I devices presenting the lowest risk and Class III devices presenting the greatest risk.[274] Based on discussions with FDA, CISA believes that requiring reporting from manufacturers of Class II and III devices provides a risk-based means balancing reporting from medical device manufacturers while supporting the collection of an adequate amount of reporting to understand cyber threats, vulnerabilities, and TTPs for this industry segment.

CISA believes that the inclusion of all three Healthcare and Public Health Sector sector-based criteria is supported by a consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) (i.e., consequence, threat, and disruption of the reliable operation of critical infrastructure). Regarding the first factor, consequence, disruption or compromise

---

[272] Dep't of Health & Human Servs., *Review of Pharmaceuticals and Active Pharmaceutical Ingredients* at 243 (June 2021), available at https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.
[273] See FDA, *Classify Your Medical Device*, https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device (last visited July 24, 2023).
[274] See *id.*

at any of these key sector assets has the potential for significant impacts to public health and safety. All hospitals play an important role in public health, but disruption or compromise impacting any of the hospitals CISA proposes to cover could have especially significant impacts on public health given the number of patients and types of services provided at large hospitals, and the fact that critical access hospitals may be the only source of emergency care in their immediate vicinity, sometimes for hundreds of miles. Similarly, a compromise or disruption resulting in unavailability, supply shortages, or compromise of essential medicines, medical countermeasures, or Class II and III medical devices has a significant potential for creating public health consequences on a scale that could impact all Americans. Regarding the second factor, threat, entities within the Healthcare and Public Health sector routinely experience cyber incidents.[275] The DHS 2024 Homeland Security Threat Assessment indicates that threats against this sector include Russian and Chinese government-affiliated actors, who are likely to continue to target the healthcare and public health sector.[276] Finally, regarding the third factor, the disruption of the reliable operation of critical infrastructure, the entities that would be covered under the criteria— large hospitals; critical access hospitals; manufacturers of essential medicines; and manufacturers of Class II and III medical devices—typically themselves are considered critical infrastructure. Moreover, as the COVID-19 pandemic demonstrated, significant events impacting the public health can have cascading affects that threaten the reliable operation of critical infrastructure across multiple sectors.

In establishing these proposed criteria, CISA also considered including criteria related to health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities. Ultimately, CISA determined it was not necessary to include specific sector-based criteria for any of those three industry

---

[275] See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.
[276] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

segments. In the case of health insurance companies and entities operating laboratories or other medical diagnostics facilities, CISA believes a sufficient number of entities already will be captured under the size-based criterion that applies across all critical infrastructure sectors. However, if as a result of public comment, CISA determines that it must modify or eliminate any aspect of the description of covered entity through which health insurance companies and entities operating laboratories or other medical diagnostics facilities are currently captured as part of this proposed rule, including the size-based criterion, CISA may incorporate a sector-based criterion or multiple criteria focused on criteria capturing these entities as part of the final rule to ensure that they remain covered entities. If CISA were to include one or more sector-based criteria that would cover health insurance companies and laboratories and other medical diagnostics facilities, it would likely set a threshold based on annual revenue, number of employees, or some other metric and only entities that exceed the threshold would be considered covered entities. Such a threshold would be set by CISA to ensure that the largest of these types of entities would be considered covered entities and CISA likely would look at the SBA Size Standards for context and to develop relevant averages using NAICS codes applicable to such entities and may consult with the Healthcare and Public Health SRMA to develop the final criterion or criteria. Regarding the health IT community, CISA believes that the most common type of cyber incident such entities will face are data breaches. As data breaches are not the primary focus of CIRCIA, and those entities already are required to report data breaches of unsecured protected health information under the HIPAA Breach Notification Rule and personal health records under the HITECH Act Health Breach Notification Rule, CISA does not believe it is necessary to include a specific criterion focused on entities in the health IT industry.

CISA would be interested in receiving comments on:

17. The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria.
18. The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities.

j. Information Technology Sector

CISA proposes including within the description of covered entity any entity that meets one or more of four proposed Information Technology (IT) Sector sector-based criteria. First, CISA proposes including within the description of covered entity any entity that knowingly provides IT hardware, software, systems, or services to the Federal government. Second, CISA proposes including within the description of covered entity any entity that has developed and continues to sell, license, or maintain any software that meets the definition of "critical software" as that term was defined by NIST pursuant to Executive Order 14028 – Improving the Nation's Cybersecurity (May 12, 2021). Third, CISA proposes to include within the description of covered entity, any entity that is an original equipment manufacturer (OEM), vendor, or integrator of OT hardware or software components. Fourth, CISA proposes to include within the description of covered entity any entity that performs functions related to domain name operations.

To conduct a cyber incident, malicious cyber actors seek to exploit some aspect of the IT Sector, through IT hardware, software, systems, or services. Moreover, given many IT providers' positions in the critical infrastructure supply chain, their roles as cyber service providers (e.g., CSPs, managed service providers) to other entities, and their important role in the functioning of the internet, a covered cyber incident impacting a member of the IT Sector has the potential to cause significant cascading impacts to tens,

hundreds, or even thousands of other entities. As a result, requiring incident reporting from a broad range of IT Sector entities is essential to developing a complete picture of the cyber threat landscape, identifying vulnerabilities that adversaries are exploiting, and sharing early warnings to better protect entities from across all critical infrastructure sectors.

The IT Sector is comprised of hundreds of thousands of companies, ranging from small businesses to large, multinational enterprises. While some of these companies are likely to be captured by the proposed CIRCIA size-based threshold, many will not be. Additionally, as opposed to many other critical infrastructure sectors with a primary regulatory agency providing oversight or a small number of clearly identifiable subsectors, industry segments, or entity types, the IT sector to a large extent lacks any of these easy means of categorization or segmentation. Given these characteristics, CISA believes it is necessary to take a multi-criteria approach including a general criterion focused on entities that knowingly provide IT hardware, software, systems, or services to the Federal government, as well as criteria designed to capture critical software, OT, and DNS services that are not used by the Federal government.

For the first IT Sector sector-based criterion, CISA is proposing to include any entity that knowingly provides or supports IT hardware, software, systems, or services to the Federal government either directly or through a reseller. CISA believes this proposed approach will be beneficial in several ways. First, in light of both the essential services provided to the nation by various Federal entities, as well as the symbolic value of the Federal government, Federal entities often are desired targets for attack, and a covered cyber incident impacting a Federal entity can result in significant consequences. Second, because an entity selling a good or service to the Federal government typically will know if it has provided a product or service to the Federal government, the proposed criterion is intended to create a clear and easy manner for an entity within the IT sector to determine

if it is a covered entity. This criterion also would include, for example, some entities that provide IT hardware, software, systems, or services to the Federal government through a reseller or by providing software development services, such as a code repository service. It is for this reason CISA proposes capturing in this criterion IT hardware, software, system, or service providers that provide their products to the Federal government only if they knowingly do so, e.g., if they provide goods to the Federal government through a procurement contract or another agreement or transaction. Third, given the breadth of the Federal government and the large number of different IT products and services it employs, CISA expects this criterion to cover a broad spectrum of entities from the IT sector, which will help ensure CISA receives adequate reporting to achieve its responsibilities under CIRCIA as they relate to the IT sector and beyond.

Note, however, while CISA is proposing to use the provision of software, hardware, systems, or services to the Federal government as a criterion for determining who must report, reporting for those entities that meet this sector-based covered entity criteria is not limited to incidents impacting the products or services they provide to the U.S. Government. Rather, an entity that meets this sector-based criteria must report any covered cyber incident it experiences regardless of whether it impacts any of their Federal customers or the specific products or services used by their Federal customers.

CISA acknowledges that entities routinely change their offerings and customers over time, and that there will be entities who have provided software, hardware, systems, or services to the Federal government at one point but no longer do so (either because they no longer offer or support that software, hardware, system, or service at all, or because their arrangement with their Federal customer(s) has ended). In recognition of this, CISA is proposing that an entity would be captured under this criterion only for as long as the entity continues to sell, provide, or provide support for the product or service they have sold to the government, or any updated versions thereof. If a software,

hardware, or system manufacturer or supplier no longer sells or supports the software, hardware, or system that it previously sold to the government, or any updated versions thereof, then it would no longer be considered a covered entity based on this criterion in relation to that particular software, hardware, or system. Similarly, if an IT service provider no longer provides any services to the Federal government, it would not remain a covered entity simply on the basis of having previously provided IT services to the Federal government.

In the second IT sector-based criterion, CISA proposes covering any entity that has developed and continues to sell, license, or maintain any software that meets the definition of "critical software" established by NIST pursuant to Executive Order 14028. On May 12, 2021, President Biden issued Executive Order 14028, with the goal of improving government efforts to identify, deter, protect against, detect, and respond to the persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and the American people's security and privacy. Section 4 of Executive Order 14028 is focused on software supply chain security, with Section 4(g) instructing NIST, in consultation with designated Federal partners, to develop a definition of the term "critical software." The Federal government would then use the definition of critical software to support the development of a list of software categories and products that would be subject to the additional security activities set forth in the Executive Order, including how the Federal government purchases and manages deployed critical software. In particular, the Executive Order seeks to limit Federal acquisition to software that has met security measures such as use of a secure development process and integrity checks defined in Section 4(e) of the Executive Order.

To develop the definition of critical software, NIST solicited position papers from the IT community, hosted a virtual workshop to gather input, and consulted with CISA, the Office of Management and Budget (OMB), the Office of the Director of National

Intelligence, and the National Security Agency (NSA). Ultimately, NIST defined critical software to be "any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: (1) is designed to run with elevated privilege or manage privileges; (2) has direct or privileged access to networking or computing resources; (3) is designed to control access to data or operational technology; (4) performs a function critical to trust;[277] or, (5) operates outside of normal trust boundaries with privileged access."[278] The definition applies to software of all forms (e.g., standalone software; software integral to specific devices or hardware components; cloud-based software) purchased for, or deployed in, production systems and used for operational purposes.[279] Other use cases, such as software solely used for research or testing that is not deployed in production systems, are outside of the scope of this definition.[280]

Given the purposes for which this definition of critical software was developed (i.e., to support the enhancement of software supply chain security), the informed process that led to its development, and its familiarity to the IT community, CISA believes it to be an appropriate basis for narrowing down the scope of entities engaged in software development for non-Federal government customers included within the description of covered entity. However, because the "critical software" definition has not been formally codified into law or regulation, CISA is proposing to incorporate the definition of "critical software" developed by NIST directly into the regulatory text rather than by

---

[277] According to NIST, the term "critical to trust" covers "categories of software used for security functions such as network control, endpoint security, and network protection." NIST, *Critical Software Definition – FAQs*, FAQ 3, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-faqs#Ref_FAQ3 (last visited Jan. 26, 2024).
[278] See NIST, *Critical Software – Definition & Explanatory Material*, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory (last visited July 24, 2023).
[279] *Id.*
[280] *Id.*

reference, to provide potential covered entities with certainty on the scope of this prong of the IT Sector sector-based criteria.[281]

CISA is also proposing to limit this criterion to entities that continue to sell, license, or maintain critical software. While CISA intends to capture under this criterion entities that continue to be in the business of providing critical software, CISA does not intend to capture former critical software developers in perpetuity if they no longer produce the software. However, to the extent that a critical software developer continues to sell (directly or indirectly), license, or otherwise maintain previously developed critical software, it would continue to be a covered entity under this prong.

For the third IT Sector sector-based criterion, CISA is proposing to include in the description of covered entity any entity that is an OEM, vendor, or integrator of OT hardware or software components. According to NIST,[282] OT is defined as "Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, Fire control systems, and physical access control mechanisms."[283]

OT components are considered vital to the operation of U.S. critical infrastructure, and the security of OT is essential for the achievement of a secure and resilient infrastructure for the American people.[284] The increasing convergence of IT and

---

[281] Additional information on the software categories considered to be critical software, the types of products typically included, and the rationale for their inclusion, can be found at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory (last visited Nov. 28, 2023).

[282] In various places throughout this document, CISA references definitions and guidance found in materials published by NIST. CISA believes it is appropriate to use NIST publications as source references given NIST's status as a widely recognized and accepted source of cybersecurity information and best practices by and for both industry and government.

[283] NIST, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160 Vol. 2 Rev. 1, at 65 (Dec. 2021), available at https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final.

OT creates opportunities for exploitation that could result in catastrophic consequences, including loss of life, economic damage, and disruption of the NCFs upon which society relies.[285] In light of this, CISA believes it is important to understand the cyberthreat environment related to OT and to receive reports on cyber incidents involving manufacturers or developers of OT products.

OT is typically used in manufacturing and distribution industries, such as electric, water and wastewater, oil and natural gas, chemical, and pharmaceutical manufacturing and distribution. Consequently, the first IT sector-based criterion—focusing on entities that provide hardware, software, systems, or services to the Federal government—may not capture many OT OEMs, vendors, or integrators, resulting in the need for this third criterion.

For the fourth IT Sector sector-based criteria, CISA proposes to include in the description of covered entity certain entities that perform functions related to domain name operations. These are entities whose activities are key to the fabric of the internet, enabling users to access resources on the internet and organizations to provide services online. The criterion is intended to capture entities that perform these functions for the benefit of their customers, business partners, or internet users generally. A successful covered cyber incident perpetuated against such entities could have significant potential consequences not just to the entity itself but also entities across all critical infrastructure sectors that rely upon domain name resolution for their business operations and for the provision of their resources online. In addition, the significance of these entities to enabling navigation of the internet and the potential for compromising one entity in order to impact multiple internet users makes these entities a target for malicious cyber activity.

---

[284] See *id.* at 1; see also CISA, *Securing Industrial Control Systems: A Unified Initiative – FY 2019-2023*, at 2 (July 2020) (hereinafter, "*Securing Industrial Control Systems*"), available at https://www.cisa.gov/resources-tools/resources/securing-industrial-control-systems.
[285] *Securing Industrial Control Systems*, *supra* note 284, at ii.

Given their importance to the use of the internet and therefore the potential impacts—to national security, economic security, and public health and safety, as well as to disruption of the reliable operation of critical infrastructure—of a cyber incident perpetrated against such entities, and the attractiveness of such entities to malicious cyber actors, CISA is proposing to include these entities within the definition of covered entities.

CISA believes the inclusion of these four IT sector-based criteria is supported by an analysis of the three factors enumerated in 6 U.S.C. 681b(c)(1) (i.e., consequence, threat, and likelihood of disruption of the reliable operation of critical infrastructure). First, the disruption to or compromise of any of the entities covered by the proposed criteria for the IT sector has the potential to cause national security, economic security, or public health and safety. This is particularly true for entities that provide or support hardware, software, or services to the Federal government, given the essential role the Federal government has in national security, economic security, and public health and safety. This same rationale is also applicable to entities that develop, license, or sell "critical software"; entities that serve as OEMs, vendors, or integrators of OT; and entities that perform functions related to domain name operations. Critical software and OT frequently are used by entities and systems in a wide variety of critical infrastructure, such as water systems, commercial nuclear power reactors, telecommunications facilities, power grids, airports, and hospitals, that, if disrupted or compromised through the supply chain for these software and technologies, could directly impact national security, economic security, and public health and safety. By definition, critical software operates in a position that provides the software extensive privileges, access, or trust, the compromise of which could be significantly consequential to the systems and networks where they are used, including critical infrastructure systems and networks. OT is used to directly perform a multitude of critical infrastructure functions, such as generating electricity, monitoring and controlling water, and distributing natural gas. As described

above, entities that perform functions related to domain name operations play a key role in ensuring the accessibility and security of online services used by entities in a critical infrastructure sector, which may include critical services that depend on those services. For these same reasons, consideration of the third statutory factor—the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure—strongly supports the inclusion of these entities within the description of covered entity. Finally, in terms of the threats targeting the IT sector, these entities have been frequently targeted by malicious cyber actors, which is the second factor identified in 6 U.S.C. 681b(c)(1). The three primary NAICS segments where IT sector entities are found (i.e., the Manufacturing Sector (for hardware); the Information Sector (for software); and the Professional, Scientific, and Technical Services Sector (for IT services)) routinely rank near the top of the list when it comes to sectors or industries experiencing the most cyber incidents.[286]

In addition to the four criteria described previously in this section, CISA considered a variety of other potential criteria for inclusion, to include different criteria that would address some of the risks associated with open source code and open source software. Open source software is defined by NIST as "[s]oftware that can be accessed, used, modified, and shared by anyone."[287] Open source code and open source software are, by their very nature, accessible and modifiable by everyone. This means that anyone can identify vulnerabilities, including both good-faith security researchers who report and help fix the vulnerability as well as bad actors who take advantage of their findings to manipulate the software instead of reporting the vulnerability. And while many open source projects are well maintained, resource constraints or limited developer knowledge

[286] See *Verizon 2023 DBIR*, *supra* note 186, at 50; *Verizon 2022 DBIR*, *supra* note 181, at 50; *IBM 2023 Threat Index*, *supra* note 217, at 42.
[287] See NIST Suborder 6106.01 Ver. 1, *Open Source Code* at 1 (Dec. 6, 2018), available at https://www.nist.gov/open/policies-directives-and-nists-public-access-plan.

in some cases lead to vulnerabilities in open source projects. As the practice of integrating open source code with proprietary code and using open source code in downstream software/services has expanded, so has the potential for the incorporation of vulnerabilities into information systems with limited tracking of where the open source software is integrated, making vulnerability management increasingly challenging. With the potential for widespread use or integration of a vulnerable code, and the lack of insight into the full distribution of the code or software in which the code has been integrated, such an inherited vulnerability may be present in millions of instances and difficult to identify potential victims. The potential compromise of a code repository that houses and shares open source code could also lead to largescale downstream effects.

To better understand these threats associated with open source code and open source software, CISA considered including in the description of covered entity any managed service provider or CSP that utilizes open source software within its proprietary software library. CISA also considered including in the description of covered entity specific criteria to cover any code repository platform that hosts open source code or open source software for public use. At this time, CISA has elected not to include specific criteria in the proposed rule, but, as explained earlier, CISA interprets the first proposed IT Sector sector-based criterion to capture software development services, such as a code repositories hosting open source code, that know their services are being used by the Federal government.

CISA is interested in receiving comments on:

19. The scope of entities that would and would not be considered covered entities based on the four unique criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the four criteria.

20. The types of entities that are "related to domain name operations" and what type of relationship such entities may have with relevant multi-stakeholder organizations, such as the Internet Corporation for Assigned Names and Numbers. Please also see Section IV.D.ii in this document for additional requests for comment on the proposed DNS Exception.
21. Whether CISA should include in the final rule specific criteria to cover managed service providers or CSPs utilizing open source software or additional, specific criteria that would require reporting related to open source code, open source software, or code repositories.
22. How the proposed IT Sector sector-based criteria might apply to members of the open-source ecosystem, including whether entities that may provide IT hardware, software, systems, or services to the Federal government know or could determine whether they are providing such goods or services to the Federal government, and, if so, the level of effort in making such a determination.

k. Nuclear Reactors, Materials, and Waste Sector

The Nuclear Reactors, Materials, and Waste Sector is composed of nearly 100 commercial nuclear power reactors; over 30 Research and Test Reactors (RTRs); approximately ten fuel cycle facilities; thousands of licensees of radioactive materials for medical, research, and industrial purposes; and the millions of radioactive packages transported yearly.[288] Of these entities, CISA proposes to include in the description of covered entity any entity that owns or operates a commercial nuclear power reactor or fuel cycle facility. Commercial nuclear power reactors are subject to regulations that require them to report cyber incidents impacting safety, security, or emergency preparedness functions to the NRC; however, other Nuclear Reactors, Materials, and

[288] See DHS, *Nuclear Reactors, Materials, and Waste SSP: An Annex to the NIPP 2013* (2015), available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf.

Waste Sector infrastructure typically are not subject to similar cyber incident reporting requirements.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of commercial nuclear power reactors and fuel cycle facilities within the description of covered entity. The first factor, which relates to consequence, the disruption or compromise of a commercial nuclear power reactor may present a significant risk to public health, economic security, and national security, as validated by the extensive security regulations imposed by the NRC on these facilities.[289] Similarly, in the latest Update to the U.S. NRC Cyber Security Roadmap, the NRC staff stated that the nuclear material and hazardous chemicals at fuel cycle facilities "present safety and security concerns that could lead to potential consequences of concern . . . as a result of a cyber attack."[290]

The second factor enumerated in 6 U.S.C. 681b(c)(1) is the likelihood that an entity may be targeted by a malicious cyber actor, including a foreign country. According to the NRC, "[c]yber threats to NRC licensees are dynamic due to emerging technologies and the continuing evolving capabilities of potential adversaries."[291] Foreign countries remain interested in perpetrating cyber incidents at U.S. nuclear entities, with DHS recently stating that "Russian government-affiliated cyber espionage likely will remain a persistent threat to . . . entities in the . . . nuclear industry[y]."[292]

The third factor enumerated in 6 U.S.C. 681b(c)(1) is the extent to which damage, disruption, or unauthorized access to such an entity is likely to enable the disruption of the reliable operation of critical infrastructure. As commercial nuclear power reactors themselves are critical infrastructure, damage, disruption, or unauthorized access at a

---

[289] See, e.g., 10 CFR part 73.
[290] U.S. NRC, *Update to the U.S. NRC Cyber Security Roadmap*, SECY-17-0034, at 5 (Feb. 28, 2017), available at https://www.nrc.gov/docs/ML1635/ML16354A282.html.
[291] *Id.* at 2.
[292] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

plant likely would result in the disruption of critical infrastructure. Additional infrastructure beyond the commercial nuclear power reactor or fuel cycle facility could also be impacted by a successful cyber incident at one of these entities either through the loss of power provided by the commercial nuclear power reactor or the emission of radiation rendering nearby critical infrastructure generally not safely accessible for some period of time.

In developing this sector-based criteria, CISA also explored including RTRs in the description of a covered entity. However, the security risks associated with RTRs are significantly lower than the risks associated with commercial nuclear power reactors.[293] Based on this lower risk assessment, CISA is not proposing to include a specific Nuclear Sector sector-based criteria capturing RTRs within the description of covered entity. An owner or operator of an RTR nevertheless may be a covered entity based on the size-based threshold or other sector-based criteria, such as the Government Facilities Sector sector-based criteria for the education subsector.

l. Transportation Systems Sector

CISA proposes to include a number of different sector-based criteria for entities in the Transportation Systems Sector. First, CISA is proposing to include criteria related to owners and operators of various non-maritime transportation system infrastructure, such as freight railroad, public transportation and passenger railroads (PTPR), pipeline facilities and systems, over-the-road bus (OTRB) operations, passenger and all-cargo aircraft, indirect air carriers, airports, and Certified Cargo Screening Facilities. Additionally, CISA is proposing to include in the description of covered entity any entity that owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106.

---

[293] See *id.*; U.S. NRC, *Backgrounder on RTRs* (2020), available at https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors-bg.html.

Transportation is one of four designated lifeline functions, meaning the reliable operation of this function is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.[294] Transportation entities have long been targeted by terrorists and other malicious actors, so it is no surprise that as the cyberthreat has evolved, transportation entities are routinely experiencing cyber incidents.[295] In light of this evolving and pervasive threat, TSA has identified and imposed heightened cybersecurity requirements on critical entities across the various transportation modes. CISA is proposing to include within the description of covered entity those entities identified by TSA as requiring cyber incident reporting and (in some cases) enhanced cybersecurity measures for primarily the same reasons TSA relied upon in determining that these entities warranted such requirements. Those specific rationales for the proposed inclusion of each of the different Transportation Systems Sector criteria are provided in the following paragraphs. CISA believes that aligning CIRCIA's Applicability section with the population of entities that TSA requires cyber incident reporting from or the implementation of enhanced cybersecurity measures at is appropriate for CIRCIA and consistent with the factors contained in 6 U.S.C. 681b(c)(1)(i.e., (1) the consequences that a disruption or compromise of one of those entities could cause to national security, economic security, or public health and safety; (2) the likelihood that one of those entities may be targeted by a malicious cyber actor; and (3) the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure). CISA recognizes that some of the criteria proposed below is based on TSA's Enhancing Surface Cyber Risk Management NPRM,

---

[294] See *Guide to Critical Infrastructure Security and Resilience, supra* note 198, at 4.
[295] See, e.g., *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.

and CISA will continue to coordinate with TSA throughout the rulemaking process to harmonize CIRCIA's Applicability section with TSA, to the maximum extent practicable.

In the rail subsector, CISA is proposing to require reporting from owners and operators of freight railroad carriers identified under 49 CFR 1580.1(a)(1), (4), and (5) and PTPR identified in 49 CFR 1582.1. This is consistent with the factors contained in 6 U.S.C. 681b(c)(1),), as TSA determined these entities should be required to report cyber incidents, with the higher-risk PTPR also warranting enhanced cybersecurity requirements, "due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to prevent against the significant harm to the national and economic security of the United States that could result from the 'degradation, destruction, or malfunction of systems that control this infrastructure.'"[296] The scope of applicability for surface transportation is broader than in TSA's Security Directives, but aligns with TSA's ongoing rulemaking to codify these requirements that is based on a more long-term and strategic view of risk as applied to these modes as well as the applicability for requirements to report physical security incidents in current 49 CFR 1570.203. This scope includes PTPR and OTRB owner/operators upon whom TSA does not impose enhanced cybersecurity requirements but is seeking to impose cyber incident reporting requirements in their ongoing rulemaking efforts. While TSA has determined it is not necessary at this time to impose requirements to implement more robust cybersecurity measures on certain PTPR and OTRBs, TSA and CISA believe it is important that these entities be required to report cyber incidents when they occur. While the costs of the imposition of robust cybersecurity measures upon these PTPRs and OTRBs may not be justified at this time based on known risks, TSA and CISA believe

[296] See, e.g., TSA Security Directive 1580-21-01 series, *Enhancing Rail Cybersecurity*; TSA Security Directive 1582-21-01 series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*; TSA Security Directive 1580/82-2021-01 series, *Rail Cybersecurity Mitigation Actions and Testing*. TSA's Security Directives imposing cybersecurity requirements on surface transportation modes are available at https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.

that the improved understanding of the threat environment to the broader transportation sector that would result from the reporting of substantial cyber incidents experienced by any of these entities outweighs the minimal costs of such reporting requirements. In the case of PTPRs, the additional costs of this requirement would be particularly minimal as all PTPRs already are required to report security incidents to TSA pursuant to 49 CFR 1570.203.

CISA is also proposing to require reporting from owners and operators of the critical pipeline facilities and systems, as identified in in 49 CFR part 1586 in TSA's rulemaking, *Surface Cybersecurity Risk Management*. The scope of applicability includes gas, hazardous liquid, carbon monoxide, and liquefied natural gas pipelines, pipeline systems, and facilities that TSA has determined warrant additional cybersecurity measures to "reduce the risk of operational disruption should the Information and/or Operational Technology system of a gas or liquid pipeline be affected by a cybersecurity incident."[297] Following a determination that a pipeline is critical, TSA informs the owners and operators of the pipeline of that determination and the additional cybersecurity requirements that thus apply to it.[298] This is similarly consistent with the factors contained in 6 U.S.C. 681b(c)(1) as, to determine which pipelines were critical, TSA considered factors such as the volume of product transported and whether the pipeline serves other critical sectors. Additionally, malicious cyber actors continue to target this industry, with the 2023 Verizon DBIR noting nearly 150 cyber incidents for the mining, quarrying, and oil and gas extraction and utilities segment during the year covered by the report.[299]

---

[297] See, e.g., TSA Security Directive Pipeline-2021-01 series, *Enhancing Pipeline Cybersecurity* and TSA Security Directive Pipeline-2021-02 series, *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*, available at https://www.tsa.gov/sd-and-ea.

[298] Of note, this means that, for at least this prong of the Transportation Systems Sector sector-based criteria, entities will clearly know that they are covered entities.

[299] *Verizon 2023 DBIR*, *supra* note 186, at 59.

Additionally, CISA is proposing to include in the description of covered entity any entity that is required to implement a TSA-approved security program under 49 CFR parts 1542, 1544, 1548, and 1549. This requirement applies to airports, passenger and all-cargo aircraft operators, indirect air carriers, and Certified Cargo Screening Facilities, respectively. In November 2021, TSA issued security program changes requiring these entities to report cybersecurity incidents to CISA. A subset of these entities were subsequently required to implement additional cybersecurity measures in what TSA described as "the latest in TSA's efforts to require that critical transportation sector operators continue to enhance their ability to defend against cybersecurity threats."[300] As specifically applied to all-cargo aircraft operators, the air cargo system faces emerging risks, including a proliferation of cyber threats.[301] Adversaries continue to threaten the air cargo system and seek to use the aviation domain to carry out terrorist plots, including through the use of the air cargo supply chain to ship dangerous and potentially deadly items for pre-operational planning.[302] The focus on these "critical transportation sector operators" in light of the "persistent cybersecurity threats against U.S. critical infrastructure, including the aviation sector"[303] is consistent with the three factors enumerated in 6 U.S.C. 681b(c)(1).

Most, if not all, of the entities that would be captured under these criteria already are required to report cybersecurity incidents to CISA pursuant to these requirements. Including these entities within the description of covered entity would further align the CIRCIA requirements with TSA's requirements to support reducing duplication and avoid unintended gaps in reporting. For example, while this approach technically creates

---

[300] TSA Press Release, *TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators* (Mar. 7, 2023), available at https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft (hereinafter "*TSA Press Release*").
[301] TSA, *Air Cargo Security Roadmap* (Dec. 2021), available at https://www.tsa.gov/news/press/releases/2021/12/09/tsa-publishes-new-roadmap-address-vision-improving-air-cargo.
[302] See *id.*
[303] *TSA Press Release*, *supra* note 300.

two legal requirements for these entities to report cyber incidents, CISA does not believe that this is likely to result in any actual duplicative reporting because TSA's existing requirement requires these entities to report to CISA. CISA is committed to working with TSA to ensure that Transportation Services Sector entities that are required to report to CISA under both CIRCIA and a separate TSA authority can do so in a single report where legally possible. If necessary to do so, CISA and TSA will explore leveraging the substantially similar reporting exception to formalize the ability to comply with CIRCIA and TSA cyber incident reporting requirements through the submission of a single cyber incident report. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

With the final Transportation Systems Sector sector-based criterion, CISA is proposing to cover those entities that own or operate assets subject to MTSA. MTSA, which is designed to protect the nation's ports and waterways from a terrorist attack, requires certain vessels, facilities, and outer continental shelf facilities to perform various security-related activities. The goal of MTSA is to prevent a transportation security incident, which is defined as an incident that results in significant loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area.[304] This goal is consistent with the first and third factors enumerated in 6 U.S.C. 681b(c)(1)—i.e., the consequences that disruption to or compromise of an entity could cause to national security, economic security, or public health and safety, and the extent damage or disruption to an entity will likely enable the disruption of the reliable operation of critical infrastructure. Including MTSA-regulated facilities is also consistent with the second factor enumerated in 6 U.S.C. 681b(c)(1)—the likelihood that an entity may be targeted by a malicious cyber actor, including a foreign country—given the recent

[304] See U.S. Coast Guard, *Operations Home – ISPS/MTSA*, https://www.dco.uscg.mil/ISPS-MTSA/ (last visited Nov. 28, 2023); 33 CFR 101.100.

assessment in the 2024 Homeland Security Threat Assessment identifying an increased risk from Chinese government cyber actors to target ports for disruption.[305] The MTSA-regulated population is generally considered to include all critical maritime assets. Considering that, CISA, after consultation with the USCG, the SRMA for the Transportation Systems Sector Maritime Subsector and regulatory agency responsible for MTSA, believes that entities that own or operate vessels, facilities, or outer continental shelf facilities subject to MTSA should be required to report cyber incidents under CIRCIA. To achieve that, CISA proposes that the description of covered entity include any entity that owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106.

CISA and USCG recognize that this proposed approach will result in two separate cyber incident reporting requirements for entities that are subject to both MTSA and CIRCIA. CISA and USCG are committed to exploring the substantially similar reporting exception or other mechanisms to allow entities that are subject to both MTSA and CIRCIA cyber incident reporting requirements to comply with both requirements through the submission of a single cyber incident report. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

m. Water and Wastewater Systems Sector

CISA proposes including within the description of covered entity any entity that owns or operates a Community Water System, as defined in 42 U.S.C. 300f(15), or a Publicly Owned Treatment Works (POTWs), as defined in 40 CFR 403.3(q), that serve more than 3,300 people. Inclusion of water and wastewater systems in the description of covered entity is supported by a review of how the three factors enumerated in 6 U.S.C. 681b(c)(1) apply to these entities. First, as noted in the 2015 Water and Wastewater Systems SSP, safe drinking water is essential to public health and all human activity, and

[305] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

properly treated wastewater is vital for preventing disease and protecting the environment.[306] According to the EPA, "[t]he collection and treatment of . . . wastewater is vital to public health and clean water."[307] The 2015 Water and Wastewater Systems SSP further notes that drinking water and wastewater treatment are essential to modern life and the Nation's economy.[308] Second, as noted in a March 3, 2023 memorandum issued by the EPA related to public water system cybersecurity, water systems are increasingly facing cyberattacks.[309] This assessment is supported by the Cyberspace Solarium Commission, which stated in its March 2020 report that the "water supply is known to be a target for malign actors."[310] Third, other critical services, such as fire protection, healthcare, and heating and cooling, are dependent on, and would be disrupted by, the interruption or cessation of drinking water services.[311] This criticality to other sectors is reinforced by water having been designated one of four designated lifeline functions, indicating that the sector's reliable operation is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.[312]

No cyber incident reporting requirements currently exist for water and wastewater infrastructure, creating a significant gap in understanding of the cyber threats to and visibility into emerging TTPs used against water and wastewater infrastructure. This proposed sector-based criterion is intended to close this gap and provide the Federal government with sufficient reporting to better understand the Water and Wastewater Systems Sector's cyber threat environment.

---

[306] See DHS, *Water and Wastewater Systems SSP* at 1 (2015), available at https://www.cisa.gov/2015-sector-specific-plans (hereinafter "*Water and Wastewater Systems SSP*").
[307] See EPA, *Municipal Wastewater*, https://www.epa.gov/npdes/municipal-wastewater (last visited Nov. 28, 2023).
[308] *Water and Wastewater Systems SSP*, *supra* note 306, at i.
[309] Assistant Administrator Fox, *Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process* (Mar. 3, 2023), available at https://www.epa.gov/waterresilience/cybersecurity-sanitary-surveys.
[310] *Cyberspace Solarium Commission Report*, *supra* note 23, at 62.
[311] See *Water and Wastewater Systems SSP*, *supra* note 306, at 2.
[312] See *Guide to Critical Infrastructure Security and Resilience, supra* note 198, at 4.

In developing this sector-based criterion, CISA considered whether a minimum size threshold, such as population served, should be included in the criterion. Following consultations with the EPA, the SRMA for this sector, CISA has determined that the proposed criterion should only include Community Water Systems and POTWs that serve populations of more than 3,300 people. In regards to Community Water Systems, this threshold, which has been used as the line of demarcation to distinguish small and very small water systems from medium, large, and very large water systems,[313] is the threshold for the risk and resilience assessment requirements established by Congress in 42 U.S.C. 300i-2(a)(1).[314] Section 300i-2(a)(1) and (b) of title 42 of the United States Code requires Community Water Systems serving a population of more than 3,300 people to conduct risk and resilience assessments and to prepare an emergency response plans that incorporate the findings of the assessments performed.[315] CISA interprets Congress's decision to limit the 42 U.S.C. 300i-2(a)(1) risk and resilience assessment requirements to facilities serving more than 3,300 individuals as an indication of Congress's assessment of the relative risk associated with these facilities, and CISA agrees with this assessment for the reasons stated above. This interpretation is consistent with the fact that, generally speaking, Community Water Systems that serve larger populations will de facto present greater potential risks to public health and safety, if compromised, in light of the significantly larger populations that rely on their water service. Similar logic supports the application of the 3,300-population-served threshold for POTWs, as does the rationale discussed in Section IV.B.iv.1.a for the proposed inclusion of larger entities in the covered entity population. By setting the threshold for coverage of water and wastewater treatment systems at a population served of more than

---

[313] See, e.g., *Water and Wastewater Systems SSP*, *supra* note 306, at 3.
[314] 42 U.S.C. 300i-2(a)(1).
[315] See *id*.; see also EPA, *America's Water Infrastructure Act Section 2013: Risk and Resilience Assessments and Emergency Response Plans*, https://www.epa.gov/waterresilience/awia-section-2013 (last visited Nov. 28, 2023).

3,300 individuals, this criterion would be limiting required reporting to approximately the largest 20% of water and wastewater treatment systems by population served.[316]

In establishing this proposed criterion, CISA, in consultation with EPA, did consider not including a size threshold and instead requiring reporting from all water systems and POTWs. CISA believes that including all water systems and POTWs as a criteria is a reasonable alternative. A cyber incident that results in a compromise of water treatment even for smaller communities arguably is a significant enough potential public health concern that it should warrant reporting to the Federal government. Moreover, because this sector is predominantly composed of smaller entities, reporting of incidents from smaller entities in this sector could be essential to CISA receiving a sufficient volume of reports to identify trends, TTPs, and vulnerabilities that can be used to provide early warnings to water and wastewater facilities of all sizes. Cutting against the argument to include all water and wastewater systems in the covered entity definition is the fact that many of the smallest water systems and POTWs, such as hand pump operated wells at a campground or other small facility, do not currently utilize information systems, and thus, could not be the target of malicious cyber activity or experience a covered cyber incident. Additionally, given that there are more than 150,000 combined Public Water Systems (which includes both Community Water Systems and non-community water systems) and POTWs, were CISA to include all of those entities in the description of covered entity, it would dramatically increase the scope and burden of the proposed regulations, with water and wastewater facilities accounting for nearly 40% of all covered entities.

After weighing these considerations, CISA ultimately concluded that proposing limiting reporting required by CIRCIA to medium, large, and very large Community

---

[316] See *Water and Wastewater Systems SSP*, *supra* note 306, at 3, 6.

Water Systems and POTWs entities is the optimal approach. CISA would be interested in comments on:

23. The proposed Water and Wastewater Systems Sector sector-based criterion.
24. The alternative criterion for the Water and Wastewater Systems Sector that was considered.

n. Sectors for Which CISA is Not Proposing Any Sector-Based Criteria

CISA is not proposing any sector-based criteria for three sectors: the Commercial Facilities Sector, the Dams Sector, and the Food and Agriculture Sector. CISA's rationale for proposing to not include sector-based criteria for each of these sectors is described below. Instead, CISA proposes to rely on the Applicability section's size-based criterion or other sector-based criteria to capture the largest entities in these critical infrastructure sectors for the reasons described below.

The Commercial Facilities Sector is made up of an extremely diverse range of physical and virtual sites where large numbers of people congregate to conduct business, purchase retail products, and enjoy recreational events and accommodations. It is divided into eight subsectors—Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues. While members of certain subsectors are at higher risk of cyber incidents, such as the Entertainment and Media, Gaming, and Lodging subsectors, the results of a cyber incident impacting an individual small entity in those industries are unlikely to affect national security, economic security, or public health and safety. To the extent that a Commercial Facilities entity is large enough where there is the potential that a cyber incident affecting it could result in impacts to national security, economic security, or public health and safety, CISA believes it likely the entity would be captured by the Applicability section's size-based

criterion. As a result, CISA is not proposing a sector-based criteria for the Commercial Facilities Sector.

The Dams Sector consists of, among other things, over 100,000 dams, an estimated 100,000 miles of levees, nearly 250 locks, and 150,000 mine tailings. The majority of these do not have integrated information systems and thus do not warrant coverage under the CIRCIA regulations at this time. Those assets that do have significant integrated information systems, such as large dams, hydroelectric power dams, and locks, frequently are owned by Federal entities or, in the case of certain hydroelectric or other dams, are likely to be covered entities under the proposed Energy Sector or Water and Wastewater Systems Sector sector-based criteria. CISA, therefore, is not proposing a sector-based criteria for the Dams Sector.

The Food and Agriculture Sector covers a broad landscape of entities, including more than 2 million farms; nearly 1 million restaurants; over 100,000 supermarkets, grocery stores, and other food outlets; and thousands of meat, poultry, egg, and imported food processors, warehousers, and distributors. Based on consultations with the FDA and the U.S. Department of Agriculture (USDA), who serve as co-SRMAs for this sector, CISA believes that given the scale of this sector and the general substitutability of the products that entities within the sector produce, the Food and Agriculture Sector entities with the greatest potential to experience a cyber incident resulting in significant consequences are the largest entities in this sector. For this reason, FDA regulations focused on food defense incorporate a size-based threshold, applying more stringent regulatory requirements to the largest entities.[317] Based on this, and after consultation

[317] See *Mitigation Strategies To Protect Food Against Intentional Adulteration*, 21 CFR part 121. As FDA explained in the NPRM for those regulations, "[The FDA assesses] that the goal of terrorist organizations is to maximize public health harm and, to a lesser extent, economic disruption. It is our assessment that such goals are likely to drive terrorist organizations to target the product of relatively large facilities, especially those for which the brand is nationally or internationally recognizable. An attack on such a target would potentially provide the wide-scale consequences desired by a terrorist organization and the significant public attention that would accompany an attack on a recognizable brand. Such facilities are likely to have

with the FDA and USDA, CISA believes that the size standard proposed by CIRCIA will capture a sufficient number of Food and Agriculture Sector entities, including the most critical Food and Agriculture Sector entities, within the description of covered entity, and that additional Food and Agriculture Sector sector-based criteria are unnecessary for the purposes of CIRCIA.

CISA believes that it can rely on other criteria for adequate reporting from these three sectors. However, if as a result of public comment CISA determines that it must modify or eliminate any aspect of the Applicability section's description of a covered entity such that coverage of these three sectors is no longer deemed adequate, CISA may incorporate sector-based criteria for these three sectors in the final rule.

For the Commercial Facilities sector, CISA is relying on the proposed size-based threshold criterion for reporting. Were that criterion to be modified or eliminated prior to the issuance of the final rule, one alternative sector-based criterion CISA likely would consider would be to capture certain sector entities that exceed one or more designated annual revenue or number of employees thresholds. This could be structured as a single threshold for all Commercial Facilities Sector entities, or it could vary based on subsectors or industry segments. If a single threshold were to be used for all entities in the sector, CISA likely would use the SBA Size Standards to inform that decision and develop a possible average threshold, but would not use the SBA Size Standards alone since the applicable size thresholds in the SBA Size Standards for Commercial Facilities Sector entities vary depending on the type of entity and associated NAICS code. An alternative approach to developing a single size threshold for the sector-based criterion for this sector would be to simply use the SBA Size Standards themselves (i.e., an entity

---

larger batch sizes, potentially resulting in greater human morbidity and mortality. Further, an attack on a well-recognized, trusted brand is likely to result in greater loss of consumer confidence in the food supply and in the government's ability to ensure its safety and, consequently, cause greater economic disruption than a relatively unknown brand that is distributed regionally." 78 FR 78033.

in the Commercial Facilities sector that exceeds the applicable SBA Size Standard), which is how entities in this sector would be considered covered entities under the current proposal. In either case, CISA would attempt to set any threshold to cover the same larger entities in the sector which would be required to report under the proposed size-based criterion.

Coverage of entities in the Food and Agriculture Sector in the current proposed approach similarly is reliant on the size-based threshold criterion. If as a result of public comment CISA determines that it must eliminate or modify the size-based criterion, CISA likely would propose multiple different Food and Agriculture Sector sector-based criteria to ensure that these entities remain covered entities. This is likely to include one criterion targeting larger food manufacturers, processors, warehouses, and similar entities; one criterion targeting larger food producers (e.g., farms, orchards, groves, ranches, hatcheries, fisheries); and one criterion larger targeting groceries, supermarkets, and other food outlets. For food manufacturers, processors, warehouses, and similar entities, a potential approach to developing this criterion would be to mirror the approach used in the Food Safety Modernization Act's International Adulteration rule (21 CFR part 121), which regulates food manufacturers, processors, warehouses, and similar entities that have more than 500 employees. For food producers, CISA could leverage the SBA size standards table to set a size threshold for this criterion based on annual revenue. As the SBA Size Standards use slightly different revenue thresholds for different types of food producers, CISA could elect to use the mean, median, or mode of the different revenue amounts used in this industry segment or simply have entities refer to the applicable size standard for their industry in the SBA Size Standards table. For the final group, i.e., supermarkets, groceries, and other food outlets, CISA could use a similar approach to set a size threshold for this criterion, except for these types of entities, the SBA Size Standards tend to use number of employees as opposed to annual revenue to

distinguish between small and large entities. Thus, this criterion is likely to be a size threshold based on the mean, median, or mode of number of employees across such entities.

As noted above, the only Dams Sector assets that are likely to have integrated information systems warranting coverage under CIRCIA are large dams, hydroelectric power dams, and locks. With the Federal government responsible for 80% of the largest dams and all navigation locks,[318] the only segment of this sector where CISA might not have insight into incidents without CIRCIA reporting would be the 2,600 non-Federal hydroelectric dams. Unlike the Commercial Facilities and Food and Agriculture Sector entities, CISA is currently not proposing a separate standard for this sector because CISA believes these entities are sufficiently covered in the proposed covered entity description not by the size-based criterion, but by other sector-based criteria, namely the Energy Sector sector-based criterion and, to a lesser extent, the Water and Wastewater Systems Sector sector-based criterion. Accordingly, if as a result of public comment CISA determines that it must modify or eliminate the proposed size-based criterion from the final rule, but the proposed Energy Sector sector-based criterion remained, CISA does not believe it would need to propose a separate Dams Sector sector-based criterion. If, however, either the Energy Sector or Water and Wastewater Systems Sector sector-based criterion were modified or eliminated as a result of public comment, CISA may need to add a Dams Sector sector-based criterion to the final rule to ensure reporting from appropriate non-Federal hydroelectric dams. In such a case, CISA would consult with FERC and the Dams SRMA to identify an appropriate criterion for this industry segment. A possible alternative criterion could be based on energy generating capacity.

CISA is interested in receiving comments on:

---

[318] See *Dams SSP: An Annex to the NIPP 2013* at v (2015), available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf.

25. The proposed approach to the Commercial Facilities Sector, Dams Sector, and Food and Agriculture Sector.
26. Potential alternative sector-based criteria for each of those three sectors if CISA modifies or removes the general size-based threshold criterion, the Energy Sector sector-based criterion, or the Water and Wastewater Systems Sector sector-based criterion in the final rule.

o. Interpretation of Sector-Based Criteria Coverage

When an entity is assessing whether it is a covered entity based on any of the sector-based criteria, the entity should not factor into its assessment the critical infrastructure sector of which the entity considers itself to be a part. By definition, each of the sector-based criterion include entities that are in a critical infrastructure sector, and entities should therefore assume they meet this threshold requirement of being "in a critical infrastructure sector" if they meet one or more sector-based criteria, without needing to undertake any determination described in Section IV.B.ii, above. CISA will determine whether an entity is a covered entity based on whether the entity meets any of the specified criteria in § 226.2 of the proposed rule. Whether or not the entity considers itself part of the specific critical infrastructure sector that the sector-based criteria targets or is based upon on is irrelevant for the purposes of determining whether the entity is a covered entity. For example, if a pharmaceutical manufacturer owns a covered chemical facility subject to CFATS (or, if CFATS is not reauthorized by the publication of the final rule, the EPA RMP), it would qualify as a covered entity regardless of whether or not the pharmaceutical manufacturer considers itself part of the Chemical Sector. Similarly, if an SLTT Government entity owns or operates a Community Water System as defined in 42 U.S.C. 300f(15), it would qualify as a covered entity regardless of its Title IV status even if it considers itself a member of the Government Facilities Sector, and not the Water and Wastewater Systems Sector. Thus, an entity may qualify as a covered entity under a

sector-based criterion for a sector with which it does not typically identify, and an entity may qualify as a covered entity under two different sector-based criteria. However, an entity only needs to meet one of the sector-based criteria proposed in the Applicability section to qualify as a covered entity.

As noted throughout this section, CISA recognizes that a number of the entities that are captured under the Applicability section already are, or in the future will be, required to report cyber incidents to a different Federal department or agency pursuant to another existing or proposed regulation. CISA could have attempted to design the sector-based criteria in a manner to avoid designating entities that may be subject to other Federal cyber incident reporting requirements as covered entities. With one exception, however, CISA has no authority over those other regulations.[319] If CISA were to carve those entities out of CIRCIA's Applicability section, CISA would have no control over what incidents the entities must report or what information must be included in those reports.[320] CISA also would be unable to guarantee it would receive such reports in a timely manner. To ensure that CISA continues to receive reports from entities containing the information needed to support the CIRCIA mission in a manner and timeframe that support CIRCIA implementation, CISA proposes not to use other existing regulatory coverage as a disqualifying factor for inclusion within the description of covered entity. As noted earlier, CISA is committed to working with its Federal partners to explore the implementation of the substantially similar reporting exception where practicable to minimize duplicative reporting. Moreover, this approach is consistent with Congressional intent behind the CIRCIA legislation, which included providing CISA, as the newly

[319] CISA is responsible for implementation of the CFATS, 6 CFR part 27, which requires CFATS-covered chemical facilities to report certain cyber incidents to CISA, although CISA acknowledges that at the time of publication of this NPRM, Congress has allowed the statutory authority for CFATS to lapse.

[320] CISA recognizes that CISA proposes to use regulations that CISA does not administer to help scope what entities meet the CIRCIA Applicability. If following the publication of a final rule implementing CIRCIA the population covered by those other regulations changes, CISA will review the change and may seek to update the CIRCIA regulations if the existing regulatory citation no longer reflects the population from which CISA seeks to receive reporting under CIRCIA.

minted central repository for cyber incident reporting, visibility into significant cyber incidents being conducted across U.S. critical infrastructure sectors and enabling coordinated, informed Federal government action against perpetrators of cyberattacks.[321]

v. Other Approaches Considered to Describe Covered Entity

In addition to the proposed approach, CISA considered various other options for how to describe covered entity. Among other approaches, CISA considered simply using the statutory definition contained in CIRCIA (i.e., any entity in a critical infrastructure sector); aligning the Applicability section to an existing definition of "critical infrastructure;" and describing covered entity as the entities identified pursuant to Section 9 of Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (78 FR 11737). CISA opted against using any of these approaches either as a standalone approach or, where it would not make the other prongs redundant, as a third prong to the proposed approach for the reasons described below.

1. Alternative A: Any Entity in a Critical Infrastructure Sector

One alternative approach CISA considered for describing covered entity was to scope the term as broadly as permissible under the statute—i.e., to include "any entity in a critical infrastructure sector, as defined in PPD-21." As discussed earlier, while the term "critical infrastructure sector" is not defined in PPD-21, public and private sector partners for each of the critical infrastructure sectors identified in PPD-21 jointly developed SSPs for their respective sectors that set out goals and priorities for the sector to address its current risk environment.[322] Each of those SSPs includes a description of the entities that compose the sector in Sector Profiles. As the examples provided earlier demonstrate, most of these sectors are quite expansive, and entities "in a critical infrastructure sector"

---

[321] See, e.g., *HSGAC Fact Sheet*, *supra* note 2, at 1 ("Today no one U.S. Government agency has visibility into all cyber-attacks occurring against U.S. critical infrastructure on a daily basis. This bill would change that—enabling a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the U.S.").

[322] See CISA, *2015 Sector Specific Plans,* available https://www.cisa.gov/2015-sector-specific-plans (last visited Nov. 28, 2023).

are not limited to—and are often broader than—entities that own or operate systems or assets that meet the statutory definition of "critical infrastructure." See Section IV.B.ii in this document. Based on a consolidated reading of these sector-developed descriptions in the various SSP Sector Profiles, CISA believes that the overwhelming majority of entities in the United States—though not all—fit within one or more of the critical infrastructure sectors and thus would meet the definition of "an entity in a critical infrastructure sector."

According to Census Bureau records, there are more than 8 million employers in the United States and another approximately 27 million legal establishments that do not have any employees.[323] Combined, that would indicate the existence of approximately 35 million entities with legal standing within the United States. Given that very few types of entities are not part of one of the 16 critical infrastructure sectors, CISA believes that the vast majority of these 35 million entities would qualify as an "entity in a critical infrastructure sector."

Although CISA anticipates the per-report cost of this regulation to be relatively low, the aggregate cost of reportable incidents across tens of millions of entities has the potential to be extremely large and burdensome. Additionally, while CISA believes receiving a large number of reports is necessary to achieve the goals of the CIRCIA regulation, CISA acknowledges that there likely is some point at which the marginal returns provided by each additional report will be outweighed by the cost of its submission. Although it is difficult to pinpoint with precision that point of diminishing marginal returns, CISA is confident that it would be surpassed were CISA to require reporting from tens of millions of entities.

2. Alternative B: Removal of Size-Based Threshold

[323] See, e.g., U.S. Census Bureau, *County Business Patterns First Look Report for 2021*, available at https://www.census.gov/data/tables/2021/econ/cbp/2021-first-look.html; U.S. Census Bureau, Nonemployer Statistics Tables for 2019, available at https://www.census.gov/programs-surveys/nonemployer-statistics/data/tables.html.

A second alternative CISA considered was to use the same general framework as in the current proposed approach, but without the size-based criterion. Under this approach, CISA would only rely upon sector-based criteria to cover the desired population of entities in each critical infrastructure sector. As the existing sector-based criteria do not cover all of the sectors and subsectors from which CISA believes reporting is necessary, were CISA to eliminate the size-based criterion, CISA would have to propose adding new sector-based criteria to ensure appropriate coverage of covered entities. Sectors or subsectors for which CISA would need to add new sector-based criteria include the Commercial Facilities Sector, the Dams Sector, the Food and Agriculture Sector, certain parts of the Healthcare and Public Health Sector (e.g., medical insurers; laboratories and other diagnostic facilities), and the Oil and Natural Gas Subsector.

Removing the size-based criterion and replacing it with some number of new sector-based criteria would have two primary effects. First, the total number of covered entities likely would be slightly reduced as there are some entities currently captured by the size-based criterion that would not meet any of the current proposed or potential additional sector-based criteria. CISA believes that such entities would be relatively few, however, as CISA estimates that the majority of entities that currently meet the size-based criterion either also meet one of the current sector-based criteria or would be brought into the covered entity definition by a new sector-based criterion.

Second, CISA believes that this alternative could slightly reduce familiarization costs associated with the regulation, as entities that would have had to expend resources to determine if they exceeded the SBA Size Standard for their respective industry no longer would have to do so. CISA believes that this impact would also be fairly limited as: (a) only a portion of potentially covered entities would need to expend resources to make such a determination since many already know if they exceed the small business

size standard for their respective industry, (b) the amount of resources necessary to do so typically are relatively minimal, and (c) a portion of the resources certain entities would save by the elimination of the size-based criterion would instead be expended by those or other entities to determine if they meet one of the new sector-based criteria.

Contrary to the minimum benefits likely to be gained by elimination of the size-based criterion, CISA believes there are significant reasons to include the criterion in the proposal. First, as described at length in Section IV.B.iv.1 above, there are a number of reasons why CISA believes requiring reporting from large entities is beneficial. Second, the size-based criterion allows CISA to capture adequate reporting populations from multiple sectors and subsectors using a single threshold. As noted above, without the size-based criterion, CISA would need to establish one or more new sector-based criteria for each of at least five critical infrastructure sectors or subsectors. In total, while CISA believes it could achieve the purposes of the CIRCIA statute without a size-based criterion, CISA believes that the benefits of including the size-based criterion far exceed the almost certainly minimal cost savings associated with an alternative where additional sector-based criteria are used in lieu of the size-based criterion.

3. Alternative C: Definition of Critical Infrastructure

CISA also explored potentially limiting the scope of the covered entity description to critical infrastructure only and using an existing definition of critical infrastructure, such as the one at 42 U.S.C. 5195c(e).[324] As discussed earlier, however, CISA believes that such a narrow scope of applicability would severely limit, and perhaps prevent, CISA's ability to achieve CIRCIA's regulatory purposes. See Section III.C.ii. Additionally, the 42 U.S.C. 5195c(e) definition of "critical infrastructure"

[324] 42 U.S.C. 5195c(e) defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

includes some ambiguity that can make it difficult for certain entities to know definitively whether they meet the definition. For example, it is not readily apparent what level of impact would constitute a "debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[325] Moreover, even if a clear definition of that level of impact existed, it would be unreasonable to expect most private sector entities to be able determine if an incident impacting one of their systems would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. Because the description of covered entity will impose regulatory requirements on entities, it is important that the description be easily understandable and allow different individuals interpreting the description to routinely come to the same conclusion.

4. Alternative D: Section 9 List

In comments submitted in response to the RFI, a number of commenters recommended that CISA use the list of entities developed pursuant to Section 9(a) of Executive Order 13636 (hereinafter referred to as the Section 9 List) as either a starting point for identifying, or the complete list of, covered entities.[326] The Section 9 List contains "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[327] Pursuant to Executive Order 13636, DHS is to review and update this list annually.

Given that the Section 9 List consists of entities against which a cybersecurity incident could result in catastrophic effects on national security, economic security, or public health, CISA agrees that the entities on the Section 9 List are entities that CISA

---

[325] *Id.*

[326] See, e.g., Comments submitted by UnityPoint Health, CISA-2022-0010-0107; National Retail Federation, CISA-2022-0010-0092; National Rural Electric Cooperative Association, CISA-2022-0010-0025.

[327] E.O. 13636 Section 9(a), available at https://www.cisa.gov/resources-tools/resources/executive-order-eo-13636-improving-critical-infrastructure-cybersecurity.

would want to report covered cyber incidents and ransom payments under CIRCIA. CISA anticipates, however, that all of the entities on the Section 9 List would be covered entities under either the proposed size-based criterion or sector-based criteria in the proposed Applicability section, rendering any benefits of using the Section 9 List as a basis for coverage under CIRCIA extremely limited. CISA further believes that the limited benefits of potentially requiring reporting from a few Section 9 List entities who would not already be required to report under other proposed criteria are outweighed by the significant potential downsides associated with using the Section 9 List in this manner.

First, CISA is concerned that using the Section 9 List, which relies in part on nominations to identify entities for inclusion, as the basis for imposing regulatory requirements would chill nominations to the list and reduce voluntary participation in cybersecurity efforts targeted at Section 9 List entities. Depending on how much the use of the Section 9 List for regulatory purposes disincentivizes cooperation in the development of the list and participation in voluntary cybersecurity activities targeted at Section 9 List entities, using the list for CIRCIA could result in a net overall negative impact to national cybersecurity efforts.

Second, because of the requirement that CISA update the list annually, entities would lack certainty regarding their future regulatory status under CIRCIA. This would not only be frustrating to entities, but it could also result in some entities wasting resources to establish regulatory reporting processes and procedures that they end up not needing or, conversely, result in some entities foregoing establishing reporting processes and procedures with the thought that they might not be subject to regulatory requirements the following year. The annual updates to the list would also present logistical challenges for CISA, which would need to inform entities whenever they are added to, or removed from, the list for the entities to be aware of their regulatory status.

vi. Request for Comments on Applicability Section

CISA seeks comments on all aspects of the Applicability Section, to include comments on the following specific topics:

27. CISA's interpretation of the terms "entity" and "in a critical infrastructure sector."
28. Potential challenges for an entity determining whether it is "in a critical infrastructure sector" and any specific changes that can be made to the proposed § 226.2 (Applicability) that would provide additional clarity for an entity to make this determination.
29. The scope of entities that would only be considered covered entities because of the size-based criterion and would not meet any of the sector-based criteria.
30. The use of both a size-based criterion and sector-based criteria as criteria in the description of covered entity.
31. The proposed decision to include a size-based criterion.
32. The proposal to use the SBA Size Standards as the basis for the size-based criterion and the Small Business Size Regulations instructions for determining if an entity exceeds the size threshold for purposes of determining applicability of these regulations to certain entities.
33. The proposed sector-based criteria used in the Applicability Section to identify certain entities as covered entities.
34. Any additional sector-based criteria that would be necessary to capture entities who are only considered covered entities because of the size-based criterion if the size-based criterion was removed the Final Rule.
35. The use of the EPA RMP rule as an alternative Chemical Sector sector-based criteria should CFATS not be reauthorized at the time of the issuance of the CIRCIA final rule.

36. The proposed decision to forgo inclusion of sector-based criteria for certain critical infrastructure sectors, subsectors, industries, or entity types, and the alternative proposed criteria for those sectors, subsectors, industries, and entity types.
37. Whether there are other lists of entities in a critical infrastructure sector that should be included as covered entities (either instead of the applicability criteria for covered entity proposed in this NPRM or in addition to the proposed applicability criteria), to the extent that those listed entities fall within a critical infrastructure sector.

C. Required Reporting on Covered Cyber Incidents and Ransom Payments

i. Overview of Reporting Requirements

Pursuant to 6 U.S.C. 681b(a)(1) – (3), four proposed circumstances exist that require covered entities (or third parties on their behalf) to submit a report to CISA, subject to certain proposed exceptions or limitations discussed in Sections IV.D and IV.E.ii of this document. First, CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. 6 U.S.C. 681(a)(1)(A). Second, CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity to report that payment to CISA. 6 U.S.C. 681b(a)(2)(A). Third, CIRCIA requires that, until a covered entity notifies CISA that the covered cyber incident in question has concluded and been fully mitigated and resolved, a covered entity must submit an update or supplement to a previously submitted report on a covered cyber incident if substantial new or different information becomes available. 6 U.S.C. 681b(a)(3). Finally, CIRCIA requires that a covered entity submit an update or supplement to a previously submitted report on a covered cyber incident if the covered entity makes a ransom payment after submitting a Covered Cyber Incident Report. 6

U.S.C. 681b(a)(3). CISA is proposing to incorporate these requirements in § 226.3 of the proposed regulation. Other parts of the proposed regulation discuss the report submission deadlines (§ 226.5; IV.D.iv), manner and form (§ 226.6; IV.D.i and ii), and information required (§§ 226.7 through 226.11; IV.D.iii) for all of these types of reports.

CISA is proposing to include the first reporting requirement, the requirement for a covered entity to report a covered cyber incident, in § 226.3(a). A covered entity would comply with this requirement by submitting, or having a third-party submit on the covered entity's behalf, a Covered Cyber Incident Report or a Joint Covered Cyber Incident and Ransom Payment Report pursuant to § 226.3(c). Cyber incidents do not occur in a single moment in time, but span from the initial moment of compromise until the cyber incident is fully mitigated and resolved. Because of this, CISA interprets the word "experiences" (in the statutory phrase "a covered entity that experiences a covered cyber incident") to include the full lifecycle of a cyber incident, such that this reporting requirement applies to any entity that qualifies as a covered entity at any point during the occurrence of the covered cyber incident. For example, this means that if an entity discovers that it experienced a covered cyber incident two years ago that has continued to the present, and that entity is a covered entity at the time of discovery, the entity would be required to submit a Covered Cyber Incident Report under the proposed rule because the incident has not concluded and been fully mitigated and resolved. Conversely, if that same entity was not a covered entity at the time of discovery, but was one year ago (i.e., during the period when the covered cyber incident was ongoing but not yet discovered), the entity would be required to submit a Covered Cyber Incident Report under the proposed rule because the entity experienced at least part of the covered cyber incident while it was a covered entity.

CISA is proposing to include the second reporting requirement, the requirement for a covered entity to report a ransom payment it has made, in § 226.3(b).[328] CISA understands CIRCIA as requiring a covered entity to report a ransom payment regardless of whether the ransomware attack that led to the ransom payment is a covered cyber incident. 6 U.S.C. 681b(a)(2)(B). Additionally, CISA interprets 6 U.S.C. 681b(d)(3) to require a covered entity to report a ransom payment regardless of whether the covered entity itself makes the ransom payment or has a third-party make the ransom payment on the covered entity's behalf. Because this reporting requirement is tied to a single action that occurs at a specific moment in time—the making of a ransom payment—CISA interprets the word "makes" (in the statutory language "a covered entity that makes a ransom payment") to apply this reporting requirement to any entity that qualifies as a covered entity at the moment in time that it makes a ransom payment as the result of a ransomware attack.

Depending on the circumstances surrounding and timing of the ransom payment, including whether the ransomware attack is a covered cyber incident, the type of CIRCIA Report a covered entity (or third party on behalf of a covered entity) might use to comply with proposed § 226.3(b) may vary. For example, if the ransom payment was made as the result of an incident that did not qualify as a covered cyber incident, the covered entity would submit a Ransom Payment Report under § 226.3(b). If the ransom payment was made as the result of a covered cyber incident that has not yet been reported, the covered entity may opt to submit a Joint Covered Cyber Incident and Ransom Payment Report under § 226.3(c) instead of a Covered Cyber Incident Report under § 226.3(a) and a separate Ransom Payment Report under § 226.3(b). Alternatively, if the ransom payment

[328] While the proposed rule includes reporting of ransom payments to CISA, as CIRCIA requires, CISA notes that "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks." Department of the Treasury, Office of Foreign Asset Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021).

was made as the result of a covered cyber incident that the covered entity has previously reported to CISA, then the covered entity would use a Supplemental Report under § 226.3(d) to report the ransom payment to CISA.

Pursuant to 6 U.S.C. 681b(a)(5)(A), a covered entity that makes a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting timeframe for reporting the covered cyber incident may submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. CISA is proposing to include this option in § 226.3(c). Additional details on this type of joint report, which CISA is proposing to call a Joint Covered Cyber Incident and Ransom Payment Report, can be found in Section IV.A.iii.4 and IV.E.ii.1 of this document.

Lastly, CISA is proposing to include in § 226.3(d) the statutory reporting requirements that mandate a covered entity provide CISA with updates or supplements in certain circumstances. As discussed in Section IV.A.iii.5 of this document, CIRCIA refers to these types of reports as Supplemental Reports, which a covered entity is obligated to provide unless and until it has notified CISA that the underlying covered cyber incident has concluded and been fully mitigated and resolved. 6 U.S.C. 681b(a)(3). CISA's proposed interpretation for "concluded" and "fully mitigated and resolved" and the process for informing CISA of the belief that the covered cyber incident at issue has concluded and been fully mitigated and resolved are discussed in further detail in Sections IV.E.iv.3.c and IV.E.v.2 of this document, respectively. Notifying CISA that the covered entity believes the underlying covered cyber incident has concluded and been fully mitigated and resolved is optional.

The first scenario resulting in the requirement to submit a Supplemental Report is when substantial new or different information becomes available to a covered entity. As with the covered cyber incident reporting requirement described above, CISA interprets this requirement as applying to an entity that is a covered entity during any point in the

incident lifecycle, such that any entity that qualifies as a covered entity for the purposes of the covered cyber incident reporting requirement is also subject to the supplemental reporting requirement to the extent new or different information becomes available.

The second scenario resulting in the requirement to submit a Supplemental Report is when a covered entity makes a ransom payment related to a covered cyber incident for which the covered entity has already submitted a Covered Cyber Incident Report. As with the ransom payment reporting requirement described above, CISA interprets this requirement as applying to an entity that is a covered entity at the time a ransom payment is made, assuming they also were subject to the covered cyber incident reporting requirement described above.

These two scenarios that require the submission of a Supplemental Report are enumerated in §§ 226.3(d)(1)(i) and (ii), respectively.

ii. Reporting of Single Incidents Impacting Multiple Covered Entities

CISA anticipates that occasions will occur where a single cyber incident causes substantial cyber incident-level impacts to multiple covered entities. Who must report and the number of reports that must be submitted in those situations may vary depending on the relationship between the impacted entities.

In cases where a single cyber incident impacts multiple unaffiliated covered entities, each covered entity that experiences substantial cyber incident-level impacts must submit a Covered Cyber Incident Report to CISA. For example, if a compromise of a CSP causes substantial cyber incident level-impacts at multiple unaffiliated customers of the CSP, more than one of whom is a covered entity, then each of the impacted customers that are covered entities are responsible for submitting (or having a third party submit on their behalf) a Covered Cyber Incident Report. The covered entity customers could, however, authorize the CSP to submit Covered Cyber Incident Reports on their behalf under § 226.12(a) if the CSP has or is provided with sufficient information to

complete the Covered Cyber Incident Reports. The CSP may also have to separately submit a Covered Cyber Incident Report if it is itself a covered entity and it experiences threshold impacts that meet the definition of a substantial cyber incident.

Conversely, in cases where a single cyber incident causes substantial cyber incident-level impacts at multiple affiliated covered entities, the covered entities can meet their reporting obligations through either (a) the submission of a single Covered Cyber Incident Report that provides the required information on all of the impacted entities, or (b) multiple Covered Cyber Incident Reports, with one or more covered entities submitting their own reports. Examples of scenarios where multiple affiliated covered entities may experience impacts from a single substantial cyber incident include a substantial cyber incident that impacts a parent corporation and one or more of its subsidiaries; a cyber incident that impacts a number of SLTT Government Entities within the same jurisdiction (e.g., an incident that impacts a single county's general government network, the county's 911 system, and the county's school district network); or a cyber incident affecting a jointly operated venture that impacts downstream systems that are individually owned by members of the joint venture. In these and similar cases, the impacted covered entities may satisfy their reporting requirements under CIRCIA through the submission of a single Covered Cyber Incident Report so long as that report details the impacts experienced by each of the affected covered entities, any other required covered entity-specific details, and point(s) of contact who individually or collectively represent all of the covered entities on whose behalf the Covered Cyber Incident Report is being submitted.

Similarly, in cases where a cyber incident impacts a facility that has separate owners and operators, both of whom qualify as a covered entity, only a single Covered Cyber Incident Report is required. Thus, for example, if a cyber incident impacts a critical access hospital or a Community Water System that is owned by one entity and

operated by another, the reporting obligations of both the owner and operator can be met by a single Covered Cyber Incident Report submitted by (or on behalf of) either the owner or the operator. However, both are separately obligated to ensure that at least one Covered Cyber Incident Report is submitted.

While the examples provided above focus on Covered Cyber Incident Reports, the principles being described apply equally to all types of CIRCIA Reports. Accordingly, if a ransom payment is made on behalf of multiple affiliated entities, a single Ransom Payment Report can be submitted on their collective behalf. Similarly, affiliated entities may opt to submit a single Supplemental Report detailing substantial new or different information that impacts multiple affiliated covered entities. By contrast, if a supply chain compromise results in multiple covered entity customers of a single service provider experiencing a ransomware attack and each paying a ransom payment, each covered entity that makes a ransom payment is responsible for submitting a Ransom Payment Report.

D. Exceptions to Required Reporting on Covered Cyber Incidents and Ransom Payments

Section 681b(a)(5) of title 6, United States Code, contains three scenarios in which a covered entity is excepted from having to report a separate covered cyber incident or ransom payment. The first of these exceptions authorizes a covered entity to submit a single CIRCIA Report containing information on both a covered cyber incident and ransom payment when the covered entity makes a ransom payment related to a covered cyber incident within the 72-hour window for reporting the covered cyber incident. 6 U.S.C. 681b(a)(5)(A). The second exception allows a covered entity to forgo providing an otherwise required CIRCIA Report to CISA if it is legally required to report substantially similar information within a substantially similar timeframe to another Federal agency with whom CISA has an information sharing agreement and mechanism.

6 U.S.C. 681b(a)(5)(B). The third exception states that CIRCIA reporting requirements shall not apply to certain covered entities, or specific functions of those entities, that are owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the DNS. 6 U.S.C. 681b(a)(5)(C). CISA additionally is proposing a fourth exception that would except Federal agencies from having to submit a CIRCIA Report to CISA if the Federal agency is required to report the incident in question to CISA pursuant to FISMA, 44 U.S.C. 3551 *et seq.*

The first exception, which requires the submission of a Joint Covered Cyber Incident and Ransom Payment Report, is discussed in Section IV.E.ii of this document. The following subsections discuss the remaining three exceptions.

i. Substantially Similar Reporting Exception

Pursuant to 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report substantially similar information on a covered cyber incident or ransom payment to another Federal agency in a substantially similar timeframe as that required under CIRCIA does not have to submit a covered cyber incident Report or Ransom Payment Report to CISA on that covered cyber incident or ransom payment if CISA has an information sharing agreement and mechanism in place with that Federal agency. Under that same provision of CIRCIA, a covered entity is excepted from having to submit a Supplemental Report to CISA if the entity is required to provide to another Federal agency substantially similar information to that which the entity would otherwise be obligated to provide to CISA in a Supplemental Report, must do so in a substantially similar timeframe as that required under CIRCIA, and CISA has both an information sharing agreement and mechanism in place with the other Federal agency. This reporting exception (hereinafter the substantially similar reporting exception) will allow covered entities subject to more than one Federal cyber incident

reporting requirement to avoid having to report duplicative information to both CISA and another Federal agency when certain conditions are met.

CISA interprets the statutory language to require five criteria for the application of the substantially similar reporting exception to apply: (1) the report must be required to contain substantially similar information to that required to be included in the applicable CIRCIA report; (2) the report must be required to be provided to the other Federal agency in a timeframe that allows CISA to receive the report in a substantially similar timeframe to that which the covered entity would otherwise have been obligated to provide the report to CISA pursuant to CIRCIA; (3) CISA and the Federal agency to which the covered entity submits the report must have an information sharing agreement in place that satisfies the requirements of 6 U.S.C. 681g(a) (hereinafter a CIRCIA Agreement); (4) CISA and the Federal agency to which the covered entity submits the report must have a mechanism in place by which the Federal agency can share the report with CISA within the required timeframe; and (5) the covered entity must have submitted the report to the other Federal agency pursuant to a legal, regulatory, or contractual obligation.

CISA is proposing to only enter into a CIRCIA Agreement when CISA has determined that the Federal agency with whom CISA is entering into the agreement receives cyber incident reports from one or more CIRCIA covered entities pursuant to a legal, regulatory, or contractual obligation, and the reporting obligation requires the submission of substantially similar information in a substantially similar timeframe.[329] When assessing whether another reporting obligation requires reporting of substantially similar information in a substantially similar timeframe to CIRCIA, CISA intends to

[329] CISA may enter into other information sharing agreements with Federal agencies that do not meet the substantially similar reporting exception criteria; however, such agreements would not be considered CIRCIA Agreements and would not indicate the applicability of the substantially similar reporting exception to entities submitting reports to the Federal entity with which CISA entered into the agreement.

coordinate with the Federal department or agency responsible for the non-CIRCIA reporting obligation which will inform CISA's decision making process.

If and when CISA has entered into a CIRCIA Agreement, CISA will announce and catalogue the existence of the CIRCIA Agreement on a public-facing website. In accordance with 6 U.S.C. 681g(a)(5)(B), to the extent practicable, CISA will publish the full CIRCIA Agreement. The listing of a CIRCIA Agreement by CISA demonstrates that CISA has determined that the applicable law, regulation, or contractual obligation requires a covered entity to report substantially similar information related to a covered cyber incident or ransom payment within a substantially similar timeframe and that the Federal agency has committed to providing the covered entity's report to CISA within the relevant deadlines under this Part. If a covered entity submits a report related to a covered cyber incident or ransom payment to another Federal agency with which CISA has an active and published CIRCIA Agreement, the covered entity's report qualifies for the exception under this section. If no CIRCIA Agreement is listed for a Federal agency, this exception does not apply, and reporting to that Federal agency will not exempt a covered entity from having to report directly to CISA in accordance with this part. A covered entity is responsible for confirming that a CIRCIA Agreement is applicable to both it and the specific CIRCIA reporting obligation that it is seeking to satisfy. CISA generally anticipates that each CIRCIA Agreement will describe or otherwise identify the scope of entities and/or reporting obligations that are the subject of the CIRCIA Agreement.

If a law, regulation, or contract that serves as the basis for a CIRCIA Agreement is modified in any way, CISA may reassess if the respective law, regulation, or contract continues to meet the requirements necessary for that law, regulation, or contract to serve as the basis for application of the substantially similar reporting exception. CISA may terminate a CIRCIA Agreement at any time as long as doing so would not violate any aspect of the agreement itself. If CISA terminates a CIRCIA Agreement for any reason,

CISA will provide notice of the termination on the public-facing website where the catalog of active CIRCIA Agreements is maintained.

1. Substantially Similar Information

To qualify for the substantially similar reporting exception, the information reported by a covered entity on a covered cyber incident or ransom payment to another Federal agency must be substantially similar to the information that the covered entity would be required (but for the exception) to report to CISA under this Part. CISA does not intend to define what constitutes substantially similar information in the final rule. Rather, CISA proposes to retain discretion in making this determination. In determining whether information is substantially similar, CISA will consider whether the information required by the fields in CISA's CIRCIA Report forms is functionally equivalent to the information required to be reported by the covered entity to another Federal agency. CISA views functionally equivalent as meaning that the information or data serves the same function or use, provides the same insights or conclusions, and enables the same analysis as the information or data requested in the relevant CIRCIA Report form fields.

CISA does not believe that the substantially similar information qualifier requires information to be reported in the same format to the other Federal agency. Other Federal agency reporting forms are unlikely to precisely mirror the CIRCIA Report. A covered entity could submit information in another Federal agency's reporting form that, while not directly aligning with a specify query in a CIRCIA Report form, nonetheless provides functionally equivalent data. CISA's determination that information is substantially similar will hinge on whether the data and information required to be submitted in a CIRCIA Report form are substantively included in the report to the other Federal agency.

2. Substantially Similar Timeframe

To qualify for this exception, the covered entity must also be required to report this information to another Federal agency under law, regulation, or contractual provision

in a substantially similar timeframe. In interpreting this requirement, CISA has to keep in mind the limitations related to sharing of reports pursuant to a CIRCIA Agreement, as set forth in 6 U.S.C. 681g(a)(5)(C). Specifically, that section requires that Federal agencies who share reports with CISA pursuant to a CIRCIA Agreement must do so "in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments." 6 U.S.C. 681g(a)(5)(C).

When read together, CISA interprets these statutory requirements to render the substantially similar reporting exception available only if CISA receives the report on a covered cyber incident or ransom payment from the other Federal agency within the same timeframe in which the covered entity would have been required to submit the report to CISA under CIRCIA had the covered entity reported directly to CISA. Thus, for a law, regulation, or contractual provision to require reporting within a "substantially similar timeframe" of CIRCIA, it must require a covered entity to report a covered cyber incident within 72 hours from when the covered entity reasonably believes that the covered cyber incident has occurred and a ransom payment within 24 hours after the ransom payment has been disbursed, leaving the Federal agency time to share the report with CISA, unless a mechanism is in place that allows CISA to receive the report at the same time as the other Federal agency. For example, a law, regulation, or contractual provision that requires a covered entity to report a covered cyber incident to a Federal agency within 36 hours after discovery would have a substantially similar timeframe for the purpose of this exception. The Federal agency would have an additional 36 hours in which to share the report with CISA to meet the CIRCIA deadline for Covered Cyber Incident Reports.[330] If

[330] Of note, CIRCIA separately provides that any Federal agency, including any independent establishment, that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to CISA as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by a CIRCIA Agreement between CISA and the recipient Federal agency. 6 U.S.C. 681g. This requirement would apply to reports that are subject to the substantially similar reporting exception as well, and would therefore be relevant in determining whether a reporting timeframe is substantially similar while allowing for sufficient time for CISA to receive the report from the recipient Federal agency.

a law, regulation, or contractual provision required a covered entity to report a covered cyber incident to a Federal agency within 72 hours of the covered entity reasonably believing a qualifying cyber incident occurred, the Federal agency would need to have a mechanism in place to share the report with CISA instantaneously upon receipt for it to be received by CISA in a substantially similar timeframe in compliance with the deadline for a Covered Cyber Incident Report under this part.

As discussed in Section IV.E.iv.1 of this document, a covered entity must report a covered cyber incident within 72 hours after it "reasonably believes" a covered cyber incident occurred. CISA recognizes that not all incident reporting requirements in law, contract, or regulation have the same trigger for "starting the clock" on when an incident becomes reportable, and that different triggers could result in dramatically different reporting timeframes even if the numerical timeframes were substantially similar. For instance, a regulation that requires reporting within 24 hours of confirmation of a reportable incident could in fact have a reportable timeframe that effectively is substantially longer than CIRCIA's 72-hour reporting timeframe as "confirmation" of a reportable incident could occur days or weeks after a "reasonable belief" that a reportable incident occurred is established. In determining whether to enter into a CIRCIA Agreement with another Federal agency, CISA will take into account when the reporting timeframe is triggered under the governing law, regulation, or contract.

3. Supplemental Reporting

Supplemental Reports may also qualify for the substantially similar reporting exception, provided that the supplemental report provided to the other Federal agency meets the relevant requirements. As with a Covered Cyber Incident Report or Ransom Payment Report, the exception is only available if the covered entity is required to submit substantially similar information in a substantially similar timeframe to another Federal agency under law, regulation, or contract and CISA and the other agency have a CIRCIA

Agreement and information sharing mechanism in place to meet the CIRCIA Report deadlines. CIRCIA requires Supplemental Reports be submitted "promptly," which CISA interprets as within 24 hours of the triggering event. See 6 U.S.C. 681b(a)(3) and Section IV.E.iv.3.a of this document. A covered entity remains responsible for submitting Supplemental Reports to CISA as required under this Part unless the covered entity submits any substantial new or different information to another Federal agency and CISA has published a CIRCIA Agreement with that Federal agency that specifically covers Supplemental Reports.

4. Communications with CISA

The exception under this section does not prevent CISA from contacting the covered entity about the information it provided to the other Federal agency. 6 U.S.C. 681b(a)(5)(B)(iii). Moreover, nothing in this section prohibits a covered entity from also submitting a CIRCIA Report to CISA even if the CIRCIA Report is qualified for an exception. 6 U.S.C. 681b(a)(5)(B)(iii)).

5. Request for Comments

CISA seeks comments on its proposed approach to implementing the substantially similar reporting exception, to include:

38. CISA's proposed interpretations of what constitutes substantially similar information and a substantially similar timeframe.
39. The application of the substantially similar reporting exception to Supplemental Reports.
40. The manner in which CISA proposes informing the public of the availability of this exception.
41. Any other aspects of the substantially similar reporting exception.

ii. Domain Name System (DNS) Exception

Pursuant to 6 U.S.C. 681b(a)(5)(C), the CIRCIA reporting requirements "shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority." Based on this language, CISA is proposing to create an exception from CIRCIA reporting requirements for ICANN, the American Registry for Internet Numbers (ARIN), and affiliates of those entities. CISA additionally proposes to create a limited exception from CIRCIA reporting requirements for the DNS Root Server Operator (RSO) function of a covered entity.

To qualify for the reporting exception provided in 6 U.S.C. 681b(a)(5)(C), a covered entity must have been determined by the Director to meet two criteria. First, the Director must have determined that the covered entity constitutes critical infrastructure. Second, the Director must have determined that the covered entity, or a specific function of that entity, is owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS. As very few entities meet the second criterion, it is more efficient to begin CISA's analysis on this topic by considering the second criterion first.

To determine what covered entities might meet the second criterion, CISA assessed the DNS ecosystem to identify multi-stakeholder organizations that develop, implement, and enforce policies concerning the DNS and to identify entities that are wholly owned, operated, or governed by such multi-stakeholder organizations. Based on this assessment, CISA believes that two specific entities meet this criterion, and a third category of entities meet the criterion as well.

The first entity that CISA has assessed is a multi-stakeholder organization that develops, implements, and enforces DNS policies is ICANN. ICANN is a not-for-profit,

multi-stakeholder organization that leads the development of bottom-up, consensus policies and guidelines that help advance the stable and secure operation of the internet's unique identifier systems and help define how the DNS functions.[331]

The second entity that CISA has assessed as meeting this criterion is Public Technical Identifiers (PTI). PTI is a 501(c)(3) non-profit whose specific purpose is to operate exclusively to carry out the purposes of ICANN, which is a multi-stakeholder organization.[332] PTI is an affiliate of ICANN that is wholly controlled by ICANN, akin to complete ownership, thus meeting the "owned, operated, or governed by" a multi-stakeholder organization clause contained within CIRCIA's statutory reporting exception.

The third group of covered entities that are multi-stakeholder organizations with responsibilities related to the development, implementation, and enforcement of DNS policies are Regional Internet Registries (RIRs). RIRs are multi-stakeholder organizations responsible for managing, distributing, and registering internet number resources (IPv4 and IPv6 address space and Autonomous System (AS) Numbers) within their respective regions.[333] Currently, there are five RIRs in the world: (1) the African Network Information Centre (AFRINIC), which services Africa and the Indian Ocean; (2) the Asia-Pacific Network Information Centre (APNIC), which services Asia and the Pacific; (3) ARIN, which services the United States, Canada, and many Caribbean and North Atlantic Islands; (4) the Latin American and Caribbean Internet Addresses Registry (LACNIC), which services Latin America and the Caribbean; and (5) the Réseaux IP Européens Network Coordination Centre (RIPE NCC), which services Europe, the Middle East, and parts of Central Asia.[334] Since ARIN is the only RIR with a legal

---

[331] See ICANN, *Policy Mission*, https://www.icann.org/resources/pages/mission-2012-08-27-en (last visited July 24, 2023); see also ICANN, *ICANN For Beginners*, https://www.icann.org/get-started (last visited July 24, 2023).

[332] See PTI Articles of Incorporation Sections II and III. The PTI Articles of Incorporation are available at https://pti.icann.org/articles-of-incorporation (last visited Nov. 13, 2023). See also later discussion of the IANA functions.

[333] See NRO, *Regional Internet Registries*, https://www.nro.net/about/rirs/ (last visited July 24, 2023).

presence in the United States, CISA has assessed that ARIN is the only relevant RIR for purposes of CIRCIA.

Finally, CISA assessed whether the CIRCIA reporting exception should apply to any specific function of a covered entity that is owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS. Given the RSO's role in operationalizing a specific, critical IANA function of overseeing operation of the internet root server system, CISA has assessed that the DNS RSO function also meets this criterion.

The Internet Assigned Numbers Authority functions (IANA functions) are administered by PTI, which is owned by ICANN, a multi-stakeholder organization responsible for development, implementation, and enforcement of policies concerning the DNS.[335] One of the key IANA functions is the management of the DNS root zone.[336] The "root zone" is the upper-most part of the DNS hierarchy.[337] The root zone management function uses the Root Server System (RSS) for publication of the root zone. The RSS is administered collectively by the RSOs, which serve as the authorities for each of the A, B, C, D, E, F, G, H, I, J, K, L, and M root servers. The root servers operated by the RSOs act exclusively as a mechanism by which the content of the root zone database is made publicly available. This activity is largely viewed by the DNS ecosystem as an operationalization of the historic IANA root zone management function on behalf of ICANN.[338] ICANN manages matters related to the operation, administration, security, and integrity of the internet root server system through the Root Server System Advisory

---

[334] *Id.*
[335] See USC/ICANN Transition Agreement, ICANN, available at https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en.
[336] See IANA, *Root Zone Management*, https://www.iana.org/domains/root (last visited Nov. 14, 2023).
[337] See IANA, *Domain Name Services*, https://www.iana.org/domains (last visited Nov. 15, 2023).
[338] See IANA, *Root Zone Management*, https://www.iana.org/domains/root (last visited Nov. 14, 2023); see also ICANN, *Brief Overview of the Root Server System*, at 4 (May 6, 2020), available at https://www.icann.org/en/system/files/files/octo-010-06may20-en.pdf ("The 13 root services respond to the queries they receive either with information found in the root zone as it is managed by the IANA Functions operated by ICANN…").

Committee (RSSAC), which is an advisory committee created by ICANN to advise the ICANN community and board.[339] As part of RSSAC's advice, it has also defined a set of service expectations that RSOs have agreed to satisfy.[340]

CISA has assessed that the RSO function is an operationalization of ICANN's responsibility to operate the internet root server system and thus qualifies as a "function[] of a covered entity . . . owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority." Accordingly, CISA has assessed that the RSO function of a covered entity that has been recognized by ICANN as responsible for operating one of the 13 root identities and agrees to follow the service expectations established by the RSSAC and ICANN may qualify for the DNS Exception, if the second criterion for the DNS Exception is met, (i.e., whether the function also constitutes critical infrastructure).[341]

Note, to the extent the proposed DNS Exception may apply to a covered entity that is an RSO, it would only apply to the RSO function of the entity. Other functions performed by an RSO that are not the RSO function would not qualify for the proposed DNS Exception under CIRCIA. Accordingly, should an RSO that is also a covered entity experience a covered cyber incident or make a ransom payment as the result of a ransomware attack that impacts the entity's activities or business streams that are separate

---

[339] You can find more information about the RSSAC at https://www.icann.org/groups/rssac#:~:text=Root%20Server%20System%20Advisory%20Committee%20%20%20,31%20December%202024%20%208%20more%20rows%20 (last visited Nov. 28, 2023).
[340] RSSAC001, Service Expectations of Root Servers, Version 1 (Dec. 4, 2015) available at https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf.
[341] There currently are 12 RSOs that perform the IANA root zone management function: Verisign, Inc.; the University of Southern California, Information Sciences Institute; Cogent Communications; the University of Maryland; NASA; Internet Systems Consortium, Inc.; the U.S. Department of Defense (NIC); the U.S. Army Research Lab; Netnod; RIPE NCC; ICANN; and WIDE Project. Verisign, Inc. manages two of the root identities. See IANA, *Root Servers*, https://www.iana.org/domains/root/servers (last visited Nov. 14, 2023).

from, or in addition to, its RSO function, the covered entity would be required to report that covered cyber incident or ransom payment under this proposed regulation.

For a covered entity to be eligible for an exception from CIRCIA reporting requirements under the proposed DNS Exception, it must also meet the first criterion included in the statutory language—i.e., be determined by the Director to constitute critical infrastructure. The USA Patriot Act (Pub. L. 107-56) and, by reference, both the Homeland Security Act of 2002, as amended, and PPD-21 define "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[342] Given their roles in ensuring the functioning of the DNS around the world, and the debilitating impacts a significant failure of the DNS would have on national security, economic security, or public health, and safety, the Director has determined that ICANN, ARIN, and their affiliates[343] (such as PTI) meet the definition of critical infrastructure for purposes of applying this statutory exception. The Director also has determined that, given the criticality of the DNS root zone to the operation of the internet, the RSO function performed by a covered entity qualifies as critical infrastructure as well.

Based on the aforementioned analysis, ICANN, ARIN, any affiliates of ICANN or ARIN (such as PTI), and the RSO function of covered entities meet both criteria contained in the statute for the DNS Exception. Accordingly, CISA proposes in § 226.4(b) that ICANN, ARIN, and their affiliates do not need to report to CISA covered cyber incidents that they experience or ransom payments they make as the result of a

---

[342] 42 U.S.C. 5195c(e).

[343] "Affiliates" in this context is meant to reflect entities that have been recognized by ICANN or IANAARIN as an affiliate and are so significantly controlled by ICANN or ARIN that the average non-technical individual might actually consider them to be part of ICANN or ARIN.

ransomware attack. CISA further proposes to exempt a covered entity from CIRCIA reporting requirements for covered cyber incidents and ransom payments made as a result of a ransomware attack that solely relate to the entity's RSO function.

Given the complexities of the DNS, as well as the long-standing U.S. Government policy goal of support of the multi-stakeholder approach to internet governance that may impact other entities in this space, CISA recognizes the importance of public feedback on the scoping of this reporting exception consistent with the legal requirements in 6 U.S.C. 681b(a)(5)(C) and the purposes for which CIRCIA has been established. In particular, CISA welcomes comments on all aspects of this topic. Among other things, CISA welcomes comments on the possible application of the DNS exception to domain name registries and registrars, and of all associated questions of law and policy. CISA will give extreme careful consideration to alternative views, including the possible application of the DNS exception to domain name registries and registrars. Consistent with Executive Order 13563, CISA is strongly committed to public participation, to maintaining openness, and to serious assessment of alternative approaches that might better balance the relevant interests. CISA invites submission of views, information, data, and comments on the following policy and legal questions that are unique to the DNS community:

42. The covered entities which CISA proposes this exception apply to, including whether any additional covered entities involved in DNS operations, such as domain name registries and registrars, should be considered by CISA for this reporting exception. If so, how do those covered entities, or specific functions thereof, meet the statutory requirements, including specifically how the entity or its functions may "constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet

Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority"?

43. Information, facts, or other views that describe or explain the relationship between ICANN and domain name registries and registrars, as well as specific cyber incident and ransom payment information that must be reported to ICANN by entities accredited by ICANN.
44. What types of covered cyber incidents could be unique to, or have a unique impact on, the covered entities that would be exempt from reporting under CIRCIA based on the scoping of the proposed DNS Exception?
45. What are the potential consequences of covered cyber incidents that would not be reported to CISA based on the proposed DNS Exception (e.g., impacts to the functionality of the internet or to services offered to critical infrastructure)?
46. What are the specific technical functions that DNS entities perform or provide in order to support the DNS versus related, but separate commercial offerings? How would this apply to different DNS entities such as root server operators, domain name registries, and domain name registrars?
47. What cyber incident reporting requirements, either in the United States or internationally, are DNS entities currently subject to? To what government agency or other entity must those entities report cyber incidents? Please describe the specific cyber incident reporting requirement (e.g., timing and trigger requirements; details that must be reported; mechanism for reporting; supplemental reporting requirements).
48. How should the U.S. government's support for the multi-stakeholder system of internet governance inform the DNS Exception?
49. Any other aspects of CISA's proposed approach to the DNS Exception.

iii. Exception for Federal Agencies Subject to Federal Information Security Modernization Act Reporting Requirements

CISA also is proposing to exempt Federal agencies required by FISMA (44 U.S.C. 3551 *et seq.*) to report incidents to CISA from reporting those incidents as covered cyber incidents under CIRCIA. FISMA requires Federal agencies (as defined in 44 U.S.C. 3502), except for systems identified in 44 U.S.C. 3553(d) and (e), to notify CISA regarding information security incidents involving their information and information systems, whether managed by a Federal agency, contractor, or other source.

While the definition for substantial cyber incident under the CIRCIA regulation will not be finalized until CISA completes the rulemaking process, CISA anticipates that all incidents that ultimately will constitute substantial cyber incidents would also be considered reportable incidents under FISMA if experienced by a Federal agency. Similarly, CISA anticipates that the content that Federal agencies must submit in reports required under FISMA will be substantially similar to the information required in CIRCIA Covered Cyber Incident Reports. Finally, FISMA requires reporting by Federal agencies to CISA in a shorter timeframe—one hour from the time of identification of the incident—than is required under CIRCIA. In light of this, CISA expects to already be receiving substantially similar information from FISMA-covered Federal agencies on all substantial cyber incidents within a shorter timeframe than required by CIRCIA. For these reasons, CISA is proposing to exempt FISMA-covered Federal agencies that are required by FISMA to report incidents to CISA from having to submit a CIRCIA Report for those incidents that constitute covered cyber incidents. Per the terms of this exception, as proposed in § 226.4(c), this exception only applies to Federal agencies, and does not exempt government contractors or subcontractors from any otherwise-required CIRCIA reporting.

Other cyber incident reporting regulations may exist for which entities may be required to provide other Federal departments or agencies with similar information about substantial cyber incidents in a similar or shorter timeframe than that which is required under CIRCIA. CISA is not offering a similar exclusion to entities based on those reporting requirements. CISA is proposing to exclude Federal agencies subject to cyber incident reporting under FISMA, but not entities subject to other Federal cyber incident reporting requirements, because CISA believes FISMA differs from those other regulations in two important ways. First, because CISA is the Federal entity responsible for implementing FISMA, CISA has control (within the boundaries of any limitations established by Congress in the FISMA authorizing legislation) over the types of incidents that must be reported, the content that must be included in those reports, and the timeframe for submission of those reports. CISA does not have similar control over those aspects of reporting required by other regulatory programs. As a result, CISA has no ability to ensure that those regulatory programs continue to require incident reports with substantially similar information for substantial cyber incidents in a substantially similar timeframe. Second, because the statutory requirements for using the substantially similar reporting exception—e.g., the information is required to be reported "to another Federal agency"—explicitly address situations involving CISA and a different Federal regulator, CISA is unable to leverage the substantially similar reporting exception to avoid duplicative reporting for requirements such as FISMA where CISA is the entity responsible for overseeing the reporting requirement. To avoid duplicative reporting requirements in situations where CISA is the entity receiving reports under two requirements, CISA needs to specifically exempt entities subject to those requirements from CIRCIA reporting requirements or otherwise make it clear in either the CIRCIA regulations or the other reporting requirements that submission of a CIRCIA Report satisfies both reporting requirements. For reporting requirements that require reporting to

a different Federal agency, the substantially similar reporting exception is the proper approach for seeking to avoid duplicative reporting requirements.

To the extent other regulations exist that require a covered entity to submit cyber incident reports containing substantially similar information to that required in CIRCIA Reports to another Federal entity in a substantially similar timeframe to that required under CIRCIA, CISA intends to work with that Federal entity to explore the possibility of enabling the covered entity's submission to the other Federal entity to satisfy the covered entity's CIRCIA incident reporting requirements. This would be done consistent with the substantially similar reporting exception authorized in 6 U.S.C. 681b(a)(5)(B) of CIRCIA. Additional information on the substantially similar reporting exception, and the process CISA will undertake to implement it, can be found in Section IV.D.i of this document.

CISA seeks comments on its proposed exception for Federal agencies subject to FISMA reporting requirements, to include:

50. The establishment of the FISMA reporting exception.
51. Any aspects of CISA's proposed approach to implementing the FISMA reporting exception.

E. Manner, Form, and Content of Reports

i. Manner of Reporting

1. Overview

Pursuant to 6 U.S.C. 681b(a)(6) of CIRCIA, covered entities must make CIRCIA Reports in the manner and form prescribed in the final rule. CIRCIA requires CISA to include procedures for submitting these reports in the final rule, including the manner and form thereof. 6 U.S.C. 681b(c)(8)(A). CIRCIA gives CISA broad discretion in determining the manner and form for submission of CIRCIA Reports, although 6 U.S.C.

681b(c)(8)(A) requires CISA to "include, at a minimum, a concise, user-friendly web-based form" as one manner for submission of required reports.

CISA has direct experience using a web-based form to receive cyber incident reports, as that is the primary manner in which CISA has been receiving cyber incident reports from external stakeholders for a number of years. CISA also has experience receiving voluntarily submitted cyber incident reports from stakeholders telephonically and via email.

A variety of means for submitting cyber incident reports are currently in effect across the numerous Federal departments and agencies that require entities to report cyber incidents to them. A number of Federal departments and agencies use a web-based form or similar online submission system as the sole mechanism or one option for submitting required cyber incident reports. These include, among others, DOD,[344] DOE,[345] TSA,[346] SEC,[347] and the NRC.[348] Other commonly allowed methods for the

---

[344] See DOD – Defense Industrial Base Cyber Security Activities, 32 CFR 236.4(b)(2) (reports must be made electronically through https://dibnet.dod.mil). DOD does offer reporting telephonically if the dibnet is unavailable. See Defense Industrial Base Cybersecurity Portal Frequently Asked Questions, available at https://dibnet.dod.mil/portal/intranet/#faq-4.

[345] DOE has established mandatory reporting requirements for electric emergency incidents and disturbances, to include those caused by cyber incidents. Entities within the electric power industry that have reportable incidents must use Form DOE-417 to report those incidents. DOE prefers that the form be submitted online through the DOE-417 Online System at https://www.oe.netl.doe.gov/OE417/, although DOE will also accept submissions via fax, telephone, or email. See DOE-417 Electric Emergency Incident and Disturbance Report (OMB No.: 1901-0288) at 1, available at https://www.oe.netl.doe.gov/oe417.aspx.

[346] See, e.g., *Security Directive 1580-21-01 – Enhancing Rail Cybersecurity*, Section B.3 ("Reports required by this section must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870."); *Security Directive 1582-21-01 – Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Section B.3 ("Reports required by this section must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870."); *Security Directive Pipeline-2021-01 – Enhancing Pipeline Cybersecurity*, Section C ("Reports must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870."). Copies of these security directives are available at https://www.tsa.gov/sd-and-ea.

[347] Regulation SCI Entities are required to use the Form SCI to notify the SEC of reportable incidents. A pdf version of Form SCI can be found at https://www.sec.gov/files/form-sci.pdf (last visited Nov. 28, 2023). Form SCI can be filed in an electronic format through the Electronic Form Filing System, a secure website operated by the SEC that can be accessed at https://tts.sec.gov/effs/do/Index.

[348] The NRC's Cyber Security Event Notifications regulations require covered licensees to provide the NRC with initial notifications of cybersecurity events telephonically to the NRC Headquarters Operations Center via the Emergency Notification System. 10 CFR 73.77(c). For certain types of cyber security events, licensees must provide the NRC with written security follow-up reports using NRC Form 366. 10 CFR 73.77(d)(3). A copy of the web-based version of NRC Form 366 can be found at https://www.nrc.gov/docs/ML1308/ML13083A106.pdf (last visited Nov. 28, 2023).

submission of cyber incident reports include telephone, email, and automated (i.e., machine-to-machine) reporting.[349] At least one regulator does not articulate specific manners in which regulated entities must submit reports to it, leaving the manner up to the discretion of the reporting party.[350]

A majority of comments on this topic provided by stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions indicated support for the use of a web-based portal as a means for submission of reports to CISA. Some commenters recommended offering a web-based portal as either the only means or the preferred means of submission, while others suggested offering the web-based portal as simply one means of submission. One reason often provided by commenters advocating for the web-based portal to be one of multiple mechanisms for reporting was to ensure the existence of an alternative method of reporting should a covered cyber incident have rendered it difficult for the covered entity to submit a report via a web-based portal. Commenters expressing this rationale often suggested telephonic reporting as the recommended alternative option. A small number of commenters recommended that CISA offer the ability for covered entities to use automated (i.e., machine-to-machine) reporting, email,

---

[349] See, e.g., Federal Reserve Board, *Computer-Security Incident Notification Requirements*, 12 CFR 225.302 ("A banking organization must notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe."); Office of the Comptroller of the Currency, *Computer-Security Incident Notification Requirements*, 12 CFR 53.3 ("A banking organization must notify the appropriate OCC supervisory office, or OCC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the OCC may prescribe."); Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Requirements*, 12 CFR 304.23 ("A banking organization must notify the appropriate FDIC supervisory office, or an FDIC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the FDIC may prescribe."); NCUA, *Cyber Incident Notification Requirements for Federally Insured Credit Unions Proposed Rule*, 87 FR 45029 (proposed rule would require "[e]ach federally insured credit union must notify the appropriate NCUA-designated point of contact of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that the NCUA may prescribe."); see also FCC-NORS, 47 CFR part 4 (regulated entities can submit reports automatically through an approved NORS Application Programming Interface).

[350] See, e.g., Commodity Futures Trading Commission Designated Contract Markets System Safeguards regulations, 17 CFR 38.1051(e)(2) (requires designated contract markets to promptly notify CFTC staff of certain cybersecurity incidents, but does specify how notifications must be provided), 39.18(g) (requires derivatives clearing organizations to promptly notify CFTC staff of certain security incidents). While the CFTC's regulations do not specify how notifications must be provided, the CFTC has a portal for such notifications that is available to registrants.

or submit through other Federal departments or agencies' field office locations. See Section III.F.vi in this document for a summary of stakeholder comments on the manner and form of submission of CIRCIA Reports.

2. Proposed Approach

Section 226.6 of the proposed rule contains CISA's proposal for the manner of submission of CIRCIA Reports. CISA is proposing that a covered entity must submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner approved by the Director.

As noted earlier, CIRCIA requires CISA to offer a web-based form as one manner of submission of CIRCIA Reports. See 6 U.S.C. 681b(c)(8)(A). Not only does CISA intend to offer a web-based form as a manner of submission of CIRCIA Reports, for several reasons CISA agrees with those commenters who suggested that an electronic, web-based form is the preferred manner for submission of CIRCIA Reports. First, a web-based form is a cost-effective way to gather information from large numbers of submitters both simultaneously and over time. If designed properly, it allows for significant standardization of data (in both form and content) and tailoring of circumstance-specific questions using dynamic prompts and responses incorporating conditional logic filters and conditional or branching questions. A web-based form can also reduce the likelihood of human error during the data submission process in various ways. For example, submission methods such as via telephone call require at least two individuals to facilitate the submission (i.e., one person from the covered entity to provide CISA with information on the incident and another person from CISA to transcribe the information into CISA's information management system) and create the possibility of human error if one individual mishears, misspeaks, erroneously transcribes, or otherwise unintentionally enters incorrect data into the system. This is especially problematic for some of the data that CISA expects covered entities may often need to

report, such as malware hashes or IP addresses, which typically are long strings of numbers and/or letters. A web-based form only requires the involvement of a single individual (i.e., the person entering the information into the form on behalf of the covered entity) and allows for that individual to review information after entry but prior to submission, greatly reducing the potential for such errors.

Similarly, by using drop-down menus, radio buttons, or other limited response options where feasible and appropriate, a web-based form reduces the likelihood of human error resulting from the submitter not understanding the types of responses a question is seeking or CISA not understanding a narrative answer provided by a submitter. Third, a web-based form both allows for greater standardization of responses and does so in a machine-readable format, and, in doing so, it facilitates a number of activities that are much more challenging when data is submitted in other manners. These activities include automated triage of reports; rapid, large-scale trend analysis; timely information sharing; and long-term storage, many of which CISA is required by CIRCIA to perform. Finally, a web-based form enables the submission of digital artifacts (e.g., malware samples), which cannot be transmitted verbally.

Conversely, web-based forms present only a small number of potential drawbacks, each of which CISA believes are easily addressed. First, the government will incur costs to develop, maintain, and implement a web-based form. Depending on the options selected, existing resources, and other factors, the governmental costs associated with developing, maintaining, and implementing a web-based form may be greater or less than other potential methods of submission. In this case, however, the issue is effectively moot because, as noted earlier, CIRCIA requires that CISA offer a web-based form as a manner of submission. Consequently, CISA will have to incur the costs associated with a web-based form regardless of whether it is the sole, primary, or one of many options.

Second, a cyber incident at a covered entity could make it impossible or insecure for a covered entity to use its own information system(s) to report via a web-based form. CISA believes that this is a relatively minor concern, however, as organizations and individuals today typically have a variety of ways to access the internet. Additionally, CISA intends to make the web-based form available via a web browser so that incident reports can be submitted from any internet-connected device. This should allow covered entities various ways to access the form even if the entity's IT system is rendered inoperable by a cyber incident. Furthermore, CIRCIA permits a third party to submit CIRCIA Reports on a covered entity's behalf, such that even if the covered entity itself cannot report via a web-based form using its own information system(s) or any other internet connected device, any number of third parties should be able to submit the CIRCIA Report on the covered entity's behalf.

Third, there is the potential that an incident at CISA could render the web-form unavailable for use by covered entities for a period of time. CISA has extensive experience building systems that operate with high availability and intends to build in redundancy to ensure the 24/7 availability of the reporting system. CISA also intends to maintain a capability to support reporting via telephone as a back-up option so that, in the unlikely event of an extended interruption of the availability of the web-based form, any impacted covered entities will have an alternative mechanism available to submit CIRCIA Reports in a timely manner. This or any other approved alternative mechanism also may be used in lieu of the web-based reporting system should a covered entity wish to submit a CIRCIA Report during any short-term unavailability of the system, such as if CISA must temporarily restrict access to the web-based form for routine maintenance.

On balance, CISA believes that the web-based form is the most useful and cost-effective manner for the submission and receipt of CIRCIA Reports and is proposing that

as the sole explicitly identified option for submission of CIRCIA Reports.[351] CISA is also proposing to include in the rule the statement that covered entities may also submit CIRCIA Reports in any other manner and form of reporting approved by the Director. This provision would allow CISA to operate a telephonic reporting capability as a backup system and maintain flexibility to offer alternative manners of submission in the future on a short- or long-term basis. CISA believes that this flexibility is important for several reasons.

First, as mentioned in the previous paragraph, in the unlikely event of an extended interruption of the availability of the web-based form or other situation that renders it impossible for an entity to submit via the web-based form, this phrase would allow CISA the flexibility to establish other means to accept CIRCIA Reports in a rapid fashion. Second, as discussed further below, CISA believes that automated (i.e., machine-to-machine) reporting has the potential to be a cost-effective method for some covered entities to submit CIRCIA Reports in the future. The "any other manner and form of reporting approved by the Director" clause will allow CISA the agility to more rapidly authorize entities to submit CIRCIA Reports via machine-to-machine reporting should CISA determine that is a viable, cost-effective approach in the future without having to undertake additional rulemaking. Similarly, this provision will allow CISA the flexibility to consider and adopt new submission mechanisms that may become feasible as technology advances. CISA will publicize any additional manners of submission on its website and through notifications to stakeholders should the CISA Director approve any.

3. Additional Reporting Methods Options Considered

In deciding upon this proposed approach, CISA considered numerous options in addition to a web-based form. The additional options CISA considered are detailed in the

[351] For similar reasons, CISA is considering encouraging entities that submit voluntary reports to CISA to do so through the CIRCIA web-based form; however, as noted in Section III.A, CISA is not proposing to address entirely voluntary reporting, including how such reports may be submitted, in this rulemaking.

following subsections. Each option has drawbacks that led CISA to determine not to offer them as a manner of submission at this time with the potential exception of a backup capability should the web-based form become unavailable for a period of time.

a. Telephone

One alternative manner CISA considered was telephonic submission of reports. Under this approach, a covered entity would be able to call CISA and verbally report the incident to CISA via telephone. To ensure that all of the necessary information is submitted and that the information is stored and made available to CISA in a manner consistent with the web-based form manner of submission, a CISA representative would ask the caller all of the pertinent questions in the web-based form and simultaneously fill out the web-based form on the caller's behalf.

The primary benefits of this approach include the ubiquity of and familiarity individuals have with telephones, their ease of use, the ability for a covered entity and a CISA representative to directly engage during the reporting process, the ability for CISA to ensure all necessary information is being submitted (including by asking real-time follow up questions), and the ability for CISA to ultimately capture information in a manner compatible with the statutorily required web-based form submissions. A few significant downsides with this approach exist, however. The first is the potentially significant additional cost to the government of manning a 24/7 telephone operation at a scale large enough to handle the receipt of all CIRCIA Reports. The second drawback is the added layer of potential transcription error introduced by requiring an individual other than the covered entity representative to physically enter the information into the web-based form. Beyond the potential for transcription error, it would likely take more time for a CISA telephone operator to solicit, transcribe, and validate the information with the covered entity than to have a covered entity enter the same information directly into a web-based form.

In light of these drawbacks, CISA is not proposing to include telephonic reporting as a primary option. CISA does, however, intend to maintain telephonic reporting capabilities as a back-up option in case a covered entity is unable to submit a CIRCIA Report using the web-based form for some legitimate reason, such as an outage affecting the availability of the web-based form.

b. Email

CISA also considered the submission of CIRCIA Reports via email. Email could be used in two primary ways for the submission of reports. First, CISA could allow covered entities to use email to submit a standardized form (e.g., a fillable PDF form or a paper form that an entity could scan and attach to an email). Second, CISA could allow covered entities to submit required information via text contained in the body of the email itself without requiring any specific format or template be used.

Offering either manner of email submissions would provide a number of benefits. For instance, given the ubiquity of email in today's society and its availability on mobile devices, employees of covered entities are likely to have both familiarity with and access to email even if a cyber incident has rendered a covered entity's information systems inoperable. Similarly, email is a standard part of CISA operations, so CISA would be able to easily establish a mechanism to receive email submissions without having to expend significant upfront costs. Email generally also comes with automated tracking (via sent email folders), which can help the covered entity provide proof that a report has been submitted and the time and date of the submission.

There are, however, several major drawbacks associated with email submissions. First, as opposed to a web-based form where CISA could require certain questions be answered for the form to be submitted, or a telephone submission where a CISA employee could directly interact with the submitter to ensure all necessary information is provided, email does not provide a means for CISA to ensure that all required

information is submitted before the report is made. Consequently, CISA envisions email submissions would result in a potentially significant number of cases in which CISA would need to follow up with the covered entity to obtain required information. Limiting the use of email as a mechanism for the submission only of a fillable reporting form might somewhat reduce the need for follow-up when compared to allowing unbound email submissions; however, CISA believes this likely still would occur frequently.

Second, regardless of which email submission approach is used, CISA would be required to establish and implement processes to transfer data from the email submissions into an online case management system so that CIRCIA Reports submitted via email could be consolidated, analyzed, stored, etc., in a similar way as CIRCIA Reports submitted via the web-form or other subsequently approved mechanisms. These additional activities are likely to result in significant additional implementation costs for CISA, increase the amount of time it takes for CISA to receive necessary details about cyber incidents and ransom payments, and introduce an additional vector for error during the transcription or conversion of the data.

Third, email generally is not a secure form of transmission. Using unsecured email would increase the likelihood that an individual outside of the covered entity and CISA could gain access to potentially sensitive information on the covered cyber incident or ransom payment being reported, especially if the threat actor has compromised the covered entity's email system. CISA also would not be able to ensure that email submissions are protected at the level required by 6 U.S.C. 681e. Another challenge is the potential security concerns associated with receiving an email attachment from an entity that is compromised at the time of sending the email. CISA would be unable to guarantee the safety of the attachment and could be opening itself up to a security risk by accepting the email. Security measures CISA may implement to protect itself from such risks, as well as cybersecurity measures CISA has in place as a matter of routine, have the

potential to block an email or attachment from making it to CISA, creating the possibility that a covered entity could take all steps intended to comply with their reporting obligation with CISA not receiving the CIRCIA Report.

Given these significant operational challenges, potentially substantial additional costs, and limited benefit associated with email submission above other options, CISA is not proposing email as a submission option at this time.

c. Fax

A fourth potential mechanism for covered entities to submit CIRCIA Reports would be via fax, which could be done by completing a report on paper and submitting it to CISA via fax machine or by submitting a fax electronically via an online faxing service or application. The primary benefit of offering faxing as a means of submission is that for many organizations, fax machines are separate from an organization's IT systems and thus may be available even when a cyber incident renders reporting via a web-based form or company email system unavailable. This benefit is somewhat limited these days, however, as fewer entities maintain actual fax machines as a means of communications, and online faxing services or applications are presumably no more likely to be an available and secure mechanism for an entity experiencing a cyber incident than reporting via a web-based form or company email system.[352]

Moreover, much like with email submissions, CIRCIA Reports submitted via fax would not provide a means for CISA to ensure that all required information is provided at the time of the submission. Consequently, CISA expects this could result in a large number of cases where CISA would need to follow up with the covered entity to obtain required information or validate the information received (e.g., in the event that

[352] See, e.g., Ashifa Kassam, *The Outdated Machine Hampering the Fight Against Covid-19*, BBC Future (Sept. 5, 2021) ("By 2000, fax's role in business was declining as companies switched to email and the internet to share information. But in other sectors, such as healthcare and real estate, the fax machine has stubbornly clung on."), available at https://www.bbc.com/future/article/20210903-how-covid-19-could-finally-be-the-end-of-the-fax-machine.

handwriting is illegible). CISA also would have to manually review and upload all submissions into an online case management system so that CIRCIA Reports submitted via fax could be consolidated, analyzed, stored, etc. in a similar way as CIRCIA Reports submitted via the web-form or other approved submission mechanisms. These additional activities are likely to result in additional implementation costs for CISA, increase the amount of time it takes for CISA to receive necessary details about the cyber incident or ransom payment, and introduce an additional vector for human error during the transcription or conversion of the data. Finally, faxing is generally considered insecure, with outdated protocols, and data that is typically transmitted without encryption.[353] For these reasons, CISA is not proposing faxes as a means for submitting CIRCIA Reports.

d. U.S. Mail or other Physical Delivery Service

Another potential means for covered entities to submit CIRCIA Reports could be the delivery of physical, written reports using the U.S. Mail or other physical delivery service (e.g., United Parcel Service, Federal Express, or a local courier). While this approach has the potential benefit of remaining available when a covered entity's information systems have been rendered unavailable or insecure due to the reportable incident, there are significant drawbacks associated with this mechanism of submission that likely would outweigh any associated benefits. Chief among these is the significant increase in the amount of time it likely would take for CISA to physically receive the submission from the covered entity. Depending on the service and postage used, it can take days for something sent via U.S. Mail or other delivery services to arrive at its destination. Even if overnight delivery service or local courier services were used, items delivered to a Federal agency such as CISA typically have to undergo security screening that frequently delays delivery to the intended office. These resulting delays could

[353] See, e.g., Lily Hay Newman, *Fax Machines Are Still Everywhere, and Wildly Insecure*, Wired (Aug. 12, 2018), available at https://www.wired.com/story/fax-machine-vulnerabilities/.

significantly impact the ability of CISA to achieve some of its statutory requirements, such as providing appropriate entities with timely, actionable, and anonymized reports of cyber incident campaigns and trends and immediately reviewing certain reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders. See 6 U.S.C. 681a(a)(3)(B), 681a(a)(7).

Much like with email and fax submissions, mail submission also does not provide a means for CISA to ensure that all required information is provided at the time of the submission. Consequently, CISA expects this would result in a number of cases where CISA would need to follow up with the covered entity to obtain required information. CISA also would have to manually review and upload all submissions into an online case management system so that CIRCIA Reports received by mail could be consolidated, analyzed, stored, etc. in similar way as all other CIRCIA Reports. These additional activities are likely to result in significant additional implementation costs for CISA, increase the amount of time it takes for CISA analysts to receive necessary details about the cyber incident or ransom payment, and introduce an additional vector for human error during the transcription or conversion of the data. For these reasons, CISA is not proposing U.S. Mail or similar delivery services as an acceptable mechanism for submitting CIRCIA Reports.

e. Automated/Machine-to-Machine Reporting

Automated (i.e., machine-to-machine or application programming interface (API)-based) reporting presents many potential benefits. If designed properly, automated reporting could provide nearly real-time, secure reporting of high volumes of incidents, in a manner and format tailored for analysis and incorporation into CISA's online case management system. Automated reporting could assure the use of consistent terminology and reduce the potential introduction of human error by eliminating the need for humans to enter or transcribe the data.

Automated cyber incident and ransom payment reporting does, however, potentially present some significant challenges. These challenges include potentially significant upfront costs to design a system and develop the associated standard; the costs for users to implement the standard, including any costs necessary to integrate it with their existing systems to feed the data exchange; and potentially significant amounts of overreporting if the automated reporting thresholds are not set properly by the covered entity.

Given the potentially significant benefits that could result from automated reporting, and the success that some other Federal regulators have had with automated reporting, this is an approach that CISA would be interested in exploring further once the CIRCIA final rule is issued and all necessary systems to support CIRCIA Reports are developed and deployed. CISA can envision this becoming an additional manner of submission approved by the Director in the future. At this time, however, CISA is not proposing automated reporting as a means for submission of CIRCIA Reports for a few reasons. First, CISA believes it is prudent to focus the finite technical and financial resources CISA has available for CIRCIA implementation on the development of the user-friendly, web-based form which CISA is required to offer as a means for submission of CIRCIA Reports. Second, until the rule is finalized and reporting begins, CISA will not know definitively the volume of reports CISA will be receiving or the number of covered entities that might be interested in using machine-to-machine reporting to comply with CIRCIA. Prior to expending potentially significant resources on the development of machine-to-machine reporting capabilities, CISA would want to better understand the utility and demand for such a reporting mechanism and the potential return on investment of offering it as a means of reporting.

f. In-person Reporting

One other method CISA considered is in-person reporting, either verbally or through provision of a written report, to a CISA staff member, such as a CISA Cybersecurity Advisor, Protective Security Advisor, Chemical Security Inspector, or a member of CISA's Cybersecurity Threat Hunting team. All of these individuals are trained security professionals who work daily with owners and operators of entities within the critical infrastructure sectors.

In-person reporting would have the benefit of facilitating direct engagement between an entity experiencing a cyber incident and CISA staff who might not only be able to receive a report, but also provide or direct the covered entity to assistance in responding to or mitigating the impacts of the incident. Direct engagement between CISA and the entity experiencing the incident may also help ensure that the most pertinent information is provided to CISA, and CISA may be able to get clarifications or answers to follow-up questions in real time, particularly for verbal reporting. In-person provision of a written report would also revert some of the downsides of mail-in reporting, such as by ensuring timeliness and real-time confirmation of receipt by CISA.

The downsides of in-person reporting include the increased burden required to broadly train CISA staff on the protocols for receiving in-person reports, the need for the individual receiving the report to subsequently input the information received into CISA's online case management system, and the additional likelihood of human error that these engagements would add into the process (though perhaps moderately less so than with telephone reporting as the parties could review the transcribed report with the reporting individual in real time). There also are logistical challenges that likely would limit the utility of this option as it would require the reporting individual and the CISA representative to be in the same physical location. This approach would almost certainly require either a representative of a covered entity to travel to meet the CISA representative or vice versa, both delaying the time before reporting could be completed

and increasing the cost of reporting (due to both the direct costs of travel and the indirect wage-related costs of the individual required to travel). Additionally, at least for verbal reporting, the CISA staff most likely to receive in-person reports are highly trained security professionals whose jobs are to engage with owners and operators of critical infrastructure. As these individuals already have significant, important day-to-day responsibilities, receiving and uploading CIRCIA Reports may not be the most cost-efficient use of their taxpayer-funded time in support of CISA's mission. In light of these drawbacks, CISA is not proposing to use direct, in-person reporting as a mechanism for receiving CIRCIA Reports.

ii. Form for Reporting

Section 681b(a)(6) of title 6, United States Code, states that Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports "shall be made in the manner and form . . . prescribed in the final rule." As discussed in the previous section, CISA is proposing to use the "concise, user-friendly web-based form" CISA is required by 6 U.S.C. 681b(c)(8) to offer as a means for submission as the primary authorized means for submitting CIRCIA Reports. CISA proposes naming this web-based form the "CIRCIA Incident Reporting Form."

For the reasons discussed below, CISA is proposing to use the same user interface for the CIRCIA Incident Reporting Form regardless of which of the four types of discrete mandatory reports identified in CIRCIA (i.e., Covered Cyber Incident Report; Ransom Payment Report; Joint Covered Cyber Incident and Ransom Payment Report; and Supplemental Report) that must be submitted by a covered entity. Additionally, CISA is proposing to use the same user interface regardless of whether a covered entity itself is submitting a CIRCIA Report or if a third party is submitting a report on behalf of a covered entity. To facilitate this approach, CISA is proposing to use a dynamic, user-friendly, web-based form with conditional logic filters, with questions that adjust based

on the answers to gateway or filtering questions used throughout the form. For instance, an early question might ask the submitter to indicate what type of report is being submitted—e.g., a Covered Cyber Incident Report, a Ransom Payment Report, a Joint Covered Cyber Incident and Ransom Payment Report, a Supplemental Report—and the questions that follow will be tailored based on the response provided by the submitter.

CISA believes that numerous benefits exist in using the same user interface for all CIRCIA Reports (and potentially for voluntarily provided reports as well). First, this approach would allow all entities to go to a single location to comply with their CIRCIA reporting obligations regardless of what type of CIRCIA Report they need to submit. Second, it would prevent the covered entity from having to choose from multiple different forms to determine which is the correct set of questions for their particular reporting situation. There are a variety of circumstances under which a covered entity may be submitting a CIRCIA Report, such as a covered cyber incident that does not involve a ransom payment, a covered cyber incident for which a ransom payment has been made, a ransom payment being reported via a Supplemental Report after a covered cyber incident has been submitted, or a ransom payment made in response to a cyber incident that does not meet the criteria of a covered cyber incident. Instead of creating unique forms for each possible reporting scenario and requiring the covered entity to correctly identify which one applies, having a single user interface that can be used to address any potential reporting circumstance eliminates both the need for the covered entity to expend resources identifying the correct form and the possibility of the covered entity selecting the incorrect form.

Finally, a single user interface also reduces the burden in situations where the covered entity's reporting requirements change during the preparation of the report. For instance, a covered entity may begin to report a covered cyber incident and, before submitting it to CISA, the entity makes a ransom payment as part of its response to the

incident. Having a dynamic user interface may make it possible to allow the covered entity to modify its responses to certain questions and/or add the additional information related to the ransom payment rather than recreate all of its previous work in a separate form designed specifically for submitting a Joint Covered Cyber Incident and Ransom Payment Report.

The dynamic nature of the concise, user-friendly, web-based form being proposed by CISA has additional benefits beyond the facilitation of a single form model. A dynamic user interface supports the tailoring of questions even within a single type of report (e.g., a Covered Cyber Incident Report), allowing CISA to present only those secondary or tertiary questions applicable to the covered entity's unique circumstances, thus minimizing the overall number of questions asked of each submitter.[354] Similarly, in addition to appropriately modifying whether a question is asked at all, a dynamic approach also allows CISA to vary whether responding to specific questions is required or optional based on the report type and other answers provided by the submitter.

In the user interface, CISA intends to use a mixture of input options, such as radio buttons, drop-down menus, and text boxes. Tailoring the response format and options for individual questions will allow CISA to advance various goals simultaneously, to include reducing the burden of completing the report, supporting consistency in terminology to facilitate analysis of data, facilitating the logic-flow based tailoring of questions, and offering opportunities for covered entities to provide additional pertinent details via narratives where useful.

---

[354] For instance, for a hypothetical first-level question on what type of entity a covered entity is (e.g., individual, corporation, State or local government), a covered entity that indicates it is a State or local government might receive a secondary question asking it to identify what State it represents and a tertiary question asking it to identify the State department or agency. If the covered entity instead indicated it was a corporation, it would not be asked those specific secondary or tertiary questions, but rather might be asked different questions that would not be visible to an entity that indicated it was a State or local government, such as the State in which the corporation was incorporated and the corporation's Data Universal Numbering System (DUNS) number.

As discussed in the previous section, CISA intends to maintain the ability to receive telephonic reports as a back-up option and, in the future, may offer alternative mechanisms for a covered entity to submit a report beyond the web-based user interface, such as automated (i.e., machine-to-machine) reporting. If CISA offers, and a covered entity elects to use, a mechanism other than the web-based user interface to submit a report, CISA will establish procedures to ensure all mandatory questions are answered and the benefits of a single, dynamic form are preserved to the maximum extent practicable. For example, if CISA were to allow telephonic reporting in the future, CISA could have an operator complete the web-based form for the caller by verbally talking the caller through the form, asking them every pertinent question, typing the responses into the form, and then transmitting the covered entity a copy of the completed report for its records. Similarly, if a fillable PDF or paper-based format is offered, CISA could design that paper-based form in a manner similar to forms used by the Internal Revenue Service for filing of taxes, where the provision of specific answers to questions on the universal section of the form direct the preparer of the form to annexes or addendums that they should complete and include with their submission given their case-specific circumstances.[355]

Consistent with what has been discussed above, 6 U.S.C. 681b(a)(5)(A) requires that CISA offer a means to comply with reporting requirements for both a covered cyber incident and a ransom payment using a single report if a covered entity makes a ransom payment prior to the 72-hour requirement for submitting a Covered Cyber Incident Report.[356] CISA's proposed approach of using a dynamic reporting user interface for all

---

[355] For example, an individual only needs to complete Schedule B to Form 1040 if they received certain interest or ordinary dividends during a given tax year (see https://www.irs.gov/forms-pubs/about-schedule-b-form-1040 (last visited Nov. 28, 2023)) or Schedule C if they need to report income or loss from a business operated or profession practiced as a sole proprietor (see https://www.irs.gov/forms-pubs/about-schedule-c-form-1040 (last visited Nov. 28, 2023)).

[356] Specifically, 6 U.S.C. 681b(a)(5)(A) states "If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting

CIRCIA Reports would enable a covered entity to submit information on both a covered cyber incident and ransom payment at the same time using the same form, thus satisfying this statutory requirement. As discussed in Section IV.A.iii.4 in this document, CISA is proposing to call this report a Joint Covered Cyber Incident and Ransom Payment Report. To complete this type of report, a covered entity should follow the processes described herein that apply to all CIRCIA Reports and include all content required in both a Covered Cyber Incident Report and Ransom Payment Report, as set out in the following section and §§ 226.7 through 226.10 of the proposed regulation.

iii. Content of Reports

Sections 681b(c)(4) and (5) of title 6, United States Code, require CISA to include in the final rule a "clear description of the specific required contents" of a Covered Cyber Incident Report and Ransom Payment Report, respectively. Sections 226.7 through 226.11 of the proposed regulation contain a description of the content required in those reports, as well as the other two types of CIRCIA Reports.

In determining what content covered entities should be required to include in either a Covered Cyber Incident Report or Ransom Payment Report, CISA considered a variety of sources. First and foremost, CISA considered 6 U.S.C. 681b(c)(4) and (5), as those sections contain extensive lists of the specific types and categories of information that submitters must include in Covered Cyber Incident Reports and Ransom Payment Reports, respectively.

Second, CISA examined what data is required for CISA to perform the activities Congress assigned to CISA within CIRCIA and evaluated whether that data is captured within the content categories enumerated in 6 U.S.C. 681b(c)(4) and (5). Based on that evaluation, CISA determined that certain data CISA will need to perform its statutory

---

requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b)."

mandates will not necessarily be captured by any of the categories of content specified by Congress in 6 U.S.C. 681b(c)(4) and (5). Accordingly, CISA is proposing to make that content required in one or more types of CIRCIA Report. For example, 6 U.S.C. 681a(a)(3)(B) of CIRCIA requires CISA to "provide appropriate entities . . . with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including . . . related contextual information, cyber threat indicators, and defensive measures." To comply with this requirement, CISA needs to collect information on cyber threat indicators from victims of cyber incidents. Accordingly, while some of the categories enumerated in 6 U.S.C. 681b(c)(4) and (5) would likely elicit the submission of some information that would qualify as cyber threat indicators (as defined in 6 U.S.C. 650(5)), CISA is proposing including additional mandatory content for CIRCIA Reports for CISA to collect a broader range of cyber threat indicators.

Third, CISA engaged with stakeholders from across the Federal government to determine what data related to cyber incidents might be useful to them to accomplish their respective missions or, for those with their own cyber incident reporting programs, what data they have found to be the most useful and other information that might be helpful to have in the future. Among the groups CISA consulted were:

- the SRMAs responsible for coordinating critical infrastructure security efforts across the 16 critical infrastructure sectors;
- members of the law enforcement and intelligence communities, such as the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the Department of the Treasury's Financial Crimes Enforcement Network, and the NSA; and
- Federal departments and agencies that oversee cyber incident reporting regulations or directives, such as DOE, NRC, SEC, FCC, TSA, and the Department of the Treasury's OCC.

In this vein, CISA also considered what incident-related information CISA has found to be the most useful in executing non-CIRCIA responsibilities, including CISA's asset response authorities under 6 U.S.C. 652(c)(1) and 659(f)(1) and as further described in Presidential Policy Directive – 41, *United States Cyber Incident Coordination*.

CISA also solicited the perspective of the public and members of the private sector on this topic through the issuance of an RFI and the hosting of more than two dozen listening sessions. CISA received numerous comments on contents of reports, which have been considered by CISA in developing the proposed content of reports. More information on the comments received by CISA in response to the RFI and during the CIRCIA listening sessions can be found in Section III.F in this document.

Finally, CISA reviewed the Model Reporting Form developed by DHS through the CIRC effort. As part of the CIRC's mandate to promote harmonization of Federal cyber incident reporting regulations and minimize the burden on entities that may need to comply with more than one cyber incident reporting requirement, DHS, informed by close collaboration with the CIRC, developed a Model Reporting Form. CISA fully supports harmonizing cyber incident reporting requirements where practicable and has sought to align the CIRCIA reporting form required content with the content recommendations in the Model Reporting Form where practical and consistent with the CIRCIA statutory requirements related to both the content of CIRCIA Reports and CISA's obligations with respect to information received through CIRCIA Reports.

Based on the above, CISA is proposing certain content be submitted by a covered entity regardless of the type of CIRCIA Report being submitted, while other content will be required only in certain types of CIRCIA Reports. The following subsections discuss the categories of content that CISA is proposing be required for inclusion in (a) all CIRCIA Reports, (b) Covered Cyber Incident Reports (and subsequent Supplemental

Reports as necessary) only, (c) Ransom Payment Reports only, and (d) Supplemental Reports only.

1. Proposed Content to be Included in All CIRCIA Reports

This subsection describes the content, such as contact information for the covered entity, that CISA is proposing must be included regardless of the type of CIRCIA Report a covered entity is submitting. Other categories of content that CISA is proposing for inclusion in a specific type of report, such as the date and amount of the ransom payment, follow, organized by report type.

The majority of the content proposed for inclusion is explicitly required by CIRCIA. Where this is the case, the discussion below will include a reference to the specific statutory provision in CIRCIA requiring the inclusion of the proposed content. Where CISA is proposing to seek content beyond what is explicitly set out in 6 U.S.C. 681b(c)(4) and (5), the rationale supporting that proposal is included.

a. Report Type

At or near the beginning of the reporting user interface will be questions related to what type of report an entity wants to submit. This will help identify if a report is a Covered Cyber Incident Report, a Ransom Payment Report, a Joint Covered Cyber Incident and Ransom Payment Report, or a Supplemental Report. The answer submitted in response to these questions will help determine the spectrum of additional content the reporting entity will be asked to provide and may be used to streamline reporting in other ways, such as by supporting the pre-population of previously submitted data when submitting a Supplemental Report, to the extent pre-population is available for the covered entity's chosen manner of submission. This section of the form also may include some optional questions such as whether this information is being additionally submitted to meet any other reporting requirements. If a covered entity is reporting an incident to CISA per another regulatory requirement and intends for this report to also meet its

reporting obligations under CIRCIA, the covered entity would need to indicate both requirements on the form. Otherwise, a separate CIRCIA Report would need to be filed.

b. Identity of the Covered Entity

All CIRCIA Reports are statutorily required to include information sufficient to clearly identify the c making the report or on whose behalf the report is being made. See 6 U.S.C. 681b(c)(4)(E) and (5)(D). This must include, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers. See 6 U.S.C. 681b(c)(4)(E) and (5)(D). Other types of information that CISA intends on requesting in this section of the form include the entity type (e.g., Federal, State, local, Territorial, Tribal, ISAC, private sector); physical address; organization's website; any internal incident tracking number used by the entity for the reported event (if one exists); any applicable business numerical identifiers, such as a NAICS code, General Services Administration-Issued Unique Entity Identifier (GSA-UEI), Dun & Bradstreet Data Universal Numbering System (D-U-N-S) Number, Tax ID Number, EPA Facility ID number; Chemical Security Assessment Tool (CSAT) ID Number, or MTSA Facility ID Number; the name of the covered entity's parent corporation or organization, if applicable; and the critical infrastructure sector or sectors of which the covered entity considers itself a part. This additional information will help ensure that CISA has the correct identity of the covered entity (including understanding the corporate familial relationship between the covered entity or covered entities that experienced the substantial cyber incident and any subsidiary, parent, or sister corporation or organization that may be reporting on behalf of affected subsidiaries, parents, or sisters), facilitate information sharing with appropriate partners, and support trend and threat analysis by specific geographic regions, entity types, critical infrastructure sectors, and other characteristics.

c. Contact Information

All CIRCIA Reports are statutorily required to include contact information, such as telephone number or email address, that CISA may use to contact the covered entity, an authorized agent thereof, or, where applicable, an authorized third party acting with the express permission and at the direction of the covered entity to assist with compliance with CIRCIA reporting requirements. 6 U.S.C. 681b(c)(4)(F) and (5)(E). To satisfy this statutory requirement, CISA is proposing requiring a covered entity to provide the name, phone number, email, and title of the reporting party and, if different, the point of contact for the covered entity. CISA is also proposing requiring a covered entity to provide the name, phone number, email address, and title of the covered entity's registered agent, if that individual is different than the identified point of contact. CISA also is proposing that in cases where a third party is submitting a report on behalf of a covered entity, the aforementioned contact information must be provided for both the third-party submitter and the covered entity point of contact.

CISA additionally is proposing to include an optional field through which contact information for a 24/7 point of contact could be provided to better enable incident response support and emergency follow-up engagement. CISA may also include optional fields for additional contact information elements such as a classified phone number or classified email account where the 24/7 point of contact or another identified individual(s) can be reached, if applicable.

d. Third Party Authorization to Submit

Pursuant to 6 U.S.C. 681b(d)(1), a covered entity may use a third party to submit a CIRCIA Report on behalf of the covered entity. As discussed in greater detail in Section IV.E.v.3.a in this document, CISA is proposing requiring a third party that submits a report on behalf of a covered entity to include in the submission an attestation that it has been expressly authorized by the covered entity to submit the report. CISA is proposing to require this indication of authorization in any CIRCIA Report submitted by

a third party on behalf of a covered entity, regardless of the type of report. This requirement is set forth in § 226.7(d) of the proposed regulation. Additional details on third-party submissions and the proposed requirement for third-party submitters to confirm their authority to submit a CIRCIA Report on a covered entity's behalf can be found in Section IV.E.v.3 in this document.

2. Covered Cyber Incident Report Specific Content

CISA is proposing requiring submission of information in the following categories of content in a Covered Cyber Incident Report. As noted in the individual content categories, CISA is proposing that some of the proposed data elements within the individual content categories are required while other proposed data elements are optional. CISA intends to ask for all the required information in an initial Covered Cyber Incident Report; however, CISA understands that a covered entity may not know all of the required information within the initial 72-hour reporting timeframe. Accordingly, answers of "unknown at this time" or something similar will be considered acceptable for certain questions in initial reporting. A covered entity must, however, comply with its Supplemental Reporting requirements and provide previously unknown information promptly to CISA once discovered if the information meets the "substantial new or different information" threshold. That includes any information required to be submitted in an initial Covered Cyber Incident or Joint Covered Cyber Incident and Ransom Payment Report that a covered entity subsequently learns after initially responding that the information was unknown at the time of reporting. See Section IV.E.iv.3.b in this document for a more fulsome discussion on what CISA is proposing constitutes "substantial new or different information." CISA is proposing that a covered entity ultimately must provide all applicable required content in either the initial Covered Cyber Incident Report or a Supplemental Report to be considered fully compliant with its reporting obligations under CIRCIA.

a. Description of the Covered Incident

The first category of content required by CIRCIA is focused on ensuring CISA receives information on the systems affected by the incident and the impacts of the incident. Specifically, 6 U.S.C. 681b(c)(4)(A) requires covered entities to include in a Covered Cyber Incident Report a "description of the covered cyber incident" containing, among other things, an identification and description of the affected information systems, networks, or devices; a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations; the estimated date range of the incident; and the impact to the operations of the covered entity. To collect this information, CISA is proposing including a combination of one or more text boxes where entities can provide a narrative description of the incident or specific aspects of the incident along with a series of questions containing radio buttons, drop-down menus, or limited data fields (e.g., dates) to ensure the provision of certain information.

For the first statutorily enumerated element under this category—identification and a description of the function of the affected information systems, networks, or devices—CISA is interested in the name and a description of the impacted systems, networks, and/or devices, to include technical details and physical locations of the impacted systems, networks, and/or devices. CISA also would like to know if any of the impacted systems, networks, and/or devices contain or process information created by or for any element of the Intelligence Community or contain information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y).

For the second statutorily enumerated element under this category—description of the unauthorized access with substantial loss of confidentiality, integrity, or availability

of the affected information system or network or disruption of business or industrial operations—CISA is interested in whether the incident involved any unauthorized access (whether or not the access involves an attributed or unattributed cyber intrusion), whether there were any informational impacts, or whether any information was compromised. If the answer to any of those questions is "yes," CISA proposes requiring the covered entity to answer a small number of follow-up questions to elicit additional details. CISA also intends to request information regarding what network location(s) the activity was observed in. While the statutorily enumerated element incorporates the "substantial loss" standard from the first prong of the definition of substantial cyber incident, CISA is proposing to require covered entities to describe any unauthorized access once an incident meets the reportable threshold so that CISA and other Federal agencies can have a broader understanding of potential impacts to the CIA of information systems, networks, or the information therein. CISA believes the "disruption of business or industrial operations" portion of this statutorily enumerated element is sufficiently addressed by the fourth statutorily enumerated element, discussed below.

For the third statutorily enumerated element under this category—incident date range—CISA is proposing to seek information on the date the covered cyber incident was detected, the date the covered cyber incident began (if known), the date the covered cyber incident was fully mitigated and resolved (if it has been), and the timeline of compromised system communications with other systems. For incidents involving unauthorized access, CISA also proposes asking about the suspected duration of the unauthorized access prior to detection and reporting. While CISA is proposing to ask for more details than just the incident date range (i.e., the beginning and end of the incident), understanding the key timeline of events that comprised the incident is key to enhancing the Federal government's understanding of the incident as a whole.

In describing this category of information, the proposed regulatory text refers to the incident as the "covered cyber incident" to refer to the incident that is subject to the CIRCIA reporting requirement. CISA does not interpret the use of that term to import any threshold definitional triggers. For example, in requiring that the Covered Cyber Incident Report include the date that the covered cyber incident began, CISA is not asking for the date on which the covered entity began experiencing impact levels that met the definition of a substantial cyber incident, and therefore a covered cyber incident. Rather, once a covered entity has determined it has experienced a covered cyber incident, it should report all relevant dates related to the underlying cyber incident. As such, the date that the covered cyber incident began would be the earliest date of identified unauthorized activity associated with the cyber incident that would ultimately become the covered cyber incident.

For the final statutorily enumerated element under this category—impacts to the operations of the covered entity—CISA proposes asking various questions to understand both the level of impact and specific impacts, such as whether any known or suspected physical or informational impacts occurred. CISA is also proposing to include questions related to the nature of the impact, i.e., was the system, network, device, or data accessed, manipulated, exfiltrated, destroyed, or rendered unavailable. To satisfy some of the requirements imposed upon CISA by CIRCIA, CISA also needs information on impacts of the incident beyond simply the operations of the covered entity. For instance, among other things, 6 U.S.C. 681a(a) requires CISA to analyze Covered Cyber Incident Reports to assess potential impacts of cyber incidents on public health and safety. Similarly, 6 U.S.C. 681a(c) requires CISA to periodically brief certain members of Congress on the national cyber threat landscape. Likewise, 6 U.S.C. 681a(a)(6) requires CISA to review any covered cyber incidents or group of incidents that are likely to result in demonstrable harm to the economy of the United States and identify and disseminate ways to prevent

similar incidents in the future. In support of these and other requirements, CISA also envisions asking questions that will help CISA assess the economic impacts of the incident and the potential impacts of the incident on public health and safety, national security, economic security, and any of the NCFs.

CIRCIA also requires a covered entity to include in its Covered Cyber Incident Report the "category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person." 6 U.S.C. 681b(c)(4)(D). CISA proposes including questions related to this topic in the Covered Cyber Incident Report form.

b. Vulnerabilities, Security Defenses, and TTPs

The second statutorily required block of content is focused on how the incident was carried out. Specifically, 6 U.S.C. 681b(c)(4)(B) requires covered entities to include in a Covered Cyber Incident Report "[w]here applicable, a description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident." This information will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents and preventing similar vulnerability classes in the future.

CISA is proposing to codify the need to submit information to address this statutory requirement in five consecutive regulatory subsections. First, proposed § 226.8(c) would require the submission of information on the vulnerabilities exploited, including but not limited to the specific products or technologies and versions in which the vulnerabilities were found. Next, proposed § 226.8(d) would require the submission of information on the covered entity's security defenses, including but not limited to any controls or measures that resulted in detection or mitigation of the incident. As part of

this, CISA is likely to ask what, if any, security controls or control families (e.g., NIST Special Pub 800-171 controls[357]; NIST Cybersecurity Framework measures[358]; CISA Cybersecurity Performance Goal activities[359]) the covered entity had in place on the compromised system, and, to the extent known, which controls or control families failed, were insufficient, or not implemented that may have been a factor in this incident. CISA also is likely to include questions aimed at helping CISA understand how the covered entity identified the incident; what, if any, detection methods were used to discover the incident; and if the covered entity has identified the initially affected device(s).

Finally, proposed § 226.8(e), (f) and (g) would require information on the type of incident (e.g., denial-of-service; ransomware attack; multi-factor authentication interception); the TTPs used to cause the incident, to include any TTPs that were used to gain initial access to the covered entity's system; indicators of compromise observed in connection with the covered cyber incident; and a description and copy or sample of any malicious software the covered entity believes is connected with the covered cyber incident. Questions CISA may ask to obtain this information potentially include what, if any, attack vectors did the covered entity identify; to the covered entity's knowledge, were any advanced persistent threat actors involved; were any malicious software, malicious scripts, or other indicators of compromise found, and, if so, what specific variants or strains were used. In addition to a description of any malware samples or indicators of compromise observed or captured by the covered entity, CISA is proposing to require covered entities provide indicators of compromise identified as well as copies of any malware samples related to the covered cyber incident that the covered entity has

---

[357] See NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171 Rev. 2, (Feb. 2020), available at https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final.

[358] See NIST, *Cybersecurity Framework 2.0*, available at https://www.nist.gov/cyberframework.

[359] See CISA, *Cross-Sector Performance Goals*, available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

in its possession. While 6 U.S.C. 681b(c)(4)(B) uses the term "description," obtaining actual indicators of compromise and copies of malware samples, rather than a mere description, is important to enable CISA to perform the activities assigned to CISA under CIRCIA (including identifying, developing, and disseminating actionable cyber threat indicators and defensive measures), and is also consistent with key requests in other incident reporting programs.[360]

In cases where the covered cyber incident involves a ransomware attack but the covered entity did not make a ransom payment and is thus not obligated to submit a Ransom Payment Report, pursuant to proposed § 226.8(e), CISA intends to ask specific questions related to ransomware attack-specific TTPs, such as information on the ransom payment demand and instructions, that a covered entity would otherwise have been required to provide in a Ransom Payment Report were one required. This information will help CISA and its partners on the Joint Ransomware Task Force established pursuant to CIRCIA more fully understand and combat existing threats related to ransomware attacks.

To assist in the development of responses to these questions and the use of common terminology, CISA anticipates providing drop-down menus or other selection options tied to the MITRE ATT&CK® framework[361] or another broadly recognized cyber incident reporting framework. CISA may also ask whether the entity has any applicable logs (e.g., network logs; system logs; memory captures) available.

CISA recognizes that some of the information requested in this section of the form may be unavailable at the time a covered entity is submitting the initial Covered Cyber Incident Report. Nevertheless, to assist CISA in conducting analysis and providing

---

[360] See, e.g., 48 C.F.R. 252.204-7012(d) (requirement in DFARS incident reporting requirement for contractors to submit copies of malicious software to DOD when they have discovered and isolated malicious software in connection with a reported cyber incident).

[361] MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, available at https://attack.mitre.org/.

early warnings in as timely a manner as possible, CISA does intend to ask for this information in Covered Cyber Incident Reports and expects covered entities to provide that information when they possess it with some degree of confidence; however, good faith answers of "unknown at this time" or something similar generally will be acceptable responses to these questions in an initial Covered Cyber Incident Report. If this information is not submitted in the initial report, to the extent the information is applicable to the incident and knowable, a covered entity will be required to include that information in a Supplemental Report before its reporting obligations are considered met under the regulation. A covered entity should keep in mind its obligation to report "substantial new and different information" to CISA "promptly" upon discovery and should not be waiting until all unknown information is gathered before submitting a Supplemental Report to CISA.

c. Information related to the Identity of the Perpetrator of the Incident

Section 681b(c)(4)(C) of title 6, United States Code, requires covered entities to include in a Covered Cyber Incident Report "[w]here applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident." CISA is proposing to include in this section questions seeking any attribution-related information the covered entity may possess. Additionally, CISA is proposing to include in this section questions regarding whether the covered entity believes they can attribute the cyber incident, what evidence supports their attribution assessment, and how confident they are in their attribution assessment.

d. Mitigation/Response

Although not included among the specifically required contents enumerated in 6 U.S.C. 681b(c)(4), CISA is proposing a small number of questions regarding the mitigation and response activities a covered entity is taking or has taken in response to a

covered cyber incident. Under 6 U.S.C. 681a(a)(3)(B) and (7), CISA is required to, among other things, leverage information gathered about cyber incidents to provide appropriate entities with defensive measures, and, with respect to Covered Cyber Incident Reports involving an ongoing cybersecurity threat or security vulnerability, immediately review those reports and disseminate defensive measures. Further, under 6 U.S.C. 681a(a)(6), CISA is required to conduct a review of details surrounding each covered cyber incident or group of such incidents that satisfy the definition of a significant cyber incident to identify and disseminate ways to prevent or mitigate similar incidents in the future. Understanding the mitigation and response activities taken by a covered entity will be key to CISA's ability to identify or develop defensive measures that can be leveraged by other entities, as well as to evaluate and identify ways to mitigate similar incidents in the future.

The questions CISA is proposing to ask to support this analysis include what mitigation measures the covered entity had in place, what responsive actions the covered entity has taken, what phase of incident response (e.g., detection, analysis, containment, eradication, recovery, and post-incident activity) the covered entity is currently in, and what is the covered entity's assessment of the efficacy of those mitigation and response activities.[362] As part of this, CISA is also proposing to ask about engagement with law enforcement agencies, if the covered entity reached out to another entity for mitigation or response assistance, and, if so, to whom.[363] CISA will also provide an opportunity for the covered entity to indicate that it would like to request assistance from CISA related to the incident. This information will facilitate CISA's coordination with its Federal partners,

---

[362] See NIST, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Rev. 2, at 21-45 (Aug. 2012), available at https://csrc.nist.gov/pubs/sp/800/61/r2/final (hereinafter "*NIST SP 800-61r2*").

[363] In response to this topic and the related topic in the required content for Ransom Payment Reports, covered entities do not need to include every vendor from whom they have sought a quote but did not ultimately use. However, covered entities should not necessarily limit their response to entities from whom they have actually received assistance, particularly as some requests for assistance may remain outstanding at the time the report is submitted.

including law enforcement, and non-Federal partners who may already be engaged in responding to the incident.

e. Additional Data or Information

CISA is proposing to require a covered entity to include in a Covered Cyber Incident Report any other data or information required by the web-based CIRCIA Incident Reporting Form or other authorized manner and form of reporting. CISA recognizes that cyber incidents are dynamic in nature and that, over time, CISA may identify additional data or information that would be useful or necessary to meet the purposes of the CIRCIA regulations. CISA may also identify ways to streamline reporting in response to particular circumstances, such as by allowing covered entities to check a box to indicate if their Covered Cyber Incident Report is related to a specific known campaign, supply chain compromise, or compromise of a third-party service provider. CISA is proposing to include § 226.8(j) to ensure that covered entities would be required to include any additional required data or information that CISA subsequently determines is necessary and consistent with CISA's authorities under CIRCIA. Additionally, CISA may include optional requests for data and information that apply to the type of covered cyber incident reported and that may help clarify the covered entity's responses to information required by § 226.8. CISA is proposing to include similar language in § 226.9(n) for Ransom Payment Reports and § 226.11(a)(4) for Supplemental Reports. CIRCIA exempts any action required to carry out 6 U.S.C. 681b, including the reporting requirements in 6 U.S.C. 681b(a)(1)-(3), from compliance with the PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described above and to solicit for optional information and data as part of CIRCIA Reports.

3. Ransom Payment Report Specific Content

Section 681b(c)(5) of title 6, United States Code, enumerates specific content that is to be included in a Ransom Payment Report. Two of the enumerated items, information identifying the covered entity that made the ransom payment (or on whose behalf the ransom payment was made) and contact information for the covered entity or an authorized agent thereof, were discussed previously and are part of the categories of information that must be included regardless of report type. The remaining items enumerated in 6 U.S.C. 681b(c)(5) are specific to Ransom Payment Reports and are discussed in the following subsections.

a. Description of the Ransomware Attack

Section 681b(c)(5)(A) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report a "description of the ransomware attack, including the estimated date range of the attack." For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(a) of the regulation and described in Section IV.E.iii.2.a in this document. While 6 U.S.C. 681b(c)(4)(A) includes much more specific detailed requirements as to what must be included in a description of a covered cyber incident than the parallel 6 U.S.C. 681b(c)(5)(A) includes for the required description of ransomware attacks, CISA is proposing to ask similar questions for this topic because, for the reasons described in Section IV.E.iii.2.a in this document, these questions would provide CISA with relevant information to understand the incident and its impact.

b. Vulnerabilities, Security Defenses, and TTPs

Section 681b(c)(5)(B) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report, "where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack." For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report or a previously submitted Supplemental Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(c) – (f) of the regulation and described in Section IV.E.iii.2.b in this document. While 6 U.S.C. 681b(c)(5)(B) does not include reference to the security defenses, as is included in the parallel 6 U.S.C. 681b(c)(4)(B), CISA is proposing to ask similar questions about security defenses in Ransom Payment Reports. This information will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents, and preventing similar vulnerability classes in the future, regardless of whether the ransomware attack that precipitated the ransom payment was a covered cyber incident or not. This information would be particularly useful to CISA in preventing others from falling victim to similar ransomware attacks that could rise to the level of being a covered cyber incident in the event those security defenses were the reason why a particular ransomware attack did not rise to the level of a substantial cyber incident.

c. Information Related to the Identification of the Perpetrator of the Attack

Section 681b(c)(5)(C) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report, "where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack." For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(h) of the regulation and described in Section IV.E.iii.2.c in this document.

d. Information on the Ransom Payment

Sections 681b(c)(5)(F)-(I) of title 6, United States Code, require a covered entity to submit a variety of information related to any ransom payment it makes or that gets made on its behalf. This information includes the date of the ransom payment (6 U.S.C. 681b(c)(5)(F)); the ransom payment demand, including the type of virtual currency or other commodity requested (6 U.S.C. 681b(c)(5)(G)); the ransom payment instructions, including information regarding where to send the payment (6 U.S.C. 681b(c)(5)(H)); and the amount of the ransom payment (6 U.S.C. 681b(c)(5)(I)). CISA is proposing including questions in the Ransom Payment Report sufficient to elicit submission of these statutorily required data elements, including details to help contextualize these elements (such as the type of assets used in the ransom payment, which is necessary to understand the value of the amount of the ransom payment), as well as information useful to identify the completed transaction, such as any transaction identifier or hash.

To ensure completeness in the response and a full understanding of the ransom demand, CISA is proposing to require the covered entity to provide either the verbatim

text of the demand or, where available, a screenshot or copy of the actual ransom demand. Additionally, if multiple demands were made during a single incident, CISA expects the covered entity to provide the required information on each such demand. Similarly, if multiple ransom payments were made in response to a single incident, a covered entity is required to report each such ransom payment.

e. Results of Ransom Payment

CISA is proposing to require a covered entity to include in a Ransom Payment Report information regarding what occurred as the result of the covered entity making the ransom payment. Examples of information that CISA would expect a covered entity to provide under this heading would be whether any data that had been exfiltrated was returned or, in cases where the perpetrator encrypted any of the covered entity's systems or information, whether a decryption capability was provided. If a decryption capability was provided, CISA would seek specific information on that capability, to include whether or not it was effective.

f. Additional Data or Information

CISA is proposing to require a covered entity to include in a Ransom Payment Report three additional items, all of which CISA is proposing to require in a Covered Cyber Incident Report as well. First, CISA is proposing to ask whether the covered entity requested assistance from another entity in responding to the ransomware attack or making the ransom payment and, if so, the identity of such entity or entities. This information will help CISA understand the capabilities covered entities typically do and do not possess to respond to a ransomware attack, where assistance may be beneficial, and the broader ecosystem of activities related to ransomware attacks. This will also help CISA have a better understanding of the universe of entities who may be subject to the responsibilities to advise a covered entity pursuant to § 226.12(d) (discussed further in Section IV.E.v.3.e in this document).

Second, CISA is proposing to require a covered entity to provide information on any engagement the covered entity has had with any law enforcement agency related to the ransom payment or underlying ransomware attack. Such information would be extremely beneficial to effective operations of the Joint Ransomware Task Force established by CIRCIA and help the Federal government minimize the potential for uncoordinated law enforcement activities.

Finally, CISA is proposing to require a covered entity to include in a Ransom Payment Report any other data or information required by the web-based CIRCIA Incident Reporting Form or any other authorized manner and form of reporting. Cyber incidents involving ransom payments are dynamic in nature and, over time, CISA may identify additional data or information that would be useful or necessary to meet the purposes of CIRCIA. CISA is proposing to include § 226.9(n) to ensure that covered entities would be required to include any additional required data or information that CISA subsequently determines is necessary and consistent with CISA's authorities under CIRCIA. Additionally, CISA may include optional requests for data and information that may help clarify the covered entity's responses to information required by § 226.9. CISA is proposing to include similar language in § 226.8(j) for Covered Cyber Incident Reports and § 226.11(a)(4) for Supplemental Reports.

CIRCIA exempts any action required to carry out the reporting requirements in 6 U.S.C. 681b(a)(1)-(3) from compliance with PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described above and to solicit for optional information and data as part of CIRCIA reports.

4. Supplemental Report Specific Content

While CIRCIA includes some specific categories of content that a covered entity must include in a Covered Cyber Incident Report or Ransom Payment Report, CIRCIA does not contain any similar requirements regarding what content must be included in a Supplemental Report. Given that the purpose of a Supplemental Report is to provide CISA with additional or updated information regarding a previously reported covered cyber incident, the content required in a Supplemental Report generally will be a subset of the content required to be reported and optional content in a Covered Cyber Incident Report and/or Ransom Payment Report, tailored to the reason for the submission of the Supplemental Report and the information previously provided by the covered entity in the previously submitted CIRCIA Report.

A unique content request proposed to be contained in a Supplemental Report is information on the purpose for filing the Supplemental Report. CISA envisions providing a list of possible answers for this question, which may include (a) providing CISA with newly discovered information that makes a previously submitted Covered Cyber Incident Report or Supplemental Report more complete, (b) providing CISA with information that corrects or amends a previously submitted Covered Cyber Incident Report or Supplemental Report, (c) informing CISA that the covered entity has made a Ransom Payment related to a previously reported covered cyber incident, or (d) informing CISA that the covered entity considers a previously reported covered cyber incident concluded and fully mitigated and resolved. CISA is also proposing to require that a Supplemental Report include the case identification number provided by CISA for the covered cyber incident with which the Supplemental Report is associated. This will facilitate pre-population of the Supplemental Report form and help CISA ensure that the Supplemental Report is properly assigned and maintained.

For Supplemental Reports being submitted by a covered entity for the purposes of informing CISA that the covered entity considers a previously reported covered cyber

incident concluded and fully mitigated and resolved, CISA proposes including optional questions in the form that would allow a covered entity to provide information on the actual recovery date and time, and an estimate of the costs incurred to fully mitigate the incident, as well as any other financial losses (e.g., losses in productivity; losses in revenue) incurred due to the incident. This data would help inform assessments of the risks associated with and impacts of cyber incidents and will assist CISA in meeting some of the briefing and reporting requirements assigned to CISA under CIRCIA.

A small number of commenters requested a mechanism for a covered entity to "de-escalate" an incident (i.e., inform CISA when the covered entity discovers additional information that causes the entity to believe an incident for which it had previously submitted a Covered Cyber Incident Report does not actually meet the criteria for a covered cyber incident). CISA believes this scenario is simply one variation that a Supplemental Report may take and proposes to include questions tailored to this within the Supplemental Report portion of the user interface for occasions where a covered entity is using a Supplemental Report for this purpose. CIRCIA exempts any action required to carry out the reporting requirements in 6 U.S.C. 681b, including 6 U.S.C. 681b(a)(1)-(3), from compliance with PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described above and to solicit for optional information and data as part of CIRCIA Reports.

5. Content in the DHS-Developed Model Reporting Form Not Included in Proposed CIRCIA Reporting Forms

As noted earlier, as part of its efforts to promote harmonization of Federal cyber incident reporting regulations and minimize the burden on entities that may need to comply with more than one cyber incident reporting requirement, DHS, informed by

conversations with the CIRC, developed a Model Reporting Form. In support of harmonization of Federal cyber incident reporting requirements, CISA carefully considered the Model Reporting Form during the development of the proposed CIRCIA reporting form and strove to align the content required by the two forms where possible while still meeting the requirements, needs, and limitations imposed by CIRCIA. Consequently, the majority of the content that CISA is proposing be submitted via its reporting form is also requested in the Model Reporting Form and vice versa (i.e., the majority of the content requested by the Model Reporting Form is proposed for inclusion in the CIRCIA reporting forms).

CISA ultimately determined that a small number of items contained in the Model Reporting Form were not appropriate for inclusion in the CIRCIA reporting forms or were only appropriate for inclusion on an optional basis. First, the Model Reporting Form includes a section where a reporting entity is afforded the opportunity to indicate if it believes one or more FOIA exemptions should apply to the information being submitted. CIRCIA Reports are statutorily exempt from disclosure under FOIA and any similar State, Local, and Tribal freedom of information laws, open government laws, sunshine laws, or similar laws requiring disclosure of information or records. 6 U.S.C. 681e(b)(2). Accordingly, the CIRCIA reporting form does not contain a similar section on FOIA exemptions that may apply under other authorities; however, it will contain a statement acknowledging this protection from disclosure under FOIA or similar laws pursuant to CIRCIA.

Second, the Model Reporting Form includes a number of questions related to whom the reporting entity has notified about the incident. This includes questions regarding whether the reporting entity has notified any governmental entities (e.g., regulators or other departments or agencies, law enforcement, Congress) and, in the case of consumer data breaches or privacy breaches, if the reporting entity has notified

impacted individuals and provided them with guidance on how to take steps to protect themselves during an ongoing incident. CISA is proposing to include as required content in CIRCIA Reports information on a covered entity's notification or other form of engagement with law enforcement agencies. CISA, however, is not proposing to require that covered entities report whether they have notified other stakeholders, such as non-law enforcement government entities, Congress, or individuals potentially impacted by the incident. While some of these additional notifications may be of general interest to CISA and support more effective or efficient information sharing among partners, none are required for CISA to meet its obligations under CIRCIA. Accordingly, CISA is not proposing requiring that covered entities report any of this information in a CIRCIA Report. CISA may include optional questions on some of these topics so that covered entities who are interested in voluntarily providing this information to CISA may do so.

iv. Timing of Submission of CIRCIA Reports

1. Timing for Submission of Covered Cyber Incident Reports

Under 6 U.S.C. 681b(a)(1)(A), a covered entity that experiences a covered cyber incident must submit a Covered Cyber Incident Report to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." CISA has included proposed language in the regulation establishing this timeframe in § 226.5(a).

CISA acknowledges that the point at which a covered entity should have "reasonably believed" a covered cyber incident occurred is subjective and will depend on the specific factual circumstances related to the particular incident. Accordingly, CISA is not proposing a specific definition for the term "reasonably believes," nor is CISA attempting to prescribe a specific point in the incident life cycle at which a "reasonable belief" will always be realized. Rather, CISA is providing the following guidance to help

covered entities understand when a "reasonable belief" generally is expected to have occurred.

CISA does not expect a covered entity to have reached a "reasonable belief" that a covered cyber incident occurred immediately upon occurrence of the incident, although this certainly may be true in some cases (e.g., an entity receives a ransom demand simultaneously with discovery that it has been locked out of its system). Oftentimes, an entity may need to perform some preliminary analysis before coming to a "reasonable belief" that a covered cyber incident occurred. This preliminary analysis may be necessary, for instance, to quickly rule out certain potential benign causes of the incident or determine the extent of the incident's impact. CISA believes that in most cases, this preliminary analysis should be relatively short in duration (i.e., hours, not days) before a "reasonable belief" can be obtained, and generally would occur at the subject matter expert level and not the executive officer level. As time is of the essence, CISA expects a covered entity to engage in any such preliminary analysis as soon as reasonably practicable after becoming aware of an incident and is proposing including such a requirement in the regulatory text.

A number of stakeholders submitted comments in response to the RFI suggesting that a "reasonable belief" occurs when an entity has confirmed, determined, or otherwise definitively established that an incident was a covered cyber incident. CISA does not agree with those commenters, and instead interprets "reasonable belief" to be a much lower threshold than "confirmation." CISA additionally believes that if Congress had intended the timeframe for reporting to begin at confirmation of an incident, it would have used specific language making that clear. CISA believes few, if any, circumstances will occur where an extended investigation must be undertaken and concluded before an entity can form a "reasonable belief" that a covered cyber incident occurred.

2. Timing for Submission of Ransom Payment Reports

Under 6 U.S.C. 681b(a)(2)(A), a covered entity that makes a ransom payment must submit a Ransom Payment Report to CISA "not later than 24 hours after the ransom payment has been made." CISA has included proposed language in the regulation reflecting this timeframe in § 226.5(b).

Different regulations have taken different approaches to when a payment is considered to have been "made" by a party. Some regulations interpret a payment to have been made on the date the payment is disbursed (e.g., sent, transmitted, submitted).[364] Others interpret a payment to have been made on the date the payment is received by the payee or otherwise becomes available to the payee.[365] For some regulations, when the payment is made varies based on the method of payment.[366]

For purposes of this provision of the regulation, CISA proposes interpreting payment to have been made upon disbursement of the payment by the covered entity or a third party directly authorized to make a payment on the covered entity's behalf. CISA is proposing this approach for two main reasons. First, when disbursement of a payment was made is easier for a covered entity to determine than when a payment has cleared, settled, posted, or otherwise been made available to the payee. Selecting payment disbursement instead of payment settlement or clearance as the trigger for when the reporting timeline begins provides greater clarity and prevents a covered entity from having to try to determine when a payment has actually been received by or otherwise made available to the payee. Second, as discussed earlier in Section III.C.ii in this document, it is imperative that CISA receive reports of covered cyber incidents and

---

[364] *Federal Acquisition Regulations*, 48 CFR 52.232-25 ("The Government considers payment as being made on the day a check is dated or the date of an electronic funds transfer."); *IRS Tax Regulations*, 26 CFR 301.7502-1 ("[I]f the requirements of that section are met, a document or payment is deemed to be filed or paid on the date of the postmark stamped on the envelope or other appropriate wrapper (envelope) in which the document or payment was mailed.").

[365] *IRS Employment Tax Regulations*, 26 CFR 31.3406(a)-4 ("Amounts are considered paid when they are credited to the account of, or made available to, the payee. Amounts are not considered paid solely because they are posted (e.g., an informational notation on the payee's passbook) if they are not actually credited to the payee's account or made available to the payee.").

[366] *Prompt Payment Act Regulations*, 5 CFR 1315.4(h) ("Payment will be considered to be made on the settlement date for an electronic funds transfer payment or the date of the check for a check payment.").

ransom payments in a timely manner so CISA can more quickly identify adversary trends, TTPs, and vulnerabilities being exploited to be able to provide other entities early warnings and mitigation strategies to help them avoid becoming victims to similar attacks. By interpreting when a payment is made to be at the earlier point of payment disbursement, rather than the later point of payment receipt, posting, or settlement, CISA will be able to receive reports of ransom payments earlier and be better situated to achieve some of the ultimate goals that Congress authorized the regulation to achieve.

CISA recognizes that in certain situations, more than one third party may be involved in the disbursement of a ransom payment. For instance, a covered entity might send funds to an intermediate third party, who might then transmit the funds to a financial institution, who then transfers the payment to the account specified by the party demanding the ransom payment. In interpreting this regulatory provision, the reporting timeline shall be deemed to be initiated at the earliest instance of disbursement. Thus, in the example provided, disbursement has occurred and the timeline for reporting would be triggered when the covered entity sent funds to the intermediate third party. In a case where a covered entity authorizes an intermediate third party to transmit funds on its behalf to make a ransom payment but does not actually disburse funds itself at that time, the reporting timeline shall be deemed to be initiated when the intermediate third party disburses funds.

3. Timing for Submission of Supplemental Reports

Under 6 U.S.C. 681b(a)(3), a covered entity that has previously submitted a Covered Cyber Incident Report must "promptly" submit to CISA an update or supplement to that report if either: (a) "substantial new or different information becomes available"; or (b) "the covered entity makes a ransom payment after submitting a covered cyber incident report." A covered entity is subject to these supplemental reporting obligations unless and until the covered entity notifies CISA that the incident that is the

subject of the original Covered Cyber Incident Report "has concluded and has been fully mitigated and resolved." Section 226.5(d) of the proposed regulation contains these Supplemental Reporting requirements.

a. Meaning of "Promptly"

CISA is proposing to use the statutory language contained in 6 U.S.C. 681b(a)(3) verbatim in the regulation to identify the timeframe and associated trigger for providing Supplemental Reports to CISA. As opposed to the statutory language for Covered Cyber Incident Reports and Ransom Payment Reports that contain specific numerical timeframes, CIRCIA requires Supplemental Reports to be submitted "promptly" upon the occurrence of either of the two identified triggering events. CISA interprets "promptly" to generally mean what it means colloquially, i.e., without delay or as soon as possible.

CISA notes that one of the two potential triggering events for a Supplemental Report has a separate timeframe for reporting mandated in CIRCIA. Specifically, making a ransom payment following the submission of a Covered Cyber Incident Report triggers a requirement for the covered entity to submit a Supplemental Report. See 6 U.S.C. 681b(a)(3). Given that CIRCIA requires covered entities to submit Ransom Payment Reports within 24 hours of making the ransom payment, CISA believes it is appropriate to interpret "promptly" to mean no longer than 24 hours after disbursement of the payment. Any other interpretation would result in a logical inconsistency where a covered entity would be able to extend the timeframe for reporting a ransom payment by filing a separate Covered Cyber Incident Report prior to making the ransom payment.

b. Meaning of "Substantial New or Different Information"

CISA proposes interpreting "substantial new or different information" as meaning information that (1) is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident, or (2)

shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner. Together, these two provisions will help ensure that a covered entity has provided to CISA all required information related to a covered cyber incident in a timely fashion and that any material inaccuracies in a previously submitted Covered Cyber Incident Report or Supplemental Report are promptly corrected.

The first prong of the interpretation—information that is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident—is focused on filling informational gaps from prior reporting. For instance, if an entity stated in its Covered Cyber Incident Report that the vulnerability exploited in perpetrating the incident was "unknown at this time," discovery of the exploited vulnerability would be information that meets this prong and would need to be reported promptly in a Supplemental Report. This prong is focused solely on completion of required data fields for which a covered entity previously did not have responsive or complete information at the time of filing a Covered Cyber Incident Report. CISA considers newly discovered information for any previously unaddressed required data field to be substantial and to meet the meaning of "substantial new or different information." If a covered entity discovers new information related to a question it has previously responded to, that information should be evaluated under the second prong, and would only be considered "substantial new or different information" that must be reported if it meets a materiality threshold.

The second prong of the interpretation—information that shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner—is focused on amendments or additions to content previously provided by a covered entity about a covered cyber incident. To reduce the

burden of supplemental reporting on covered entities, CISA is proposing to limit supplemental reporting requirements under this prong to times when the amendment or addition would result in a material change in CISA's understanding of the covered cyber incident. Limiting this prong to material changes will help ensure that CISA gets material updates in a timely manner while avoiding making a covered entity submit a Supplemental Report every time it learns anything new about the incident.

Examples of the types of information that CISA believes typically should be considered material include updated or corrected information on the TTPs used to perpetrate the incident; the discovery or identification of additional indicators of compromise; additional or corrected information related to the identity of the individual or individuals who perpetrated the incident; or identification of significant new consequences. Changes to the covered entity's point of contact information should also be considered material and reported promptly. Additionally, while newly discovered information that is responsive to an "optional" question need not be reported, material corrections to previously submitted information must be reported even if the originally submitted information was submitted in response to an "optional" question.

Examples that generally would not be considered material include minor technical corrections or changes to the extent, but not the type, of the impact (unless the changes to the extent of the impact were orders of magnitude higher than what was previously reported). CISA encourages covered entities to provide that information to CISA, but covered entities are not required to do so. Similarly, CISA encourages covered entities to voluntarily provide additional information that is not required by CIRCIA Reports but "enhances the situational awareness of cyber threats" consistent with 6 U.S.C. 681c(b).

While covered entities are not expected to submit Supplemental Reports for Ransom Payment Reports (unless the Ransom Payment Report is associated with a Covered Cyber Incident Report), CISA expects a covered entity to correct material

inaccuracies. For example, if a covered entity submitted the incorrect phone number for its point of contact, the covered entity should correct its Ransom Payment report submission.

c. Meaning of "Concluded" and "Fully Mitigated and Resolved"

A covered entity's supplemental reporting requirements remain in effect until the covered entity notifies CISA "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved." 6 U.S.C. 681b(a)(3). Although the point at which an incident is concluded and fully mitigated and resolved may vary based on the specific facts of the incident, reaching the following milestones is a good indication that an incident has been concluded and fully mitigated and resolved: (1) the entity has completed an investigation of the incident, gathered all necessary information, and documented all relevant aspects of the incident; and (2) the entity has completed steps required to address the root cause of the incident (e.g., completed any necessary containment and eradication actions; identified and mitigated all exploited vulnerabilities; removed any unauthorized access). The completion of a lessons learned analysis (i.e., after action report) is a valuable part of incident response, but CISA does not believe that such analysis needs to be completed for an incident to be considered concluded and fully mitigated and resolved. Similarly, CISA does not believe that all damage caused by the incident must have been fully addressed and remediated for an incident to be considered concluded and fully mitigated and resolved.

For an incident to be concluded and fully mitigated and resolved, a covered entity should have a good-faith belief that further investigation would not uncover any substantial new or different information about the covered cyber incident. If, following the provision of a notification to CISA that the covered entity believes the covered cyber incident to be concluded and fully mitigated and resolved, the covered entity becomes aware of any substantial new or different information, the covered entity is responsible

for submitting a Supplemental Report. In such a situation, CISA will consider the prior notification that the incident is concluded and fully mitigated and resolved to be rendered void and the covered cyber incident ongoing and active. The covered entity remains responsible for submitting Supplemental Information until such time as the covered cyber incident is concluded and fully mitigated and resolved and no new or different information indicates that the covered cyber incident is ongoing.

v. Report Submission Procedures

1.Submission of CIRCIA Reports to CISA

As discussed above, CISA is proposing that covered entities or third parties submitting CIRCIA Reports on behalf of a covered entity are required to do so using the web-based user interface or other mechanism subsequently approved by the Director. To submit a report using the web-based user interface, the submitter will need to have completed all required fields, to include, in the case of a third-party submitter, an attestation that the third party has been expressly authorized by the covered entity to submit the report on the covered entity's behalf. In recognition that a covered entity may not have all the required information within the 72-hour time limit for submission of a Covered Cyber Incident Report, CISA may accept submission of a report where the response to some required answers is "unknown at this time," "pending the results of additional investigation," or some other similar option to submit the initial report.

CISA is proposing that, upon receipt of a report, CISA issue the covered entity (and, in the cases of a third-party submitter, the third party) a confirmation of receipt along with a unique case management number. The confirmation of receipt is simply meant to inform the covered entity that the report has been properly submitted to and received by CISA; the confirmation is not, however, an indication that a covered entity has necessarily met all of its reporting requirements. The case identification number is meant to facilitate tracking and performance of future actions related to the specific

incident or ransom payment, to include supporting pre-population of data fields during the preparation of Supplemental Reports.

CISA intends to provide covered entities the opportunity to register with CISA under this proposed rule. Registration would allow a covered entity to pre-populate a number of the required data fields, such as entity identifying information, on the proposed web-based CIRCIA Incident Reporting Form. Registering with CISA would allow a covered entity to submit certain information to CISA for use in future CIRCIA reporting. Any covered entity that had previously submitted a CIRCIA Report would also have the information they submitted stored for future use. CISA believes that allowing this optional registration, which is completely voluntary, would reduce the time burden associated with submitting a CIRCIA Report when required due to the advanced submission and pre-population of certain information that is required in a CIRCIA Report.

2. Process for Notifying CISA that an Incident Has Concluded and Been Fully Mitigated and Resolved

covered entities have the option of notifying CISA that a previously reported covered cyber incident has concluded and has been fully mitigated and resolved. See 6 U.S.C. 681b(a)(3). Although notifying CISA that a previously reported covered cyber incident has concluded and been fully mitigated and resolved is not required, doing so terminates the covered entity's responsibility to provide Supplemental Reports.[367]

CISA is proposing that the process for notifying CISA that a previously reported covered cyber incident has concluded and been fully mitigated and resolved is through the submission of a Supplemental Report. A covered entity or a third party submitting a

[367] As noted in Section IV.D.iv.3.c, CISA interprets notification to terminate the requirement to submit Supplemental Reports only if no substantial new or different information is subsequently discovered by the covered entity. CISA believes the discovery of such information would indicate that the covered entity's belief that the incident was concluded, fully mitigated, and resolved, was inaccurate, rendering the declaration of closure void.

notification on a covered entity's behalf simply would indicate in the Supplemental Report that the purpose (or one of the purposes) of the Supplemental Report is to notify CISA that the covered entity believes the incident has concluded and been fully mitigated and resolved. The process for doing so would be the same as for the submission of any other Supplemental Report, which is described in § 226.6 of the regulation, although the submitter may be asked certain questions related to how the incident was concluded, mitigated, and resolved.

3. Third-Party Submission of CIRCIA Reports

CIRCIA authorizes covered entities to use third parties to submit Covered Cyber Incident Reports or Ransom Payment Reports on behalf of the covered entity. Specifically, 6 U.S.C. 681b(d)(1) states "[a] covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)." The following subsections address various aspects of third-party submission of CIRCIA Reports.

a. Who May Serve as a Third-Party Submitter

In response to the RFI, a number of commenters requested that CISA clarify the types of third parties authorized to submit CIRCIA Reports on behalf of a covered entity. A few commenters encouraged CISA to allow anyone approved by a covered entity to be able to submit a report on their behalf, while others encouraged CISA take the opposite approach and limit the types of entities that could serve as a third-party submitter. Some commenters provided specific types of entities that they believe CISA should authorize to serve as third-party submitters, including, but not limited to, ISACs, incident management firms, external legal representatives, state water associations, and SLTT jurisdictions to whom an entity is also obligated to report.

In 6 U.S.C. 681b(d)(1), Congress provides a list of entities that covered entities might use to report Covered Cyber Incident Reports or Ransom Payment Reports on the covered entity's behalf. Specifically, 6 U.S.C. 681b(d)(1) states a covered entity that is required to submit a Covered Cyber Incident Report or a Ransom Payment Report "may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm," to submit the required report. As Congress preceded this list with the phrase "such as," CISA interprets the list to be illustrative examples and not a closed list of which categories of third parties a covered entity may use to submit CIRCIA Reports on its behalf.

The few comments CISA received on this topic demonstrate that there may be a wide variety of types of organizations or individuals that a covered entity may wish to have submit a report on the covered entity's behalf. CISA does not at this time see any policy rationales for limiting the types of organizations or individuals that a covered entity can choose to submit a report on the covered entity's behalf, especially considering that the responsibility for complying with the regulation remains with the covered entity even if it uses a third party to submit a report on its behalf. 6 U.S.C. 681b(d)(3). On the contrary, CISA sees value in allowing the covered entity the flexibility to determine which party is best situated to submit CIRCIA Reports on its behalf. Accordingly, CISA is proposing that a covered entity may use any organization or individual it chooses to submit a CIRCIA Report on its behalf.

While CISA is proposing that a covered entity may select any organization or individual it chooses to submit a report on its behalf, the third party must be expressly authorized by the covered entity to submit a report on the covered entity's behalf for the report to be accepted by CISA for purposes of compliance with the regulation. As the requirement to submit a timely and accurate report under CIRCIA remains in all cases with the covered entity itself, it is imperative that the covered entity have expressly

authorized a third party to submit a report on its behalf. Express authorization can be granted in any number of ways, including verbally or in writing. Any report submitted by a third party that has not been expressly authorized by the covered entity to submit the report will not be imputed to the covered entity or considered by CISA for purposes of CIRCIA compliance.[368]

To better ensure that a report being submitted by a third party is being submitted subject to the express authorization of the covered entity, CISA is proposing requiring the third party to include in the submission an attestation that it has been expressly authorized by the covered entity to submit the report. This likely would be accomplished by requiring a third party to check a box in the online form attesting to this, or some other similar electronic mechanism. As a general legal prohibition against knowingly providing false information to the Federal government exists (see 18 U.S.C. 1001), CISA believes that requiring this attestation from the third party is a sufficient deterrent to prevent individuals or organizations from seeking to submit a CIRCIA Report on behalf of a covered entity without express authorization.

CISA considered requiring a third party to provide some sort of evidence verifying its claim of authorization, such as a contract or email clearly conferring the authority. CISA believes, however, that the deterrent value of requiring the third party to attest in the reporting form that they have the express authority to submit on behalf of the covered entity is sufficient to prevent most cases of unauthorized submissions, and that the marginal benefit provided by requiring evidence of such express authorization is

[368] Historically, CISA has on occasion received reports from individuals or organizations not directly affiliated with the entity experiencing the impact or otherwise not authorized to report the incident on behalf of the affected entity. This may occur, for instance, where an individual or organization is directly experiencing an incident that is causing cascading effects on another entity's information systems, where an individual or organization has become aware of what it believes to be an incident on another entity's cyber system, or where an employee of an organization that is experiencing a cyber incident elects to report an incident despite not having authority from the entity to report on its behalf. In these and other situations where an individual wants to submit a report about an incident without the consent of the covered entity experiencing the incident, it may do so through CISA's voluntary reporting portal; however, the information contained in that report will not be imputed to the entity experiencing the incident, nor will it be considered a report submitted for the purposes of CIRCIA compliance.

exceeded by the burden of providing specific evidence. Additionally, CISA believes requiring evidence beyond an attestation has the potential to disincentivize the use of third-party submitters, which CISA believes may be detrimental to organizations seeking to leverage third parties to assist with incident response and recovery.

Some commenters suggested that a third party must be in a formal, contractual relationship with the covered entity to submit on the entity's behalf. CISA believes this level of formality is not necessary and may not be practical in certain arrangements, such as where an entity is using an ISAC or an SLTT Government entity to submit on the entity's behalf. Accordingly, CISA is not proposing that a covered entity and third party must have entered into a formal, contractual agreement for the third party to be authorized to submit on the covered entity's behalf.

b. Types of CIRCIA Reports a Third Party May Submit

Section 681b(d)(1) of title 6, United States Code, states "[a] covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)." The subsection that clause refers to is 6 U.S.C. 681b(a) which, among other things, sets forth the general requirements related to Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports. Although the first part of 6 U.S.C. 681b(d)(1) only mentions Covered Cyber Incident Reports and Ransom Payment Reports, CISA interprets the phrase "submit the required report under subsection (a)" to cover not only Covered Cyber Incident Reports and Ransom Payment Reports, but Supplemental Reports as well.

CISA is not aware of any persuasive policy reasons for allowing a covered entity to use a third party to submit a Covered Cyber Incident Report or Ransom Payment Report on the entity's behalf, but not allow a third party to submit a Supplemental Report

to CISA on the covered entity's behalf; nor does CISA believe that was Congress's intent. Conversely, CISA believes that there would be benefits to allowing a covered entity to use a third party to submit a Supplemental Report on the covered entity's behalf, especially in cases where a covered entity used the same third party to submit a previous report on the covered entity's behalf. Accordingly, CISA is proposing that covered entities be allowed to use a third party to submit and update any type of CIRCIA Report—i.e., a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report—on behalf of the covered entity, so long as any other regulatory requirements related to using a third party to submit a CIRCIA Report on a covered entity's behalf are met. CISA further proposes that a covered entity need not have used a third party to submit its initial report (be it a Covered Cyber Incident Report or a Ransom Payment Report) to use a third party to submit a Supplemental Report or vice versa. Similarly, a covered entity can use different third-party submitters for subsequent CIRCIA Reports. Whether a covered entity submits a report itself or uses a third party, and who the third-party submitter is if one is used, is something the covered entity may decide each time it submits a CIRCIA Report.

CISA also is proposing to allow third parties to submit a single report on behalf of multiple covered entities if the circumstances leading to the reporting requirement for the various covered entities is similar enough to be reported collectively. For example, if a single cyber incident perpetrated against a CSP, managed service provider, or other third-party service provider impacts a number of the service provider's customers in a similar fashion, and those impacted customers are covered entities, the service provider may be well situated to submit a single report on behalf of itself and some or all of its affected customers. In such a situation, the rules regarding third party submissions still would apply, with the third-party service provider needing to have the authorization to report on behalf of any customer on whose behalf it is reporting, as well as the ability to provide all

of the information that the covered entity customer would have has to submit on its own, were it submitting its own CIRCIA Report. CISA believes this proposed approach will help reduce reporting burden while still providing a complete picture of the covered cyber incident.

c. Process for Submission of CIRCIA Reports by Third Parties

CISA is proposing that the process for the submission of a report by a third party on behalf of the covered entity be the same process as that which exists for the submission of a report by the covered entity itself, with two minor modifications. First, as noted in Section IV.E.iii.1.d in this document, CISA is proposing that a third-party submitter must attest in the reporting form to the fact that it has been authorized by the covered entity to submit the report on behalf of the covered entity. Second, as noted in Section IV.E.iii.4 in this document, CISA is proposing that any CIRCIA Report submitted by a third party include a small number of additional questions to ensure that CISA has a name and point of contact information for both the third-party submitter and the covered entity on whose behalf the report is being submitted. CISA's rationale for these two minor modifications are discussed in the respective sections of this document cited earlier in this paragraph.

d. Burden of Compliance when a Covered Entity Uses a Third Party to Submit a Report

A number of comments received by CISA in response to the RFI encourage CISA to confirm that the responsibilities for complying with the CIRCIA regulatory requirements do not shift from the covered entity to a third party when the covered entity uses a third party to submit a CIRCIA Report on the covered entity's behalf. CISA interprets the statutory language to affirm that use of a third party does not shift compliance responsibilities from the covered entity to the third party. While the statute authorizes a covered entity to use a third party to submit a report on the covered entity's

behalf, it does not at any point authorize CISA to hold a third-party submitter accountable for a covered entity's reporting responsibilities, nor does it at any point absolve the covered entity of its reporting obligations. In fact, 6 U.S.C. 681b(d)(3) indicates the contrary, stating third-party reporting "does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission." While 6 U.S.C. 681b(d)(3) does not mention Supplemental Reports, there similarly is nothing in the statute absolving a covered entity of the responsibility for submitting Supplemental Reports as required or shifting that responsibility to a third party, and CISA is unaware of any policy rationales for treating Supplemental Reports differently in this circumstance from Covered Cyber Incident Reports or Ransom Payment Reports.

Additional support for the interpretation that the burden does not shift to the third party when a covered entity uses a third party to submit on its behalf is found in 6 U.S.C. 681d(a), which explicitly refers to covered entities as the entity to which CISA is authorized to issue an RFI or a subpoena when it believes a covered entity has failed to submit a required CIRCIA Report. Likewise, the venue provision contained in 6 U.S.C. 681d(c)(2)(B) focuses on where the covered entity resides, is found, or does business for purposes of determining where a civil action may be brought. These sections make clear that any enforcement action for noncompliance is to be brought against the covered entity, not a third party that submitted (or failed to submit) a report on the covered entity's behalf. Consistent with this understanding, CISA interprets it to be the covered entity's responsibility to ensure that any CIRCIA Report submitted by a third-party on the covered entity's behalf is accurate and to correct any inaccurate or update incomplete information through the submission of a Supplemental Report.

e. Third Party Ransom Payments and Duty to Advise

Pursuant to 6 U.S.C. 681b(d)(2), a third party that makes a ransom payment on behalf of a covered entity impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for such ransom payment. The obligation to report that ransom payment remains with the covered entity, although the covered entity may authorize the third party who made the ransom payment, or a different third party, to submit a Ransom Payment Report to CISA on the covered entity's behalf. Accordingly, CISA proposes reflecting this in the proposed regulation by stating in § 226.12(d) that a third party that makes a ransom payment on behalf of a covered entity impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for the ransom payment.

Pursuant to 6 U.S.C. 681b(d)(4), however, a third party that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack does have a duty to advise that covered entity of its obligation to report the ransom payment to CISA. CISA proposes codifying this in the regulation in § 226.12(d). CISA recognizes that there may be situations where a chain of third parties is involved in making a ransom payment on behalf of a covered entity. CISA intends the duty to advise the covered entity of its reporting obligations to apply only to a third party who is directly engaging with the covered entity knowingly for the purposes of making the ransom payment. Third parties involved in the payment of the ransom who do not have a direct relationship with the covered entity or who are not aware that the funds being transmitted are for the purpose of paying a ransom payment are not obliged to inform the covered entity of CIRCIA reporting requirements.

vi. Request for Comments on Proposed Manner, Form, and Content of Reports

CISA seeks comments on all aspects of the proposed manner, form, and content of CIRCIA Reports, and the proposed procedures for submitting CIRCIA Reports, to include the following:

52. The proposed use of a web-based form as the primary means of submission of CIRCIA Reports, the proposed maintenance of telephonic reporting as a back-up reporting option, assumptions used in evaluating different possible manners of submission, and the possibility of allowing automated (i.e., machine-to-machine) reporting or other manners of submission in the future at the discretion of the Director.
53. The proposal to use a single, dynamic, web-based form for the submission of all types of CIRCIA Reports, regardless of whether the report is submitted by a covered entity or a third party on the covered entity's behalf.
54. The content CISA is proposing be included in all CIRCIA Reports and the specific proposed content for Covered Cyber Incident Reports, Ransom Payment Reports, Joint Covered Cyber Incident and Ransom Payment Reports, and Supplemental Reports, respectively, as well as additional content CISA is proposing to require when a third-party submitter is used to submit a CIRCIA Report on behalf of a covered entity.
55. The proposals CISA is making related to the timing of reports, including the proposed interpretation of "reasonable belief," the proposed interpretation for when a ransom payment "has been made," the proposed meaning of "promptly," the proposed meaning of "substantial new or different information," and the proposed meaning of "concluded" and "fully mitigated and resolved."

56. The proposed CIRCIA Report submission procedures, to include the process for notifying CISA that an incident has concluded and been fully mitigated and resolved.
57. The proposed rules regarding the submission of a report by a third party on behalf of a covered entity, to include who may serve as a third-party submitter, the types of CIRCIA Reports a third party may submit on behalf of a covered entity, the burden of compliance when a covered entity uses a third party to submit a report, and a third party's duty to advise a covered entity of the covered entity's CIRCIA reporting requirements when the third party makes a ransom payment on behalf of a covered entity.

F. Data and Records Preservation Requirements

Under CIRCIA, any covered entity that submits a CIRCIA Report must preserve data relevant to the reported covered cyber incident or ransom payment in accordance with procedures established in the final rule. 6 U.S.C. 681b(a)(4). To implement this requirement, CISA is to include in the final rule, a clear description of the types of data that covered entities must preserve, the period of time for which the data must be preserved, and allowable uses, processes, and procedures. See 6 U.S.C. 681b(c)(6).

As noted earlier, a covered entity's use of a third party to submit a CIRCIA Report on behalf of the covered entity does not shift compliance responsibilities from the covered entity to the third party. See IV.D.v.3.d. That principle holds true for data preservation requirements as well. A covered entity will retain responsibility for complying with the data preservation requirements established in the final rule even when the covered entity has a third party submit a required CIRCIA Report to CISA on behalf of the covered entity.

i. Types of Data That Must be Preserved

The preservation of data and records[369] in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom. Access to forensic data, such as records and logs, can help analysts uncover how malicious cyber activity was conducted, what vulnerabilities were exploited, what tactics were used, and so on, which can be essential to preventing others from falling victim to similar incidents in the future. How an incident was perpetrated may not be immediately identifiable upon discovery, and the failure to properly preserve data or records during the period of initial incident response can render it difficult to subsequently perform this analysis. This can especially be true in incidents involving zero-day vulnerabilities or highly complex malicious cyber activity by nation state threat actors, such as the "SUNBURST" malware that compromised legitimate updates of customers using the SolarWinds Orion product or the Hafnium campaign on Exchange servers, with the full extent, cause, or attribution of an incident often not being known until months after the initial discovery.[370]

Preservation of data is also central to law enforcement's ability to investigate and prosecute the crime. As stated by the Department of Justice (DOJ) in their guidance for Federal prosecutors entitled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, "Electronic records such as computer network logs,

---

[369] The section in CIRCIA addressing this topic, 6 U.S.C. 681b(a)(4), uses the terms "data" and "information" at different times to characterize what a covered entity must preserve. CIRCIA does not, however, define either term. Rather than add to, or attempt to select from, the numerous definitions that have been proffered for both terms in a wide variety of cyber-related resources, CISA is proposing instead to include in the regulation a list of items that a covered entity will be required to preserve. See proposed § 226.13(b). The proposed list includes data and information in various forms, such as logs, images, registry entries, and reports. To better reflect the spectrum of information CISA is proposing to require entities to preserve, and in recognition of the fact that the term "records" is commonly used in the area of data or records retention, CISA is proposing to use the term "data and records" instead of simply "data" or "information."

[370] See, e.g., Adam J. Hart, *Evidence Preservation: The Key to Limiting the Scope of a Breach*, American Bar Association Cybersecurity and Data Privacy Committee Newsletter (Spring 2021), available at https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/evidence-preservation/ (hereinafter "*Evidence Preservation*").

email, word processing files, and image files increasingly provide the government with important (and sometimes essential) evidence in criminal cases."[371] Failure to properly preserve relevant data and other forensic evidence can make identification and prosecution of the perpetrators of a cyber incident significantly harder, if not impossible.

In order to support these activities, and consistent with the authorities provided to CISA in 6 U.S.C. 681b(a)(4) and 681(c)(6), CISA is proposing requiring covered entities to preserve a variety of data and records related to any covered cyber incidents or ransom payments reported to CISA in a CIRCIA Report. Specifically, CISA is proposing to require covered entities preserve data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data;[372] data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity. See § 226.13(b).

CISA developed the proposed list of data and records to be preserved based upon its own experience with conducting incident detection, response, prevention, and analysis; by reviewing both best practices related to incident management, data preservation, and post-incident forensic analysis and stakeholder recommendations provided in response to the CIRCIA RFI and at the CIRCIA listening sessions; and following consultations with various Federal partners, to include the FBI and DOJ. Each of the proposed categories of data and records contains information directly relevant to questions and reporting elements of incident reports, as well as potentially helps CISA or

---

[371] Department of Justice Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at ix (2009), available at https://www.justice.gov/criminal/criminal-ccips/ccips-documents-and-reports.

[372] CISA is not proposing that a covered entity be required to preserve copies of all of the exfiltrated data; rather, CISA is proposing that a covered entity preserve information related to the data, such as the type and amount of data exfiltrated.

other investigators identify and understand the TTPs used to perpetrate the incident, the vulnerabilities exploited in doing so, and potentially the identity of the perpetrator of the incident. The data and records proposed for preservation additionally may be useful in subsequent law enforcement investigations and prosecution of the individual or individuals who perpetrated the incident.

A covered entity that has any of the data or records listed above must preserve those data or records regardless of what format they are in, whether they are electronic or not, located onsite or offsite, found in the network or in the cloud, etc. A covered entity is not, however, required to create any data or records it does not already have in its possession based on this regulatory requirement. The requirement for a covered entity to preserve data or records applies only to the extent the entity already has created, or would be creating them, irrespective of CIRCIA.

CISA is aware that retaining data and records is not without cost. In recognition of this, CISA attempted to reduce or focus the list of items to be retained to those that CISA believes would most likely be of value in support of future analysis or investigation. For instance, rather than require covered entities retain all log entries or memory captures from the time of the incident in case any of them may have contained pertinent data, CISA is proposing to limit this to log entries, memory captures, or forensic images that the covered entity believes in good faith are relevant to the incident. Similarly, CISA is not proposing that a covered entity be required to preserve copies of all data that was exfiltrated during an incident, but rather simply proposes that a covered entity preserve information sufficient to understand what type of and how much data was exfiltrated.

ii. Required Preservation Period

CISA is proposing that covered entities that submit CIRCIA Reports must begin preserving the required data at the earlier of either (a) the date upon which the entity

establishes a reasonable belief that a covered cyber incident has occurred, or (b) the date upon which a ransom payment was disbursed, and must preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted pursuant to § 226.3, to include any Supplemental Reports. Accordingly, if a covered entity only submits a single CIRCIA Report to CISA on a covered cyber incident or ransom payment, then the data preservation obligation is two years from the submission of the Covered Cyber Incident Report, Ransom Payment Report, or Joint Covered Cyber Incident and Ransom Payment Report. If, however, a covered entity submits one or more Supplemental Reports on a single covered cyber incident or ransom payment, the two-year retention period restarts at the time of submission of each Supplemental Report.

In establishing this proposed two-year timeframe, CISA considered existing best practices regarding preservation of information related to cyber incidents, data retention or preservation requirements from comparable regulatory programs, and comments received on this issue from stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions. In Section 3.4.3 of its *Computer Security Incident Handling Guide*,[373] NIST discusses best practices for retaining evidence in the aftermath of a cybersecurity incident. Specifically, NIST Special Publication 800-61 Revision 2 (NIST SP 800-61r2) encourages organizations to establish policies regarding retention of evidence from an incident and states that "[m]ost organizations choose to retain all evidence for months or years after the incident ends." In determining how long an entity should choose to preserve evidence, NIST recommends entities consider three factors. First, NIST notes that evidence may be needed in order to prosecute the threat actor which, in some cases, may take several years. On this point, NIST also notes that sometimes evidence that seems insignificant at the time of the incident will become more important in the future.

[373] *NIST SP 800-61r2*, *supra* note 362, at 41.

The second factor NIST suggests entities consider is any existing internal data retention policies. As a point of reference, NIST notes that the General Records Schedule for Information Systems Security Records requires Federal departments and agencies to maintain computer security incident handling, reporting, and follow-up records for three years after all necessary follow-up actions have been completed.[374] The final factor NIST mentions as something that should be considered is cost. NIST notes that certain items preserved as evidence generally may be inexpensive individually, but costs can be substantial if an organization stores such items for years. Outside of noting the three-year retention period included in the General Records Schedule, NIST SP 800-61r2 does not recommend a specific timeframe as a best practice for data preservation.

While most existing cyber incident reporting requirements do not include timeframes specifically targeted at preservation of records related to a cyber incident, many do have broader recordkeeping requirements that frequently apply to cyber incident reports and/or other data or records related to a reportable cyber incident. For instance, facilities subject to CFATS are required to maintain records on incidents and breaches of security for three years.[375] The NRC similarly requires regulated entities to maintain a copy of any written report submitted to the NRC on a cyber incident for three years.[376] MTSA requires covered facilities to retain all records related to MTSA, including those related to cybersecurity incidents, for at least two years.[377] And while not a regulation, M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," requires Federal government entities subject to Executive Order 14028, "Improving the Nation's Cybersecurity," to retain

[374] National Archives, *General Records Schedule 3.2: Information Systems Security Records*, Item 020 (Jan. 2023), available at https://www.archives.gov/records-mgmt/grs.html.
[375] 6 CFR 27.255(a).
[376] 10 CFR 73.77(d)(12).
[377] 33 CFR 105.225(a).

most logs and certain other items related to cybersecurity incidents for a period of 30 months.[378]

CISA did not receive many comments from stakeholders on the topic of data preservation in response to the RFI or at CIRCIA listening sessions, but those stakeholders who did comment on the length of preservation generally recommended timeframes consistent with those identified above. Specifically, one commenter recommended requiring data be preserved for no longer than two years,[379] one commenter recommended requiring data be preserved for no longer than three years,[380] one commenter recommended being consistent with M-21-31,[381] and one commenter stated that data should be preserved for as long as needed, but not in perpetuity.[382] While not providing specific recommendations on the duration of preservation requirements, at least two commenters did note that data preservation can be costly, and encouraged CISA to develop preservation requirements that are not overly burdensome and limited in scope and duration.[383]

Based on the above, CISA believes that a data preservation requirement typically lasting anywhere between two and three years would be consistent with existing best practices across industry and the Federal government, would be implementable by the regulated community, and would achieve the purposes for which data preservation is intended under CIRCIA. Recognizing that the costs for preserving data increase the longer the data must be retained, and wanting to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the purposes of the regulation,

---

[378] See Office of Management and Budget, M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 27, 2021), available at https://www.fedramp.gov/2023-07-14-fedramp-guidance-for-m-21-31-and-m-22-09/.
[379] Comments submitted by SAP, CISA-2022-0010-0114.
[380] Comments submitted by the National Association of Chemical Distributors, CISA-2022-0010-0056.
[381] Comments submitted by Sophos, Inc., CISA-2022-0010-0047.
[382] Comments submitted by the American Chemistry Council, CISA-2022-0010-0098.
[383] See, e.g., Comments Submitted by CTIA, CISA-2022-0010-0070, and the Information Technology Industry Council, CISA-2022-0010-0097.

CISA thus is proposing that covered entities must preserve the required data and records for the lower end of the spectrum of best practice for data preservation, i.e., a period of two years, unless substantial new or different information is discovered or additional actions occur that require the submission of a Supplemental Report and a commensurate extension of the data preservation timeframe.

iii. Data Preservation Procedural Requirements

Section 681b(c)(6) of title 6, United States Code, requires CISA to include in the final rule a clear description of the processes and procedures a covered entity must follow when preserving data. In light of the different manners in which the various required data and records can be stored, CISA is proposing to give covered entities significant flexibility in determining how to preserve the data and records, so long as the preservation method retains all salient details. This may include electronic or non-electronic (i.e., hard copy) storage, onsite or offsite storage, network or cloud storage, and active or cold (i.e., archived) storage. CISA believes that this flexibility will allow a covered entity to determine the most cost-effective way to preserve the data and records given the entity's specific circumstances and the nature and format of the data and records being preserved.

CISA is proposing to impose two limitations on this flexibility, however. First, CISA is proposing that the covered entity must store the data and records in a manner that allows the data and records to be readily accessible and retrievable by the covered entity in response to a lawful government request. CISA does not intend for this provision to require entities to maintain the data onsite and have it immediately available upon request. Rather, CISA expects a covered entity to be able to retrieve and provide the data and records in response to a lawful government request within a reasonable amount of time.

Second, CISA is proposing to require covered entities to employ reasonable safeguards to protect the data and records against unauthorized access or disclosure, deterioration, deletion, destruction, and alteration. These safeguards must include protections against both natural and man-made, intentional and unintentional events, including cyber incidents. NIST Special Publication 1800-25, "Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events," provides examples of the types of best practices that a covered entity might employ to meet this proposed requirement.

iv. Request for Comments on Proposed Data Preservation Requirements

CISA seeks comments on the proposed data preservation requirements, to include:

58. The types of data CISA is proposing covered entities preserve.

59. The proposed length of time covered entities must preserve data for.

60. The proposed procedural requirements governing the preservation of data.

61. Any other aspect of the proposed data preservation requirements.

G. Enforcement

i. Overview

CIRCIA provides a variety of mechanisms for CISA to use if CISA believes that a covered entity has failed to submit a CIRCIA Report in accordance with CIRCIA regulatory requirements. See 6 U.S.C. 681d. The potential approaches CISA has to address noncompliance include issuance of an RFI (6 U.S.C. 681d(b)), issuance of a subpoena (6 U.S.C. 681d(c)(1)), referral to the Attorney General to bring a civil action to enforce the subpoena and/or pursue a potential contempt of court (6 U.S.C. 681d(c)(2)), and other enforcement mechanisms to include potential acquisition penalties, suspension, and debarment (6 U.S.C. 681b(c)(8)(B)(ii)). Section 681b(c)(8)(B) of title 6, United

States Code, requires CISA to include in the final rule procedures to carry out these enforcement provisions. Sections 226.14 through 226.17 of the proposed rule contain CISA's proposed procedures for each of these enforcement mechanisms, each of which is described in greater detail below.

Pursuant to 6 U.S.C. 681d(e), CISA must consider certain factors when determining whether to exercise any of these enforcement authorities. Specifically, CIRCIA mandates the Director take into consideration the complexity of determining whether a covered cyber incident occurred, and the covered entity's prior interaction with CISA or its understanding of the policies and procedures for reporting for covered cyber incidents and ransom payments, as part of the process for evaluating whether to exercise an enforcement mechanism. CISA is proposing to include this statutory requirement essentially verbatim in § 226.14(b) of the proposed regulation. CISA will develop policies and procedures to ensure that the factors stated above are applied similarly to covered entities in similar circumstances.

CIRCIA additionally states that its enforcement provisions do not apply to SLTT Government Entities. 6 U.S.C. 681d(f). CISA proposes including this SLTT exclusion in § 226.14(a). What qualifies as a SLTT Government entity is defined in proposed § 226.1 and discussed in Section IV.A.iv.12 in this document.

ii. Request for Information

CIRCIA authorizes the Director to request information from a covered entity if the Director has reason to believe that the covered entity has experienced a covered cyber incident or made a ransom payment but failed to report the covered cyber incident or ransom payment in accordance with CIRCIA regulation. 6 U.S.C. 681d(b)(1). Through an RFI, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment occurred. 6 U.S.C. 681d(b)(1). Proposed § 226.14(c) contains the language CISA is proposing regarding

CISA's authority to issue an RFI, the form and content of an RFI, requirements a covered entity must follow to adequately respond to the RFI, the treatment of information included in a response to an RFI, and the inability for the issuance of an RFI to be appealed.

1. Issuance of Request

Proposed § 226.14(c) begins with a description of CISA's authority to issue an RFI. The proposed language starts first with the acknowledgement that the Director has the authority to delegate the issuance of an RFI, and then identifies the two different scenarios that may be the basis of the issuance of an RFI.

Although CIRCIA prohibits the delegation of the Director's subpoena authority to another individual, CIRCIA does not similarly restrict who may issue an RFI. To provide CISA with additional flexibility regarding who may be able to issue an RFI, CISA is proposing to allow an RFI to be issued by either the Director or a designee of the Director. This would allow the Director to formally designate another individual (or more than one individual) as having the authority to issue an RFI. CISA believes this flexibility will help ensure CISA's ability to issue RFIs in a timely manner, which may be essential in a rapidly unfolding, potentially substantial cyber incident. Accordingly, CISA proposes defining the Director in § 226.1 to include the Director of CISA or any designee.

Section 681d(b)(1) of title 6, United States Code, authorizes CISA to issue an RFI when CISA has reason to believe that a covered entity has experienced a covered cyber incident or made a ransom payment, but failed to report it "in accordance" with 6 U.S.C. 681b(a). CISA proposes including this authority in § 226.14(c)(1), which would authorize the issuance of an RFI to a covered entity when CISA has reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with section 226.3. CISA interprets this language to

allow CISA to issue an RFI in two distinct circumstances. First, CISA interprets this to allow CISA to issue an RFI when it believes a covered entity failed to report a covered cyber incident it experienced or a ransom payment it made. Second, CISA interprets this to allow issuance of an RFI to receive additional information following a covered entity's submission of a report that CISA believes is deficient or otherwise noncompliant. This second scenario includes when CISA believes a covered entity failed to submit a Supplemental Report as required.

A plain reading of 6 U.S.C. 681d(b)(1) makes it clear that CISA is authorized to issue an RFI when CISA believes a covered entity experienced a covered cyber incident or ransom payment but failed to report it. That section of CIRCIA also provides additional context for what the Director, or Director's designee, may use to determine that a covered entity failed to submit a required CIRCIA Report. Specifically, CIRCIA states that CISA may base its decision to issue an RFI (or subpoena, if necessary) on public reporting or information in the possession of the Federal government. CISA proposes including this in § 226.14(c)(1) of the proposed regulation. CISA construes "information in the possession of the Federal government" broadly, to include, among other categories, information derived by CISA analysis, information reported by the covered entity, information from other sources typically used or shared by the government, or any combination of such information.

CISA interprets the language of 6 U.S.C. 681d(b)(1) to also authorize CISA to issue an RFI in cases where a covered entity submitted a report, but the report was deficient or otherwise noncompliant. For a number of reasons, CISA believes this to be the correct interpretation. First, CISA interprets the phrase "in accordance" to not only require that a covered entity submitted a report, but that it did so in a manner that complies with all the CIRCIA regulatory requirements for a report of the type in question. CISA believes that the use of the phrase "to confirm whether or not a covered

cyber incident or ransom payment has occurred" in 6 U.S.C. 681d(b)(1) also supports this interpretation. CISA interprets "confirm" to include verification, thus allowing CISA to request information from a covered entity necessary for CISA to confirm (i.e., verify) that an incident or payment discussed in an incomplete report submitted by the covered entity was in fact a covered cyber incident or reportable ransom payment. Finally, CISA believes this interpretation also is supported by the fact that CIRCIA authorizes CISA to issue a subpoena to "obtain the information required to be reported pursuant to section 681b of this title." 6 U.S.C. 681d(c)(1). As the enforcement process requires the issuance of an RFI prior to the issuance of a subpoena, it is only logical that CISA would be able to issue an RFI for information it has the authority to request through a subsequent enforcement mechanism. For the same reason, CISA interprets the language to allow for the issuance of an RFI when CISA believes an entity has failed to submit a Supplemental Report as required.

2. Form and Contents of the RFI

Proposed § 226.14(c)(2) contains CISA's proposal regarding the content CISA will include in an RFI. While not required to do so by the statute, CISA believes that enumerating the minimum content that CISA must include in an RFI will help ensure that a covered entity receives information explaining why the RFI is being issued and the necessary elements for the covered entity's response to be adequate. CISA proposes that an RFI must include the covered entity's contact information; a summary of the facts describing CISA's reason to believe that the covered entity failed to report a covered event in compliance with the regulation; a description of other requested information to allow CISA to confirm whether a reportable event occurred; the form in which information must be provided; and the date the information is due. As set forth in proposed § 226.14(c)(2), CISA interprets "information" broadly, including, among other things, tangible items, electronically stored information, and verbal or written responses.

In certain cases, CISA may want to issue an RFI based on facts that are derived from nonpublic, confidential, or classified information, sources, or processes. CISA is proposing in § 226.14(c)(2)(ii) and (f) that, in such a case, CISA will not reveal the nonpublic, confidential, or classified information, sources, or processes, and may limit the summary of the facts to a statement that CISA is aware of facts indicating that the covered entity has failed to report a covered cyber incident or ransom payment as required.

3. RFI Response

Proposed § 226.14(c)(3) states that a covered entity must reply in the manner and format, and within the deadline, set forth in the RFI. If the covered entity's response to the RFI is inadequate, the Director, or Director's designee, may request additional information from the covered entity to determine whether a covered cyber incident or ransom payment occurred, or the Director may issue a subpoena to compel the provision of information. Examples of an inadequate response to an RFI include, but are not limited to, failing to respond to the RFI, providing a response with insufficient information for CISA to confirm that a covered cyber incident or ransom payment occurred, or a covered entity's continued failure to comply with the mandatory covered cyber incident, ransom payment, and/or Supplemental Report reporting obligations set forth in § 226.3.

4. Treatment of Information Received

Under 6 U.S.C. 681d(b)(2), information provided to CISA in response to an RFI is to be treated as if it was submitted through the standard reporting procedures established for submission of a CIRCIA Report. As a result, information submitted by a covered entity in response to an RFI receives the protections afforded by § 226.18 as well as the privacy and civil liberties procedures of § 226.19, to information submitted in a CIRCIA Report. This includes information provided to CISA in response to a request for additional information following a covered entity's inadequate response to an RFI. CISA

has included language in § 226.14(c)(4) of the proposed regulation confirming that the information protections that apply to information contained in CIRCIA Reports applies to information submitted in response to an RFI. As discussed below, however, these protections do not apply to information provided by the covered entity in response to a subpoena.

5. Unavailability of Appeal

CISA does not consider an RFI to constitute a final agency action. RFIs have no immediate regulatory implications for the entity, but rather are an interim step in CISA's compliance communications with an entity and are not final agency action that has legal consequences for a party.[384]

In other words, the substance of any enforceable requirements triggering legal liability are not established by the RFI—any such requirements, if they are imposed, will not be established until CISA issues a subpoena for information. Consequently, the RFI is not final agency action. Pursuant to 5 U.S.C. 704, only final agency actions are subject to judicial review. Accordingly, as an RFI is not a final agency action, the issuance of an RFI cannot be appealed. CISA proposes including § 226.14(c)(5) to provide notice that the issuance of an RFI is not appealable.

iii. Subpoena

Pursuant to 6 U.S.C. 681d(c)(1), if the Director has not received an adequate response to an RFI within 72 hours of issuance of the RFI, the Director may issue to the covered entity a subpoena to compel disclosure of information deemed necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required within the applicable CIRCIA Report, as well as information

[384] See *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (agency action may not be interlocutory in nature, but must represent the "consummation of the agency's decision making process" and be an action "by which rights or obligations have been determined or from which legal consequences will flow" (internal quotation marks omitted)).

necessary to assess potential impacts of the incident to national security, economic security, or public health and safety. CISA views the use of the word "may" in 6 U.S.C. 681d(c)(1) as providing the Director discretion in determining whether or not to issue a subpoena, and there could be times that the Director issues a second RFI if the covered entity's reply was incomplete or unclear such that CISA cannot confirm whether or not a covered cyber incident or ransom payment has occurred. Proposed § 226.14(d)(1) codifies this in the regulation, articulating that the Director may issue a subpoena to compel disclosure of information from a covered entity if the entity fails to reply to an RFI or provides an inadequate response. CISA interprets "inadequate response" to mean the submission of a response to the RFI with omitted, incomplete, unclear, or otherwise insufficient answers to the Director's, or Director's designee's, RFI. CISA also interprets "inadequate response" as including the covered entity's continued failure to comply with the mandatory Covered Cyber Incident, Ransom Payment, and/or Supplemental Report reporting obligations set forth in 226.3.

1. Timing of Subpoena

Section 681d(c)(1) of title 6, United States Code, provides that the Director may issue a subpoena if a covered entity fails to respond to an RFI within 72 hours. CISA interprets this timeframe as the minimum period after which the Director may issue a subpoena. Thus, CISA is proposing to state in § 226.14(d)(2) that the Director may not issue a subpoena earlier than 72 hours after the date of service of an RFI. There is no deadline by which the Director must issue a subpoena; the Director may issue a subpoena any time after 72 hours from the date on which the Director issues an RFI.

2. Form and Contents of Subpoena

Proposed § 226.14(d)(3) contains CISA's proposal regarding the content CISA will include in a subpoena. Similar to the form and content of an RFI, CISA believes that enumerating the minimum required content that must be included in a subpoena will help

ensure that a covered entity receives information explaining why the subpoena is being issued and the requirements for an adequate response. CISA proposes a subpoena must include the name and address of the covered entity, an explanation of the basis for issuing the subpoena and a copy of the relevant RFI, a description of the information requested, the date by which the covered entity must reply, and the manner and form in which the covered entity must provide the information to CISA. As in regard to the information that may be required in response to an RFI, CISA interprets "information" broadly here, including, among other things, tangible items, electronically stored information, and verbal or written responses.

In certain cases, CISA may want to issue a subpoena based on facts that are derived from nonpublic, confidential, or classified information, sources, or processes. CISA is proposing in § 226.14(d)(3)(ii) and (f) that, in such a case, CISA will not reveal the nonpublic, confidential, or classified information, sources, or processes, and may limit the summary of the facts to a statement that CISA is aware of facts indicating that the covered entity has failed to report a covered cyber incident, ransom payment, or substantial new or different information as required.

3. Reply to the Subpoena

Proposed § 226.14(d)(4) sets forth the subpoena response requirements for a covered entity. It states that the subpoenaed covered entity must respond by the deadline identified in the subpoena, and in the manner and format specified in the subpoena by the Director.

If the covered entity's response to the subpoena is inadequate, the Director may request or subpoena additional information from the covered entity or request civil enforcement of the subpoena. Examples of inadequate response include, but are not limited to, a complete failure to respond, providing a response that does not allow CISA to determine whether a covered cyber incident or ransom payment occurred, providing a

response that does not fully comply with the regulatory reporting requirements, or providing a response that is otherwise insufficient to assess the potential impacts to national security, economic security, or public health and safety. As further discussed below, information provided in response to a subpoena may be referred to the Attorney General for criminal prosecution or the head of a regulatory enforcement agency for enforcement if the Director believes that there is a basis for such action based on the information received.

CISA considers any responses to CISA's subsequent engagement with a subpoenaed entity related to the covered cyber incident or ransom payment as subpoenaed information for the purpose of referral to the Attorney General or head of a regulatory agency and application of information protections. Thus, this information may be provided to the Attorney General or head of a regulatory enforcement agency as discussed in § 226.14(d)(6)(ii) and is not entitled to the protections set forth in § 226.18. The Director will take into account the covered entity's engagement and cooperation with CISA when determining whether to provide information to the Attorney General or head of a regulatory agency for criminal prosecution or regulatory enforcement, respectively, or to pursue civil enforcement.

4. Authentication Requirement for Electronic Subpoenas

Section 681d(c)(4)(A) of title 6, United States Code, states that any electronically issued subpoena must be authenticated with a cryptographic digital signature of an authorized representative of CISA, or other comparable technology, that allows CISA to demonstrate that CISA issued the subpoena and that the subpoena has not been altered or modified since its issuance. CISA will make available, for example on its website, information by which subpoena recipients can verify that the signature was provided by an authorized representative of CISA. A recipient of any electronically issued subpoena without the required authentication does not need to consider the subpoena to be valid.

See 6 U.S.C. 681d(c)(4)(A). Proposed § 226.14(d)(5) reflects this requirement essentially verbatim. This authentication requirement applies solely to electronically issued subpoenas.

5. Treatment of Information Received in Response to a Subpoena

CIRCIA provides a number of protections to information submitted to CISA voluntarily, as part of a compliant CIRCIA Report, or in response to an RFI. These protections, all of which are mandated by CIRCIA, are set forth in § 226.18 of the proposed regulation and described in Section IV.H.i in this document. CIRCIA does not explicitly require similar protections be afforded to information provided in response to a subpoena issued under CIRCIA. CISA is proposing to explicitly note in § 226.14(d)(6) of the regulation that these protections do not apply to information submitted in response to a subpoena. Similarly, CIRCIA does not require that the privacy and civil liberties procedures apply to information provided in response to a subpoena issued under CIRCIA, and thus CISA proposes to note explicitly in the regulatory text that these procedures do not apply to information submitted in response to a subpoena. The reason CISA is proposing that the CIRCIA-specific privacy and civil liberties procedures would not apply to responses to subpoenas is that such information is subject to different handling limitations and authorized uses than information received in a CIRCIA Report or in response to an RFI. Of note, subpoenaed information may be shared with certain law enforcement and regulatory officials. Although the CIRCIA-specific privacy and civil liberties procedures that CISA is proposing would not apply, CISA notes that any personal information contained in responses to subpoenas would still be handled in accordance with the Privacy Act of 1974[385] and the E-Government Act of 2002.[386]

[385] See 5 U.S.C. 552a.
[386] See 44 U.S.C. 3501 note, Pub. L. 107–347.

CISA is proposing this approach in the hopes that the unavailability of these protections for information submitted in response to a subpoena will serve as an incentive for covered entities to comply with the applicable regulation or an RFI, thus preventing the need for issuance of a subpoena. The RFI provides a window for covered entities that have failed to submit a CIRCIA Report, as required, to comply with their legal obligations. If the covered entity remedies their noncompliance at that time, the covered entity is entitled to protections under § 226.18 and procedures under § 226.19. If the entity remains noncompliant and CISA elects to issue a subpoena, any subsequent information provided by the covered entity in response to the subpoena will not benefit from those protections.

This section of the proposed regulation also includes language related to the Director's authority under 6 U.S.C. 681d(d)(1) to provide information submitted by a covered entity in response to a subpoena to the Attorney General or head of a Federal regulatory agency if the Director determines that the facts relating to the covered cyber incident or ransom payment may constitute grounds for criminal prosecution or regulatory enforcement action. As part of the decision-making process related to the exercise of this authority, the Director is allowed to consult with the Attorney General or the head of the appropriate Federal regulatory agency. See 6 U.S.C. 681d(d)(2). For reasons similar to those discussed in Section IV.G.ii.5 in this document above regarding the appealability of the issuance of an RFI, CISA proposes including in § 226.14(d)(6)(ii) a statement that any decision by the Director to execute this authority is not a final agency action and cannot be appealed.

6. Withdrawal and Appeals of Subpoena Issuance

Section 226.14(d)(7)(i) provides that CISA, in its discretion, may withdraw a subpoena. If CISA withdraws a subpoena, CISA will serve the notice of withdrawal as set forth in § 226.14(e). Section 226.14(d)(7)(ii) addresses appeals of a subpoena issuance.

CISA is proposing to allow covered entities to appeal the issuance of a subpoena within seven calendar days after the date of service by providing a written request to the Director to withdraw the subpoena. CISA is proposing requiring a Notice of Appeal to contain, at a minimum, the name of the covered entity appealing the subpoena issuance, the request that the Director withdraw the subpoena, the rationale for the request (e.g., why the entity believes it is not a covered entity; why the entity believes that the incident is not a covered cyber incident), and any additional information the covered entity would like the Director to consider.

iv. Service of an RFI, Subpoena, or Notice of Withdrawal

Proposed § 226.14(e) sets forth the service process for an RFI, subpoena, or notice of withdrawal of a subpoena. CISA is proposing that these documents may be served on an officer, managing or general agent, or any other agent authorized by appointment or law to receive service or process, and that they may be served through a reasonable electronic or non-electronic means that demonstrates receipt, such as certified mail with return receipt, express commercial courier delivery, or electronic delivery. CISA further is proposing that the date of service of any RFI, subpoena, or notice of withdrawal of a subpoena shall be the date on which the document is mailed, electronically transmitted, or delivered in person, whichever is applicable. These proposed processes are consistent with standard processes used for service of legal documents.

v. Enforcement of Subpoenas

Pursuant to 6 U.S.C. 681d(c)(2)(A), if a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce the subpoena. A civil action to enforce a subpoena under CIRCIA may be brought in any judicial district in which the covered entity against whom the action is brought resides, is found, or does business. 6 U.S.C.

681d(c)(2)(B). A court may punish a failure to comply with a CIRCIA subpoena as contempt of court. 6 U.S.C. 681d(c)(2)(C). CISA has proposed language reflecting these statutory authorities in § 226.15 of the proposed regulation.

The Director's referral of a subpoena to the Attorney General is discretionary. As discussed above, prior to making such a referral, the Director must consider, among other things, the covered entity's prior engagement with CISA.

vi. Acquisition, Suspension, and Debarment Enforcement Procedures

Section 681b(c)(8)(B)(ii) of title 6, United States Code, requires CISA to include in the final rule procedures related to "other available enforcement mechanisms including acquisition, suspension and debarment procedures." CISA is proposing procedures to effectuate this clause in §§ 226.16 and 226.17 of the proposed regulation.

Proposed § 226.16 would require the Director to refer all circumstances concerning a covered entity's noncompliance that may warrant suspension and debarment action to the DHS Suspension and Debarment Official. Suspension and debarment are meant to help protect the Federal government from fraud, waste and abuse by supporting the Federal government's ability to avoid doing business with non-responsible contractors.[387] By including this requirement in CIRCIA, Congress has provided CISA with an enforcement mechanism to both discourage and, when necessary, punish noncompliance by making it more difficult for entities who meet the standard for suspension and debarment to do business with the Federal government.

Proposed § 226.17 address the "acquisition" portion of 6 U.S.C. 681b(c)(8)(B)(ii), by authorizing the Director to provide information regarding a noncompliant entity who has a procurement contract with the Federal government to the contracting official

[387] See GSA, *Frequently Asked Questions: Suspension & Debarment*, https://www.gsa.gov/policy-regulations/policy/acquisition-policy/office-of-acquisition-policy/gsa-acq-policy-integrity-workforce/suspension-debarment-and-agency-protests/frequently-asked-questions-suspension-debarment (last visited Nov. 28, 2023).

responsible for oversight of the contract in question and to the Attorney General. Whether or not any action can or should be taken against the entity who is the subject of the referred information is up to the contracting official's Department or Agency or the Attorney General, not CISA.

vii. Penalty for False Statements and Representations

Any person that knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, RFI Response, or reply to an administrative subpoena is subject to penalties under 18 U.S.C. 1001. CISA interprets materially false or fraudulent statements or representations relating to CIRCIA to potentially include, but not be limited to, knowingly and willfully doing any of the following: submitting a CIRCIA Report for an incident that did not occur, claiming to be a representative of a covered entity whom you do not in fact represent, certifying you are a third party authorized to submit on behalf of a covered entity when you do not have authorization, and including false information within a CIRCIA Report, RFI Response, or response to an administrative subpoena. CISA would not consider scenarios where a covered entity reports information that it reasonably believes to be true at the time of submission, but later learns through investigation that it was not correct and submits a Supplemental Report reflecting this new information, to constitute a false statement or representation. Penalties for making false statements and representations under 18 U.S.C. 1001 include a fine or imprisonment for not more than five years. The maximum penalty for making false statements and penalties increases to eight years imprisonment if the false statement is related to international or domestic terrorism or certain sexual offenses. As part of implementing this proposed provision, CISA would refer potential violations of this proposed provision to DOJ, and DOJ would determine whether to prosecute violators of 18 U.S.C. 1001. Further, the inclusion of materially false or fraudulent statements or representations in submissions to CISA would not

receive the protections and restrictions on use enumerated in § 226.18 because they would be inaccurate, incomplete, or invalid submissions that do not satisfy the regulatory reporting obligations and requirements proposed by this Part.

viii. Request for Comments on Proposed Enforcement

CISA seeks comments on its proposed approach to enforcement and noncompliance, including the following:

62. The proposed approach for RFIs, to include the delegation of authority to issue an RFI; the circumstances in which an RFI should be issued; the form and content of an RFI; the manner, form, and timeline for responding to an RFI; the treatment of information received in response to an RFI; and the lack of availability of an appeal for an RFI;
63. The proposed approach for subpoenas, to include the circumstances in which a subpoena should be issued; the timing of issuance of a subpoena; the form and content of a subpoena; the manner, form, and timeline for responding to a subpoena; the treatment of information received in response to a subpoena; and the withdrawal and appeal of a subpoena;
64. The proposed service process for an RFI, Subpoena, or Notice of Withdrawal;
65. The proposed process for enforcement of subpoenas, to include the referral of the matter to the Attorney General to bring a civil action; and
66. The proposed acquisition, suspension, and debarment enforcement procedures.

H. Protections

i. Treatment of Information and Restrictions on Use

1. Overview

CIRCIA applies a variety of information protections and restrictions on the use of CIRCIA Reports, as well as information submitted in response to an RFI. See

6 U.S.C. 681d(b)(2), 681e(b), 681e(a)(1) and (5). CIRCIA also provides liability protection for any person or entity that submits a CIRCIA Report in compliance with the reporting requirements established in the CIRCIA regulation or in a response to an RFI, as described in greater detail below. See 6 U.S.C. 681e(c). To ensure that the full suite of information protections and restrictions on use of CIRCIA Reports authorized by CIRCIA applies consistently to CIRCIA Reports or information in CIRCIA reports (as applicable), as well as responses to RFIs, CISA proposes to include them in § 226.18 of the proposed rule. However, as discussed in the section on Treatment of Information Received in Response to a Subpoena (Section IV.G.iii.5 in this document), CIRCIA does not require similar protections to be afforded to information provided in response to a subpoena issued under CIRCIA. Therefore, CISA proposes to specifically exclude all information and reports submitted in response to a subpoena from receiving any of the protections provided under § 226.18 of the proposed rule.

Consistent with 6 U.S.C. 681e, § 226.18 generally includes protections governing how CIRCIA Reports or the information submitted therein and responses to RFIs must be treated within the U.S. Government and restricts how CIRCIA Reports or the information submitted therein and responses to RFIs may be used. The proposed rule separates these protections into two broad categories with the specific protections afforded to (1) CIRCIA Reports or information submitted in CIRCIA Reports and responses to RFIs and (2) reporting entities and persons detailed under each. Specifically, CISA proposes under the first category, Treatment of Information, the following protections which are consistent with 6 U.S.C. 681e: (a) Designation as Commercial, Financial, and Proprietary Information, (b) Exemption from Disclosure under FOIA, (c) No Waiver of Privilege or Protection Provided by Law, and (d) an Ex Parte Communications Waiver. Under Restrictions on Use, CISA proposes the following restrictions consistent with 6 U.S.C. 681e: (a) Prohibition on Use in Regulatory Actions, (b) Liability Protection and

Evidentiary and Discovery Bar for CIRCIA Reports, and (c) Authorized Uses. CISA's understanding and interpretation of each of these protections and restrictions is provided in more detail below. Consistent with 6 U.S.C. 681e, § 226.18(a) notes that each provision of § 226.18 applies to CIRCIA Reports or the information in CIRCIA Reports, as stated in the respective subsection.

2. Treatment of Information

a. Designation as Commercial, Financial, and Proprietary Information

Consistent with 6 U.S.C. 681e(b)(1), § 226.18(b)(1) provides that a covered entity may designate a CIRCIA Report, a response to an RFI, or any portion thereof, as commercial, financial, and proprietary information by clearly designating the report or a portion thereof as such with appropriate markings at the time of submission. CISA intends to enable covered entities or third parties to easily perform this designation when submitting a CIRCIA Report by including in the web-based form for all CIRCIA Reports a mechanism such as a check box through which such a designation can be made. Upon a covered entity or third-party submitter making the designation, CISA will treat the CIRCIA Report, or the designated portions thereof, as commercial, financial, and proprietary information belonging to the covered entity.

b. Exemption from Disclosure Under FOIA

Consistent with 6 U.S.C. 681e(b)(2), § 226.18(b)(2) provides that CIRCIA Reports and responses to RFIs submitted in compliance with the CIRCIA regulation are exempt from disclosure under section 552(b)(3) of the FOIA and any State, Local, or Tribal government freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. CISA proposes that, in the event CISA receives a FOIA request for which a CIRCIA Report or response to RFI would be responsive, CISA would assert that this

exemption from disclosure under FOIA applies to such CIRCIA Report or response to RFI if submitted by a covered entity or third-party submitter in conformance with the manner, form, and content requirements described in §§ 226.6 through 226.11. CISA does not see any compelling policy reason or legal rationale to interpret this CIRCIA statutory exemption from disclosure under the FOIA any differently than as the plain language states and interprets the CIRCIA FOIA exemption to protect against disclosure of CIRCIA Reports and responses to RFIs. Further, if CISA receives a FOIA request for a CIRCIA Report, response to RFI, or information contained therein, CISA will apply any other applicable exemptions, consistent with DHS FOIA regulations.

c. No Waiver of Privilege

Consistent with 6 U.S.C. 681e(b)(3), § 226.18(b)(3) provides that a covered entity does not waive any applicable privilege or protection provided by law, including trade secret protection, as a consequence of submitting a CIRCIA Report or response to an RFI in conformance with the CIRCIA regulations. Accordingly, to the extent that any claim of a waiver is based on disclosure of the information to the Federal government, CISA proposes to interpret the CIRCIA provisions to cover all circumstances where state or Federal privileges and protections may attach, including privileges or protections such as the attorney-client and work-product privileges, as well as others recognized under common law.

d. Ex Parte Communications Waiver

Consistent with 6 U.S.C. 681e(b)(4), § 226.18(b)(4) provides that CIRCIA Reports and responses to RFIs submitted in conformance with the CIRCIA regulation are not subject to the rules or procedures of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official, including any concerns about ex parte communications related to rulemaking or other processes under the Administrative Procedure Act, 5 U.S.C. 553 *et seq.* Consistent with this

understanding, CISA proposes that the ex parte communications waiver offered by CIRCIA also extends to the procedures of any Federal agency or department regarding ex parte communications as CISA notes that not all Federal departments and agencies have rules that govern this issue.

3. Restrictions on Use

a. Prohibition on Use in Regulatory Actions

Consistent with 6 U.S.C. 681e(a)(5), proposed § 226.18(c)(1) provides that Federal and SLTT governments are prohibited from using information obtained solely through a CIRCIA Report submitted pursuant to the CIRCIA regulation or in a response to an RFI to regulate, including through an enforcement proceeding, the activities of a covered entity or any entity that made a ransom payment on behalf of a covered entity.[388] CISA also proposes two exceptions to this prohibition that track 6 U.S.C. 681(a)(5)(A) and 681(a)(5)(B), respectively. First, CISA is proposing that information in CIRCIA Reports and responses to RFIs may be used to regulate if a Federal or SLTT Government entity expressly allows the covered entity to meet any separate regulatory reporting requirement that Federal or SLTT Government entity has in place through submission of CIRCIA Reports to CISA. Second, CISA is proposing that CIRCIA Reports and responses to RFIs may be used consistent with Federal or State authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems to inform the development or implementation of regulation relating to such systems.

CISA views the first exception described above as applying to situations where a Federal or SLTT Government entity has independent regulatory authority to mandate reporting of covered cyber incidents or ransom payments but has elected to streamline its

[388] CISA notes that cyber incident reporting that another agency separately obtains pursuant to reporting requirements issued under its own authorities, even if subsequently shared with CISA under an approved information sharing agreement (such as a CIRCIA Agreement), is not a "CIRCIA Report" as proposed to be defined in § 226.1. Therefore, such information is not obtained "solely" through a CIRCIA Report (even if separately obtained through a CIRCIA Report), and therefore is not subject to this bar.

own independent regulatory reporting requirements by allowing covered entities to submit such reports to CISA to satisfy both regulatory reporting requirements. Both currently and prior to the passage of CIRCIA, a small number of Federal regulators either direct or permit regulated entities to meet the respective regulator's cyber incident reporting requirements via reporting to CISA. For example, entities subject to TSA's cyber incident reporting requirements must report cybersecurity incidents to CISA via the internet reporting form or by telephone, and certain entities within the BES are required to provide cyber incident reports to both CISA and the Electricity ISAC. Pursuant to this exception, reports such as these, which are submitted to CISA by a covered entity in part to satisfy another independent regulatory reporting requirement, are permitted to be used by Federal and SLTT regulators for regulatory purposes, notwithstanding the otherwise generally applicable bar on regulatory use in § 226.18(c).

CISA notes that the second exception to the general prohibition on regulatory use of CIRCIA Reports and responses to RFIs is that they can provide Federal and SLTT government regulators with information to better understand the cyber threat landscape and the threats and trends that may be impacting the particular community that they are responsible for regulating.

b. Liability Protection

Consistent with 6 U.S.C. 681e(c)(1), proposed § 226.18(c)(2)(i) provides that no cause of action shall lie or be maintained in any court by any person for the submission of a CIRCIA Report submitted in conformance with the requirements of the CIRCIA regulation or response to an RFI and must be promptly dismissed by the court. Section 226.18(c)(2)(i) also clarifies the extent of this liability protection, which only applies to or affects civil litigation that is solely based on the submission of a CIRCIA Report or response to an RFI. This liability protection does not serve to shield covered entities from liability for the underlying covered cyber incident, ransomware attack, or ransom

payment, should there be a separate basis for liability (e.g., a violation of state consumer protection laws that was exploited by the cyber incident). Nor does the provision shield covered entities from liability for associated criminal acts. Additionally, § 226.18(c)(2)(iii) creates an exception that is consistent with 6 U.S.C. 681e(c)(3), which exempts actions taken by the Federal government to enforce CIRCIA's reporting requirements as described in the enforcement Section IV.G in this document. Therefore, civil actions brought by the Federal government to enforce a subpoena are exempt from liability protection afforded under CIRCIA and may proceed in court.

Finally, § 226.18(c)(2)(ii) creates an evidentiary and discovery bar that prohibits CIRCIA Reports, responses to RFIs, and any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting CIRCIA Reports or responses to RFIs from being received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof. Consistent with 6 U.S.C. 681e(c)(3), § 226.18(c)(2)(ii) clarifies that the evidentiary and discovery bar created by CIRCIA does not create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI.

While the scope of the liability protection offered by CIRCIA is limited to litigation solely based on the submission of a CIRCIA Report, the submitted CIRCIA Report or response to an RFI itself is subject to a broad evidentiary and discovery bar. The scope of settings and venues for which this bar applies is broad—evidence, discovery, or other uses in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or any political subdivision. However, CISA notes that the scope of materials subject to this bar is

narrow. Legislative history also makes clear that the intent was for this evidentiary and discovery bar to be limited to CIRCIA Reports, responses to RFIs, and the underlying materials created solely for the purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI, but does not apply to the underlying information contained in the report or response. Based on this understanding of legislative intent and a plain reading of CIRCIA, CISA understands this to mean that while a CIRCIA Report or response to an RFI could not, for example, be attached to a warrant application, the underlying information contained in the CIRCIA Report or response to an RFI could be used to support the warrant application.

Further, CISA cannot provide a CIRCIA Report or response to an RFI in response to a third-party discovery request. Similarly, the protection for other records is limited only to those created solely to facilitate preparing, drafting, or submitting a report; this would include, for example, a draft submission, or an email seeking to verify information for the express purpose of populating a CIRCIA Report or response to an RFI. However, a forensic incident report that was developed for the purpose of investigating the underlying incident, which happened to have been used in populating a CIRCIA Report or response to an RFI, would not be "created for the sole purpose of preparing, drafting, or submitting" a CIRCIA Report or response to an RFI. Therefore, CISA's view is that this bar would not create a defense to discovery for a record, such as the forensic record example above, that was not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI.

c. Limitations on Authorized Uses

Consistent with 6 U.S.C. 681e(a)(1), CISA proposes including a section in the regulations identifying the statutory limitations on the uses of information provided to CISA in a CIRCIA Report or response to an RFI. Specifically, proposed § 226.18(c)(3) generally states that information provided to CISA in a CIRCIA Report or response to an

RFI may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government solely for the delineated purposes. These purposes are generally consistent with the authorized use limitations for cyber threat indicators and defensive measures shared with the Federal government under the Cybersecurity Act of 2015 (6 U.S.C. 1501-1533), with the additional authorized purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of events required to be reported in accordance with § 226.3.[389] This additional authorized purpose would allow, for example, information provided to CISA in a CIRCIA Report or response to an RFI to be used by Federal law enforcement agencies to investigate, identify, capture, and prosecute perpetrators of cybercrime. In light of the often interconnected nature of cyber incidents and cyber campaigns, and the resulting holistic response actions that the Federal government may take to respond to such cyber incidents and campaigns, CISA views the proposed term "events" in proposed § 226.18(c)(3)(v)(A) to broadly to include events such as campaigns, individual cyber incidents, or otherwise related cyber incidents. CISA therefore interprets the statutory provision as authorizing the Federal government to use all of the information about cyber incidents provided to CISA in accordance with proposed § 226.3 or voluntarily for this additional authorized purpose. While not separately defined in the regulation, CISA understands "cybersecurity purpose" and "security vulnerability" to have the meaning given those terms in the Homeland Security Act of 2002, as amended, specifically at 6 U.S.C. 650.[390]

---

[389] This includes, for example, the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, which CISA interprets to include a terrorist act or use of a weapon of mass destruction.

[390] 6 U.S.C. 650(6) defines "cybersecurity purpose" as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." 6 U.S.C. 650(25) defines "security vulnerability" as "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control." In turn, 6

ii. Protection of Privacy and Civil Liberties

CIRCIA requires that the rule include procedures for protecting privacy and civil liberties consistent with processes adopted pursuant to 6 U.S.C. 1504(b) and for anonymizing and safeguarding, or no longer retaining information received through CIRICA Reports that is known to be personal information that is not directly related to a cybersecurity threat. See 6 U.S.C. 681b(c)(8)(D). CISA is proposing to include these procedures in § 226.19, and they would apply to personal information in CIRCIA Reports, as well as in information submitted in response to an RFI. CISA is proposing to place privacy controls and safeguards at the point of receipt of a CIRCIA Report as well as for the retention, use, and dissemination of a CIRCIA Report. CISA proposes that the procedures proposed in this section will not apply, however, to information and reports submitted in response to a subpoena. Although the CIRCIA-specific privacy and civil liberties procedures that CISA is proposing would not apply to subpoenaed information, CISA notes that information contained in responses to subpoenas would still be handled in accordance with the Privacy Act of 1974[391] and the E-Government Act of 2002.[392]

1. Instructions for Personal Information

CISA is proposing steps to minimize the collection of unnecessary personal information in CIRCIA Reports and in responses to RFIs. First, CISA is proposing that covered entities should only include personal information that is requested in the reporting form or in the RFI and should exclude any unnecessary personal information. CISA would include on the CIRCIA Incident Reporting Form instructions and guidance on when personal information should and should not be included in a CIRCIA Report. While some personal information, such as the contact information for the covered entity

---

U.S.C. 650(24) defines "security control" as "the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information."

[391] See 5 U.S.C. 552a.

[392] See 44 U.S.C. 3501 note, Pub. L. 107–347.

and information about the identity of the actor perpetrating the incident (if known), will be required for the CIRCIA Incident Reporting Form, CISA will endeavor to provide clear guidance to help covered entities avoid submitting extraneous personal information. For example, while the CIRCIA Report would require categories of information that were believed to have been accessed or acquired by an unauthorized person, CISA would provide guidance that CIRCIA Reports should not include any specific personal information that was accessed. Thus, while a covered entity might indicate whether, for example, medical or driver's license information was accessed in the incident, the covered entity should not provide the medical information itself nor a list of the compromised driver's license numbers or images.

CISA would also include privacy-preserving measures in the CIRCIA Incident Reporting Form tool itself to help prevent covered entities from including unnecessary personal information. Such measures could include limiting the number of fields requiring open-ended responses, as well as mechanisms to scan for indicators that unnecessary personal information might be included (e.g., information in standard social security number format) and prompts for the covered entity to verify whether the information is necessary to submit before proceeding with the report submission.

CISA considered, but is not proposing, prohibiting submission of unnecessary personal information in CIRCIA Reports. The Cybersecurity Act of 2015 includes a provision that requires non-Federal entities to review cyber threat indicators before submission to CISA to assess whether those indicators contain any information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information. See 6 U.S.C. 1502(b). Although a requirement to remove irrelevant personal information would likely reduce the amount of personal information collected through CIRCIA Reports, CISA is not proposing this option due to

the increased burden such a requirement would likely place on compliance with CIRCIA reporting requirements. Because such a prohibition would likely have required that CISA reject reports that include such information or otherwise determine that the report was not correctly submitted, such a prohibition would place a greater burden on covered entities to comply with CIRCIA reporting requirements and would likely make meeting the required report submission timelines more difficult. CISA welcomes comment on these and any other steps that could reduce the collection of unnecessary personal information.

2. Assessment of Personal Information

CISA is proposing to review each CIRCIA Report to determine if the report contains personal information other than the personal information specifically requested. Because some fields in the CIRCIA Incident Reporting Form specifically ask for personal information, such as covered entity contact information and certain information about the threat actor (if known), CISA would assume that those fields in a submitted CIRCIA Report contain personal information, and would not necessarily review those fields, though CISA may do so to determine if extraneous personal information might have been included. CISA would then assess the personal information to determine if it is directly related to a cybersecurity threat, as that term is proposed to be defined in proposed § 226.1. personal information that is necessary to detect, prevent, or mitigate a cybersecurity threat would be considered directly related to a cybersecurity threat. Examples of personal information directly related to a cybersecurity threat would include malicious IP addresses, spoofed email addresses, domains that contain names from which malicious emails were sent, compromised usernames, and spoofed identities in malicious emails. Examples of personal information that would typically not be directly related to a cybersecurity threat would include contact information of the victim or entity reporting on behalf of the victim, and the name of a recipient of a malicious email.

CISA would automate its reviews for personal information be automated to the extent practicable taking into consideration costs, technical complexities, and any other challenges associated with automation, and to use human review when necessary. Privacy controls and safeguards include the internal administrative, technical, and physical safeguards that CISA employs to ensure compliance with privacy requirements and manage privacy risks. Examples of the controls CISA would employ include ensuring only those who have a need to know can access, retain, or disseminate covered reports; ensuring those with a need to know are trained on proper handling procedures; and that activities using CIRCIA Reports are solely used for purposes in which the CIRCIA Report was first collected.

When CISA determines that personal information submitted in a CIRCIA Report is not directly related to a cybersecurity threat, CISA proposes to delete the information, unless it is necessary contact information. For personal information necessary for contacting the covered entity or the report submitter, CISA proposes to safeguard and anonymize the information prior to sharing the report outside of the Federal government, unless CISA receives the consent of the individual to share their personal information and the personal information can be shared without revealing the identity of the covered entity. CISA proposes to retain personal information that is directly related to a cybersecurity threat and may share such personal information consistent with the provisions of section 226.18 and the privacy and civil liberties guidance, which is described below.

Consistent with the approach to privacy and civil liberties protections in 6 U.S.C. 1504(b), CISA is proposing to develop and publish privacy and civil liberties guidance that would apply to CISA's retention, use, and dissemination of personal information contained in a CIRCIA Report, and which would also provide guidance to other Federal departments and agencies with which CISA shares CIRCIA Reports. The guidance is not

intended to place any requirements on regulated entities. CISA would draft the guidance to be consistent with the need to protect personal information from unauthorized use or disclosure and mitigate cybersecurity threats; thus, in the guidance, CISA would endeavor to balance the privacy and civil liberties concerns relating to the handling of personal information with the need, where applicable, for personal information to address cybersecurity threats.

In the guidance, CISA would describe how CISA would review reports to identify personal information and to determine whether the information is or is not related to a cybersecurity threat. CISA would also plan to describe in the guidance the use of technical capabilities to remove or anonymize personal information not directly related to a cybersecurity threat. CISA would also describe a process for the timely destruction of personal information that is not directly related to a cybersecurity threat and that is not contact information needed to contact the submitter or covered entity.

CISA would make the guidance publicly available, likely by publishing the guidance on its website at the same time as the publication of the final rule for this rulemaking. CISA proposes to review the effectiveness of the guidance one year after publication to ensure it is appropriate to the needs for retention, use, and dissemination of personal information for mitigation and protection against cybersecurity threats and appropriately protect privacy and civil liberties of individuals. CISA proposes to conduct periodic subsequent reviews after the initial review. The CISA Chief Privacy Officer will also conduct an initial review of CISA's compliance with the guidance after one year and subsequent periodic reviews not less than every three (3) years. Where reviews result in a change needed to the guidance, CISA would publish updated guidance on its website.

CISA has included draft guidance in the docket for this proposed rule and is accepting public comment on any aspect of the draft guidance.

iii. Digital Security

CISA recognizes that reports submitted under CIRCIA and responses to RFIs often will include sensitive security, business, or other confidential information. In addition to the legal protections described above that exist in part to ensure that sensitive information submitted in CIRCIA Reports and responses to RFIs is only shared with appropriate individuals or entities, CISA is committed to maintaining physical and cybersecurity measures in place to prevent illicit unauthorized access to the information CISA receives in CIRCIA Reports and responses to RFIs. At a minimum, and consistent with 6 U.S.C. 681e(a)(4), CISA will ensure that CIRCIA Reports, responses to RFIs, and any information contained therein are collected, stored, and protected in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

iv. Request for Comments on Proposed Protections

CISA seeks comments on its proposed approach to the treatment of information, restrictions of use, and applicable protections, including the following:

67. The proposed approach to designating CIRCIA Reports, responses to RFIs, or the information contained therein as commercial, financial, and proprietary information;
68. The proposed application of the exemption from disclosure under FOIA and similar freedom of information laws;
69. The proposed implementation of the statement that submission of a CIRCIA Report or response to RFI does not waive any applicable privilege or protection;
70. The proposal that CIRCIA Reports and responses to RFIs are not subject to the rules governing ex parte communications;

71. The proposed restrictions on the use of information obtained solely through CIRCIA Reports or response to RFIs in regulatory actions or as independent causes of liability;
72. The proposed restrictions on the receipt of CIRCIA Reports or responses to RFIs in evidence, their discoverability, or their other use in any trial, hearing, or similar proceeding; and
73. The proposed privacy and civil liberties protections, to include the steps proposed by CISA to minimize the collection of unnecessary personal information in CIRCIA Reports, the assessment of personal information contained therein, and the draft guidance CISA is proposing to create.

I. Severability

To the extent that any portion of this proposed rule becomes final and is declared unenforceable by a court, CISA has structured the proposed rule so that all remaining provisions are severable from each other to the extent practicable and remain in effect unless they are dependent on the vacated or enjoined provision. Thus, even if a court decision invalidating or vacating a portion of the CIRCIA final rule results in a partial amendment to the regulation or a reversion to the statutory language itself, CISA intends that the rest of the rule continue to operate.

V. Statutory and Regulatory Analyses

A. Regulatory Planning and Review

Executive Orders 12866, Regulatory Planning and Review,[393] as amended by Executive Order 14094, Modernizing Regulatory Review,[394] and 13563, Improving Regulation and Regulatory Review,[395] direct agencies to assess the costs and benefits of

[393] See EO 12866, *Regulatory Planning and Review*, 58 FR 190 (Oct. 4, 1993), available at http://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf.
[394] See EO 14094, *Modernizing Regulatory Review*, 88 FR 21879 (Apr. 11, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-04-11/pdf/2023-07760.pdf.

available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

The Office of Management and Budget (OMB) has designated this rule a "significant regulatory action" as defined under section 3(f)(1) of EO 12866, as amended by Executive Order 14094, because its annual effects on the economy would exceed $200 million in at least one year of the analysis. Accordingly, OMB has reviewed this proposed rule.

CISA has prepared a Preliminary Regulatory Impact Analysis (RIA) which can be found in the docket for this proposed rule. CISA welcomes comment on the Preliminary RIA, and includes a summary of findings below.

Through this NPRM, CISA proposes the following reporting requirements, collectively known as CIRCIA Reports:

- A covered entity that experiences a covered cyber incident must report that incident to CISA no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.
- A covered entity that makes a ransom payment, or has another entity make a ransom payment on its behalf, as the result of a ransomware attack against the covered entity must report that payment to CISA no later than 24 hours after the ransom payment has been disbursed.
- A covered entity that experiences a covered cyber incident and makes a ransom payment, or has another entity make a ransom payment on its behalf, that is

---

[395] See EO 13563, *Improving Regulation and Regulatory Review* (Jan. 18, 2011), available at http://www.reginfo.gov/public/jsp/Utilities/EO_13563.pdf.

related to the covered cyber incident may report both events to CISA in a joint report no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

- A covered entity must promptly submit a Supplemental Report about a previously reported covered cyber incident if substantial new or different information becomes available.
- A covered entity must submit a Supplemental Report if the covered entity makes a ransom payment, or has another entity make a ransom payment on its behalf, that relates to a covered cyber incident that was previously reported. The covered entity must submit the Supplemental Report to CISA no later than 24 hours after the ransom payment has been disbursed.

In addition to reporting, CISA proposes data and records preservation requirements, which would require that certain data and records related to reported covered cyber incidents and ransom payments be maintained beginning on the date upon which the covered entity establishes reasonable belief that a covered cyber incident occurred or the date upon which a ransom payment was disbursed and until two years following the last report submitted to CISA. This data and records preservation is essential to enabling investigation of cyber incidents.

CISA estimates that the total affected population of this proposed rule would be 351,383 covered entities based on the above criteria. However, due to overlap across the sector criteria as well as overlap between the entities covered under both the sector-based criteria and the size-based criterion (i.e., all large entities that are also captured under the sector-based criteria), CISA believes that this affected population represents an overestimate of the number of covered entities. As such, CISA assumes that there would be a 10% overlap, which has been removed from the total number of the affected

population. Table 1 below presents the total affected population by covered entity[396] criteria and the 10% reduction for the affected population.[397] For the rest of this analysis, CISA based its estimates on 316,244 covered entities, accounting for the 10% overlap.

Table 1: Affected Population, by Criteria

Criteria	Affected Population	
	Total	**Excluding the 10% Overlap**
Non-Small Entities	35,152	31,637
Sector-Based Criteria		
Owns or Operates a Covered Chemical Facility	3,249	2,924
Provides Wire or Radio Communications Service	71,250	64,125
Owns or Operates Critical Manufacturing Sector Infrastructure	42,728	38,455
Provides Operationally Critical Support to the DoD or Processes, Stores, or Transmits Covered Defense Information	80,000	72,000
Performs an Emergency Service or Function	9,257	8,331
Bulk Electric and Distribution System Entities	4,214	3,793
Owns or Operates Financial Services Sector Infrastructure	42,965	38,669
Qualifies as an SLTT Government Entity	3,231	2,908
Qualifies as an Education Facility	13,421	12,079
Involved with Information and Communications Technology to Support Election Processes	106	95
Provides Essential Public Health-Related Services	14,418	12,976
IT Entities	6,708	6,037
Owns or Operates a Commercial Nuclear Power Reactor or Fuel Cycle Facility	107	95
Transportation System Entities	5,752	5,177
Subject to Regulation Under the Maritime Transportation Security Act	4,530	4,077
Owns or Operates a Qualifying Community Water System or Publicly Owned Treatment Works	14,295	12,866
Total[398]	**351,383**	**316,244**

[396] This table identifies the covered entities that would be required to comply with the rule. In addition to these entities, CISA estimates that an additional approximately 13 million entities would not actually be covered entities but would still incur some burden to determine they are not covered entities. This is detailed in Section 2 of the Preliminary RIA.

[397] CISA does not expect there to be a 10% overlap uniformly across all sectors, but the overlap is applied uniformly for presentational purposes. Since the costs do not differ across criteria or covered entities, there is no difference in applying the overlap to each sector as opposed to applying it to the total number of affected covered entities.

The Preliminary RIA estimates the costs of complying with the proposed requirements for an affected population of 316,244 covered entities over the period of analysis.[399] The main industry cost drivers of this proposed rule are the costs associated with becoming familiar with the rule, data and records preservation, and reporting requirements. Other costs include those associated with help desk calls and enforcement actions. Although this analysis uses a base year of 2024, CISA estimates industry costs beginning in 2025 upon the expected publication of the Final Rule. The combined cost of the NPRM is based on an 11-year period of analysis, as CISA estimates government costs starting in 2023 to account for costs incurred before the expected publication of the final rule, which is covered under the pre-regulatory baseline costs, as discussed in the preliminary RIA.

Under this proposed rule, familiarization costs include the time spent by an entity in a critical infrastructure sector to review the rule and/or other materials to help the entity determine if it is a covered entity subject to the rule, as well as time spent by a covered entity reading the rule to understand the requirements imposed by the rule. Familiarization costs also include an annual burden for covered entities to review any necessary CIRCIA documents to ensure proper compliance. For the reporting requirements, covered entities would have to submit a CIRCIA Report if they experience a covered cyber incident or make a ransom payment as the result of a ransomware attack. The costs associated with these reporting requirements are the opportunity cost of time spent completing the forms, including preparation time to gather the necessary information to complete the forms. Data and records preservation costs include the time

---

[398] As discussed in Section 2.3 of the Preliminary RIA, CISA anticipates the total number of covered entities is an overestimate as some of the not-small entities would also be captured by the sector-based criteria. In addition, CISA anticipates there to be overlap across the sector-based criteria. For example, the 80,000 DoD contractors likely include entities also captured under the critical manufacturing, transportation, and IT sectors. Other examples include likely overlap between the communications service providers and IT entities, and between CFATS and Maritime Transportation Security Act populations.

[399] For the purposes of this analysis, CISA presents a static affected population over the period of analysis.

burden for data and information to be collected and placed into appropriate storage, either physical or digital, and storage costs the entity incurs that they would not have incurred but for the proposed CIRCIA data and records preservation requirements.

i. **Number of Reports**

CISA expects the Final Rule to publish in late 2025. In order to comply with Administrative Procedure Act and Congressional Review Act requirements, CISA would be required to delay the effective date of the rule for a total of 60 days, which would likely push the effective date to 2026. Due to this required delay and uncertainty surrounding the publication date, covered entities will likely not begin submitting CIRCIA reports until 2026. As such, reporting costs, and other associated costs, other than familiarization costs, will be estimated starting in 2026.[400] Because there is a great deal of uncertainty regarding the number of CIRCIA Reports that would be required to be submitted upon implementation of this proposed rule, CISA presents a range for industry costs. As presented in the Preliminary RIA, CISA developed a sensitivity analysis for the range of expected number of CIRCIA Reports based on several sources, including current CISA voluntary reporting through CISA's web-based Incident Reporting Form, reporting under DOD and DOE mandatory reporting programs, and cyber loss data from the Information Risk Insights Study (IRIS) 2022 by the Cyentia Institute,[401] which was sponsored by CISA. Using these sources to inform the percentage of covered entities expected to submit CIRCIA Covered Cyber Incident Reports, CISA applies percentages of 2%, 5%, and 10% to the total affected population to conduct our low, primary, and high estimates for the number of cyber incidents that would need to be reported. These percentages were determined using the reporting rates from CISA, DoD, DOE, and the

[400] For this analysis, CISA uses 2024 as Year 1 to account for initial government costs to implement the CIRCIA regulatory program, making 2026 year 3 of the analysis. CISA also includes government costs from 2023 as part of the pre-regulatory baseline.
[401] Cyentia Institute, *Information Risk Insights Study 2022*, tbl. 3, Loss Summary, available at https://www.cyentia.com/iris-2022/.

Cyentia Institute ranges as reference points. As none of the reporting populations discussed above are fully representative of the CIRCIA population of covered entities, CISA developed reporting percentages that present a reasonable range of possible outcomes. This takes into account the low reporting estimate of 0.725% for DoD DFARS reporting as well as the higher reporting ranges presented by Cyentia. Recognizing that the majority of entities that are proposed to be subject to the CIRCIA reporting requirements are small businesses through the sector-based criteria,[402] CISA determined that it was appropriate to present reporting percentages in line with the lowest revenue categories presented by Cyentia and not the high end of their range.

The number of Ransom Payment Reports is based on data from Federal Bureau of Investigation (FBI) annual internet crime reports regarding the number of ransomware attacks for which complaints are received annually. In the 2021 and 2022 reports, the FBI reports the number of voluntary complaints that indicated organizations in one of the 16 critical infrastructure sectors had been victims of a ransomware attack. The Internet Crime Complaint Center received 649 such complaints in 2021,[403] and 870 in 2022.[404]

Based on this limited data, CISA forecast the number of ransomware attacks in critical infrastructure sectors by estimating the linear trend in the data based on available data from 2021 and 2022.[405] This results in an estimated 1,312 ransomware attacks that would be reported in 2024, which is Year 1 for this analysis, and an estimated 1,754 ransomware attacks in 2026, which is likely the first year in which covered entities would begin incurring reporting costs. CISA recognizes that not all ransomware attacks will

---

[402] According to the SBA, over 99% of all businesses are small businesses (see Section 2.1 of the Preliminary RIA). Additionally, the size standard criteria for covered entities represent approximately 6% of the regulated population, further supporting the assumption that the vast majority of covered entities would be considered small businesses.

[403] FBI, Internet Crime Complaint Center, *Internet Crime Report 2021*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

[404] FBI, Internet Crime Complaint Center. *Internet Crime Report 2022*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

[405] CISA conducted the forecast using Microsoft Excel's TREND function, which forecasts a linear trend based on the available data.

result in a ransom payment being made; however, given the lack of a consensus regarding what percentage of ransomware attacks do result in a ransom payment, CISA has elected to provide a very conservative estimate and assume that all ransomware attacks result in ransom payments.

CISA bases the estimated number of Ransom Payment Reports on these values on the FBI Internet Crime Complaint Center data.[406] For the purposes of this analysis, CISA anticipates receiving Ransom Payment Reports from 2026 to 2033, which would be a total of 20,220 Ransom Payment Reports. CISA also makes assumptions regarding the number of Joint Covered Cyber Incident and Ransom Payment Reports. For the purposes of this analysis, CISA assumes a low estimate of 1%, a primary estimate of 2%, and a high estimate of 3% of covered entities submitting a Ransom Payment Report would submit a Joint Covered Cyber Incident and Ransom Payment Report.[407]

In addition to the ranges presented for Covered Cyber Incident Reports, CISA also developed a range of estimates for Supplemental Reports. CISA assumes the number of Supplemental Reports would be based on a percentage of entities submitting Covered Cyber Incident Reports and Joint Covered Cyber Incident and Ransom Payment Reports. Due to the lack of available data on how many Supplemental Reports would need to be filed, CISA assumes 25% of entities submitting Covered Cyber Incident Reports and Joint Covered Cyber Incident and Ransom Payment Reports for the low estimate, 50% for the primary estimate, and 75% for the high estimate.[408] These percentages for Supplemental Reports are applied to the range of covered entities submitting Covered Cyber Incident Reports. For example, for each estimate in the range of covered cyber

---

[406] As reporting to the FBI Internet Crime Complaint Center is voluntary, this may be an underestimate to the extent that it does not capture any non-reported ransomware attacks in critical infrastructure sectors; however, it may be an overestimate to the extent that it is capturing ransomware attacks that did not result in ransom payments.

[407] The percentage of ransomware attacks that would be part of or would themselves be a covered cyber incident are based on CISA subject matter expertise. CISA requests comment on the number of Joint covered cyber incident and Ransom Payment Reports that would be filed.

[408] CISA requests comments on the number of Supplemental Reports that would be filed.

incidents (2%, 5%, and 10%), CISA applies the range of percentages of Supplemental Reports. Table 2 presents the range of Supplemental Reports for the primary estimate for this analysis, which applies the 50% of Covered Cyber Incident and Ransom Payment Reports resulting in a Supplemental Report across the range of estimates.[409]

In Table 2, CISA presents the estimated number of CIRCIA Reports, by report type for the primary estimate, which is 210,525.

Table 2: Number of CIRCIA Reports, Primary Estimate

Year	Covered Cyber Incident Reports	Ransom Payment Reports	Joint Covered Cyber Incident and Ransom Payment Reports	Supplemental Reports	Total
2024	0	0	0	0	**0**
2025	0	0	0	0	**0**
2026	15,812	1,754	35	7,906	25,507
2027	15,812	1,975	40	7,921	25,748
2028	15,812	2,196	44	7,924	25,976
2029	15,812	2,417	48	7,926	26,203
2030	15,812	2,638	53	7,928	26,431
2031	15,812	2,859	57	7,930	26,659
2032	15,812	3,080	62	7,932	26,886
2033	15,812	3,301	66	7,935	27,114
Total	**126,498**	**20,220**	**404**	**63,403**	**210,525**

In Table 3, CISA presents the estimated range for the number of CIRCIA Reports that would be submitted over the period of analysis, with a low estimate of 83,760, a primary estimate of 210,525, and a high estimate of 463,850 over the period of analysis.[410]

Table 3: Number of CIRCIA Reports

Year	Low Estimate	Primary Estimate	High Estimate
2024	0	0	0
2025	0	0	0

[409] Section 3.1 of the Preliminary RIA presents the number of Supplemental Reports in greater detail, breaking down the ranges for the low, primary, and high estimates for the number of reports submitted.
[410] Due to the high degree of uncertainty, CISA requests comment on the number of reports submitted, as well as the ranges used in this sensitivity analysis.

2026	9,681	25,507	57,149
2027	9,905	25,748	57,377
2028	10,129	25,976	57,639
2029	10,353	26,203	57,872
2030	10,577	26,431	58,104
2031	10,800	26,659	58,337
2032	11,024	26,886	58,570
2033	11,291	27,114	58,802
Total	**83,760**	**210,525**	**463,850**

Note. Totals may not sum due to rounding.

ii. Industry Cost

The main costs to industry associated with this proposed rule are those associated with covered entities and entities that fall within a critical infrastructure sector that are not covered entities (hereinafter, "non-covered entities") becoming sufficiently familiar with the rule to determine whether they are covered, and if it is determined that they meet one or more of the criteria for a covered entity, becoming familiar with how to comply with the requirements. The second largest cost associated with this rule would be data and records preservation costs, followed by the cost for covered entities to complete the forms for the CIRCIA Reports (including preparation time). Covered Entitles would also potentially incur costs associated with help desk calls and enforcement actions. For this analysis, all cost estimates are based on 2022 dollars.

Familiarization costs are estimated based on the opportunity cost of reading some or all of the rule or related materials to determine whether or not an entity is a covered entity, and if so, how to comply with the proposed rule. CISA estimates that covered entities would begin to incur familiarization costs upon publication of the Final Rule, with familiarization costs divided equally across years 2 and 3 of the period of analysis.[411] The Preliminary RIA presents a primary estimate of $33.58 for a non-covered entity to determine that they are not a covered entity, and a primary estimate of $1,587.49

[411] Some covered entities could begin reviewing and familiarizing themselves with the Final Rule upon publication in late 2025, before the effective date, which would likely not be until 2026 due to required delays for major rules associated with the Administrative Procedure Act and Congressional Review Act. Other covered entities could wait until the effective date.

for a covered entity to familiarize themselves with the proposed rule. This cost per entity is based on personnel in either the lawyer or general manager labor category (or some combination thereof) spending 0.275 hours per non-covered entity and 13 hours per covered entity to review the rule or related materials. This per entity cost and the total cost is presented in Table 4.

Table 4: Familiarization Cost by Entity Type, Primary Estimate

	Non-Covered Entities	**Covered Entities**
Hourly Time Burden	0.275	13
Weighted Average Cost per Entity	$33.58	$1,587.49
Number of Entities	12,864,239	316,244
Total Cost	**$432,000,574**	**$502,034,650**

Note: Totals may not sum due to rounding

In addition to initial familiarization costs for the affected population to read the rulemaking documents, CISA estimates an annual familiarization cost for covered entities to review CIRCIA program information. CISA bases this cost on each covered entity having a staff member equivalent to a General and Operations Manager spending 30 minutes (0.5 hours) reviewing the CIRCIA reporting forms, CIRCIA definitions, or any other information to ensure they are prepared to comply with the requirements if necessary. At an hourly compensation rate of $102.42, the per-entity cost is estimated to be $51.21.[412]

Combining the primary cost estimate for initial familiarization with the annual familiarization costs results in a total cost of $1.1 billion over the period of analysis, as presented in Table 5.

Table 5: Total Familiarization Costs ($ Millions, Undiscounted)

Year	**Initial Familiarization**	**Annual Familiarization**	**Total**

[412] $51.21 per entity = 0.5 hours × $102.42 per hour. Information on the hourly compensation rates used is contained in Section 3.2 of the Preliminary RIA.

	Non-Covered Entities	Covered Entities		
2024	$0	$0	$0	$0
2025	$251.0	$216.0	$0.0	**$467.0**
2026	$251.0	$216.0	$8.1	**$475.1**
2027	$0.0	$0.0	$16.2	**$16.2**
2028	$0.0	$0.0	$16.2	**$16.2**
2029	$0.0	$0.0	$16.2	**$16.2**
2030	$0.0	$0.0	$16.2	**$16.2**
2031	$0.0	$0.0	$16.2	**$16.2**
2032	$0.0	$0.0	$16.2	**$16.2**
2033	$0.0	$0.0	$16.2	**$16.2**
Total	**$502.0**	**$432.0**	**$121.5**	**$1,055.5**

Note. Totals may not sum due to rounding.

The reporting cost is estimated based on the time spent completing the CIRCIA Reports. CISA estimates that both Covered Cyber Incident and Ransom Payment Reports would take three hours to complete, a Joint Covered Cyber Incident and Ransom Payment Report would take 4.25 hours to complete, and a Supplemental Report would take 7.5 hours to complete. As described in the Preliminary RIA, CISA assumes a weighted average compensation rate of $86.29 for the personnel responsible for completing the report. Multiplying this compensation rate by the time burden and number of reports from the primary estimate results in an estimated cost of $79.1 million for CIRCIA Reports, as presented in Table 6.

Table 6: Cost of CIRCIA Reporting

Year	Covered Cyber Incident Reports	Supplemental Reports	Ransom Payment Reports	Incremental Cost of Joint Covered Cyber Incident and Ransom Payment Reports	Total
2024	$0	$0	$0	$0	**$0**
2025	$0	$0	$0	$0	**$0**
2026	$4,093,099	$5,116,373	$454,035	$3,784	**$9,667,290**
2027	$4,093,099	$5,126,294	$511,242	$4,260	**$9,734,895**
2028	$4,093,099	$5,127,724	$568,449	$4,737	**$9,794,009**
2029	$4,093,099	$5,129,154	$625,657	$5,214	**$9,853,123**
2030	$4,093,099	$5,130,584	$682,864	$5,691	**$9,912,237**
2031	$4,093,099	$5,132,015	$740,071	$6,167	**$9,971,352**
2032	$4,093,099	$5,133,445	$797,279	$6,644	**$10,030,466**
2033	$4,093,099	$5,134,875	$854,486	$7,121	**$10,089,580**

Total	**$32,744,788**	**$41,030,464**	**$5,234,082**	**$43,617**	**$79,052,951**

CISA also estimates costs associated with Data and Records Preservation. CISA estimates that a covered entity would spend six hours per submission to collect, store, and maintain records in the first year of the preservation period.[413] The cost of this provision is based on an hourly compensation rate of $35.19, which is the rate for Office and Administrative Support.[414] Based on six hours per year, at $35.19 per hour, the annual labor cost of data and record preservation would be $211.12.

CISA also estimates costs associated with acquiring additional storage to save records related to CIRCIA Reports. According to CISA Cybersecurity Division, a cyber incident generates four terabytes of data, on average.[415] To estimate the cost of storage for this amount of data, CISA conducted market research to determine the cost of sufficient cloud storage to store and access the data. Based on this research, the price of cloud storage for four terabytes of data would have an annual cost ranging from under $700 to almost $1,300.[416] Based on this range, CISA assumes that all covered entities that submit a CIRCIA Report would spend $1,000 per year on cloud storage for two years.[417] Applying the $1,000 cost for data and record preservation for the number of reports for two years results in a storage cost range of $132.4 million to $512.6 million, with a primary estimate of $275.1 million over the period of analysis.

---

[413] ICR 1670-0007 includes a burden of six hours per month to conduct electronic recordkeeping for CSAT. CISA applied the same six hours per month for CIRCIA, but only applies the burden to one month, as the covered entity is expected to undergo the recordkeeping burden only once, not on a recurring basis as with CSAT.

[414] Information on the hourly compensation rates used is contained in Section 3.2 of the Preliminary RIA. CISA requests comment on this cost, specifically on the level of burden required to compile the data and the appropriate personnel to complete the task.

[415] The estimate of four terabytes is based on the average of all incident response activities that CISA Threat Hunting engaged in in FY 2022 and FY 2023, and includes incidents across Federal, SLTT, critical infrastructure and non-critical infrastructure private entities.

[416] Enterprise Storage Forum, *Cloud Storage Pricing in 2023: Everything You Need to Know*, available at https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/.

[417] CISA recognizes that the data retention period may be longer than two years, particularly for the estimated 50% of covered entities that submit one or more Supplemental Reports for a covered cyber incident. CISA assumes that covered entities currently retain data under normal business practices, and as such, only estimates the marginal cost of an additional two years over the current retention practices. CISA requests comment on this assumption.

Combining the labor and storage costs results in a total data and record preservation cost range from $147.4 million to $570.4 million, with a primary estimate of $306.1 million, as presented in Table 7.

Table 7: Data and Record Preservation Costs

Year	Low Estimate	Primary Estimate	High Estimate
2024	$0	$0	$0
2025	$0	$0	$0
2026	$9,805,715	$21,317,218	$40,488,895
2027	$18,172,475	$39,191,526	$74,195,639
2028	$18,666,018	$39,689,956	$74,698,955
2029	$19,159,562	$40,188,386	$75,202,271
2030	$19,653,105	$40,686,816	$75,705,588
2031	$20,146,648	$41,185,246	$76,208,904
2032	$20,640,191	$41,683,675	$76,712,220
2033	$21,133,735	$42,182,105	$77,215,537
Total	**$147,377,449**	**$306,124,929**	**$570,428,009**

The cost associated with the help desk is the opportunity cost for personnel in the General and Operations Manager occupation at covered entities to call the help desk. CISA assumes that, on average, each covered entity that submits a report would call the help desk one time for each report submitted. The number of help desk calls is based on the number of reports, although a help desk call could be for any aspect of CIRCIA compliance such as registration, reporting, or data and record preservation. Based on similar costs for CSAT, CISA estimates an average time of ten minutes for a help desk call.[418] CISA estimates the cost per call by multiplying the time burden by the hourly compensation rate for the General and Operations Manager occupation of $102.42. Multiplying this hourly compensation rate by ten minutes (0.17 hours) results in an average cost of a help desk call of $17.07 for covered entities. Applying this cost to the

[418] CISA, ICR 1670-0007 Supporting Statement A, uploaded May 23, 2019, available at https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201905-1670-001. See Table 2, Estimated Annual Burden Hours and Costs by Reporting by Instrument. CISA uses the previous ICR estimate of ten minutes for the help desk burden rather than the most recent estimate of seven minutes, since CFATS is a more mature program and has been able to reduce help desk call times over time.

number of calls, CISA estimates the cost for help desk calls ranging from $1.4 million to $7.9 million, with a primary estimate of $3.6 million.

The Preliminary RIA also details potential enforcement costs based on the opportunity cost for a covered entity to respond to a Request for Information or a subpoena issued by CISA, including costs associated with a potential appeal of a subpoena. CISA estimates a total 10-year enforcement cost of $237,573, undiscounted. This is based on the issuance of 100 RFIs, five subpoenas, and one appeal per year.

CISA estimates the undiscounted cost to industry could range from $1.2 billion to $3.2 billion, with a primary estimate of $1.4 billion. Discounted at 2%, the primary cost would be $1.3 billion, with an annualized cost of $148.8 million. Table 8 presents the industry cost range for this analysis for the period from 2024 through 2033.

Table 8: Industry Cost Range, ($ Millions, Undiscounted)

Year	Low Estimate	Primary Estimate	High Estimate
2024	$0.0	$0.0	$0.0
2025	$467.0	$467.0	$1,171.6
2026	$488.1	$506.6	$1,244.3
2027	$37.6	$65.6	$114.5
2028	$38.1	$66.2	$115.1
2029	$38.7	$66.7	$115.7
2030	$39.2	$67.3	$116.2
2031	$39.8	$67.8	$116.8
2032	$40.3	$68.4	$117.4
2033	$40.9	$69.0	$117.9
Total	**$1,229.8**	**$1,444.5**	**$3,229.6**

Note. Totals may not sum due to rounding.

Table 9 presents the primary industry cost estimate for the period of analysis.

Table 9: Total Industry Cost, Primary Estimate ($ Millions)

Year	Familiarization Costs	Reporting Costs	Data Preservation Costs	Help Desk Costs	Enforcement Costs	Total	Discounted 2%
2024	$0.0	$0.0	$0.0	$0.00	$0.00	$0.0	**$0.0**
2025	$467.0	$0.0	$0.0	$0.00	$0.00	$467.0	**$448.9**

2026	$475.1	$9.7	$21.3	$0.44	$0.03	$506.6	**$477.3**
2027	$16.2	$9.7	$39.2	$0.44	$0.03	$65.6	**$60.6**
2028	$16.2	$9.8	$39.7	$0.44	$0.03	$66.2	**$59.9**
2029	$16.2	$9.9	$40.2	$0.45	$0.03	$66.7	**$59.2**
2030	$16.2	$9.9	$40.7	$0.45	$0.03	$67.3	**$58.6**
2031	$16.2	$10.0	$41.2	$0.46	$0.03	$67.8	**$57.9**
2032	$16.2	$10.0	$41.7	$0.46	$0.03	$68.4	**$57.2**
2033	$16.2	$10.1	$42.2	$0.46	$0.03	$69.0	**$56.6**
Total	**$1,055.5**	**$79.1**	**$306.1**	**$3.59**	**$0.24**	**$1,444.5**	**$1,336.2**
Annualized							***$148.8***

Note. Totals may not sum due to rounding.

Table 10 presents the total undiscounted industry cost by affected population.

Table 10: Cost by Covered Entity Criteria ($ Millions, Undiscounted)

Affected Population	Total 10-Year Cost, Undiscounted
Not Covered Entities	$432.0
Non-Small Entities	$101.3
Owns or Operates a Covered Chemical Facility	$9.4
Provides Wire or Radio Communications Service	$205.3
Owns or Operates Critical Manufacturing Sector Infrastructure	$123.1
Provides Operationally Critical Support to the Department of Defense or Processes, Stores, or Transmits Covered Defense Information	$230.5
Performs an Emergency Service or Function	$26.7
Bulk Electric and Distribution System Entities	$12.1
Owns or Operates Financial Services Sector Infrastructure	$123.8
Qualifies as a State, Local, Tribal, or Territorial Government Entity	$9.3
Qualifies as an Education Facility	$38.7
Entities Involved with Information and Communication Technologies Used to Support Core Election Processes	$0.3
Provides Essential Public Health-Related Services	$41.5
Information Technology Entities	$19.3
Owns or Operators a Commercial Nuclear Power Reactor or Fuel Cycle Facility	$0.3

Transportation System Entities	$16.6
Subject to Regulation Under the Maritime Transportation Security Act	$13.1
Owns or Operates a Qualifying Community Water System or Publicly Owned Treatment Works	$41.2
Total	**$1,444.5**

As discussed throughout Section 4 of the Preliminary RIA, there is a great deal of uncertainty in the cost estimates presented in this analysis. Because this would be a completely new regulatory program, it is difficult to predict precisely how the regulated population would respond. A number of assumptions used to estimate the costs have significant uncertainty around them, which has led CISA to develop a sensitivity analysis in the Preliminary RIA to account for this uncertainty. The main areas of uncertainty are:

- Number of CIRCIA Report Submissions – The number of reports is difficult to predict, as a mandatory reporting program with this scope does not currently exist, nor does a truly comparable program that CISA could use as a proxy. As such, CISA presents a range of possible outcomes for the number of reports submitted with percentages of entities reporting based on several data sources.
- Time Burden for Familiarization – Particularly as it relates to non-covered entities, CISA has no way to predict what level of effort such entities would invest in reading the rulemaking documents, nor can CISA predict the number of entities that would read all or some of the rulemaking documents, yet ultimately not be a covered entity. CISA also recognizes that there is a significant uncertainty regarding the time burden associated with a covered entity familiarizing themselves with the requirements. In this analysis, CISA estimates the cost based on the time necessary to read the NPRM, which is expected to be similar to that of reading the Final Rule. There is additional

uncertainty regarding the number of non-covered entities that would incur costs associated with familiarization. The current analysis estimates that approximately 12.9 million entities in critical infrastructure sectors would incur some costs associated with familiarization. However, it is unclear how many such entities would familiarize themselves with the rule, and whether or not entities outside critical infrastructure would potentially incur some familiarization costs to confirm that they are not covered entities (e.g., by reading the Applicability section and assessing whether they are or not in a critical infrastructure sector).

- Means for Data and Records Preservation – The analysis currently assumes that all covered entities that submit a report will comply with the Data and Records Preservation requirements by storing and maintaining digital records. CISA acknowledges that there may be some instances where hard copy records or data are maintained either in lieu of or in addition to at least some digital records, but does not estimate the potential cost of physical records. CISA expects that the cost of preserving physical records would replace, and be comparable to, the costs for digital records, rather be an additional cost of this provision.
- Number of Enforcement Actions – While CIRCIA empowers CISA to take enforcement action against covered entities that have not submitted required CIRCIA Reports, it is unclear how many of these actions CISA would take and which mechanisms would be leveraged. There is a great deal of uncertainty regarding how CISA would identify potentially non-compliant entities, as that would require CISA to be aware of an event that was not reported, or for CISA to be aware that an entity that reported has subsequently uncovered substantial new or different information than that which was

previously reported. Until CISA operationalizes this program, it is unable to accurately predict the number or nature of enforcement actions that would be needed.

There may also be implementation costs to the government and cost savings to the affected population associated with CIRCIA's substantially similar reporting exception, as discussed earlier in this NPRM. This reporting exception will allow covered entities subject to more than one Federal cyber incident reporting requirement to avoid having to report duplicative information to both CISA and another Federal agency when certain conditions are met. CISA believes that this exception would provide an overall cost savings, with the potential cost savings to the affected population through the avoidance of duplicative reporting requirements outweighing the implementation costs the government would incur (e.g., the costs associated with drafting, negotiating, and entering into CIRCIA Agreements, as defined in § 226.1 of the proposed rule). Because CIRCIA Agreements cannot be fully developed, and this exception cannot be fully implemented, until the final rule stage or after implementation of the regulatory program, at this time, CISA is unable to estimate what the impact of this exception would be on either government costs or industry savings.[419]

iii. Government Cost

CISA anticipates incurring significant costs associated with the creation, implementation, and operation of the government infrastructure to run the CIRCIA program. Implementing and operationalizing CIRCIA as statutorily mandated would require significant new government investment. This investment is necessary to develop and maintain the infrastructure, in both technology and personnel, necessary to receive, analyze, and share information from CIRCIA Reports submitted to CISA. While CISA

[419] While CISA does not estimate the cost for this provision, it is expected that the benefits to industry of avoiding duplicative reporting would exceed the costs to the government.

exercised some discretion in the description of covered entities, this description was scoped in such a way that reducing the number of the entities subject to the rule in a manner that would materially impact the government cost (i.e., by materially reducing the number of CIRCIA Reports received) would also sacrifice the extent to which the proposed rule would achieve the purpose of CIRCIA and the proposed rule, as described in section III.C.[420] This is particularly true for the government costs, where much of the costs would be incurred regardless of the scope of covered entities (e.g., the different aspects of the technology infrastructure). Further, as noted in section III.C, CISA believes that, due to advances in technology and strategies for managing large data sets, the potential challenges associated with receiving large volumes of reports can be mitigated through technological and procedural strategies.

CISA also has discretion in the period for Data and Records Preservation. However, this would not impact the government cost, as this is a cost borne by industry. For fiscal year 2023, CISA budgeted $34.5 million for CIRCIA related work. In 2024, CISA has requested $97.7 million, to perform work necessary to prepare for CIRCIA implementation. This includes funding to support several efforts specifically mandated by CIRCIA or necessary for the practical implementation of the CIRCIA mandates, such as the rulemaking process; stakeholder outreach; and efforts to begin creating the technology infrastructure necessary to receive and share reports, report on and use the information collected under CIRCIA, and other key functions. Because funding requested for 2023 has already been allocated, this is considered part of the pre-regulatory baseline

[420] For more information on how CISA considered rescoping the description of covered entities, see Section 0 and Section 5 of the Preliminary RIA, which present alternative approaches to the description of covered entities.

in the Preliminary RIA. Including the pre-regulatory baseline, CISA presents an 11-year government cost estimate for this proposed rule.[421]

CISA anticipates needing an annual budget of approximately $115.9 million to cover all the functions associated with CIRCIA. CISA anticipates this budget request to include funding for additional federal staff, contractor support, and new technology costs. Additional staffing would be necessary to conduct a myriad of mission-critical activities, such as analyzing the CIRCIA Reports to conduct trend and threat analysis, vulnerability and mitigation assessment, the provision of early warnings, incident response and mitigation, supporting Federal efforts to disrupt threat actors, and advancing cyber resiliency. Additional full-time equivalent staffing would be added to support the ingest of reports; engagement efforts, including a CIRCIA help desk;[422] CIRCIA enforcement actions; and other mission support roles. Technology costs would account for developing the infrastructure necessary to collect, maintain, automatically analyze, and share information from CIRCIA Reports as well as licenses, updates, and maintenance for CISA systems.[423]

As noted by the Cyberspace Solarium Commission, the government's cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its cyber risk identification and assessment efforts rely on comprehensive data and, prior to the passage of CIRCIA, the Federal government lacked a mandate to systematically collect cyber incident information reliably and at the scale necessary.[424] The government

---

[421] To account for the pre-regulatory baseline, CISA includes costs incurred in 2023. These costs are reverse discounted by applying the discount factor of 1.020 to the undiscounted cost of $34.5 million in year 2023.

[422] CISA would need to provide a means for the regulated public to contact CISA for assistance with complying with the final regulation when it becomes effective.

[423] Although CISA does not estimate industry costs for submitting CIRCIA reports until Year 3 (2026), CISA anticipates requesting the full CIRCIA annual budget of $115.9 million starting in Year 2 (2025) to ensure that all personnel and technology are in place once the Final Rule is published. As discussed below, there is a level of uncertainty regarding the government costs.

[424] *Cyberspace Solarium Commission Report*, supra note 23, at 103; see also Sandra Schmitz-Berndt, "Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive," *Journal of Cybersecurity* at 2 (Apr. 5, 2023) ("[L]ow reporting levels result in a flawed picture

investment discussed in the Preliminary RIA will provide CISA with the resources to meet the stated goals of CIRCIA. Specifically, the government cost presented in this NPRM will be used by CISA to develop and operationalize the system and infrastructure necessary to receive and analyze a sufficient quantity of Covered Cyber Incident Reports and Ransom Payment Reports from across critical infrastructure sectors, share information with stakeholders, and use that information and analysis to develop informational products and other tools to be shared with and leveraged by CISA's Federal and non-Federal stakeholders.

Because CISA has already begun making investments to operationalize the CIRCIA program in anticipation of the publication of the final rule in 2025, this analysis accounts for government costs from 2023 through 2033, or the full 10-year period of analysis and one year of pre-regulatory costs, even though industry would not incur costs until 2025 upon publication of the final rule. As presented in Table 11, CISA estimates an undiscounted government cost for CIRCIA of $1.2 billion over the period of analysis from 2023 through 2033. Discounted at 2%, the government cost would be $1.1 billion, with an annualized cost of $108.1 million.

Table 11: Government Cost ($ Millions)

Year	Undiscounted	Discounted at 2%
2023	$34.5	$34.5
2024	$97.7	$95.8
2025	$115.9	$111.4
2026	$115.9	$109.2
2027	$115.9	$107.1
2028	$115.9	$105.0
2029	$115.9	$102.9
2030	$115.9	$100.9
2031	$115.9	$98.9

of the threat landscape, which in turn may impact cybersecurity preparedness."), available at https://academic.oup.com/cybersecurity/article/9/1/tyad009/7160387.

2032	$115.9	$97.0
2033	$115.9	$95.1
Total	**$1,175.3**	**$1,057.7**
Annualized		***$108.1***

Note. Totals may not sum due to rounding.

iv. Combined Costs

Table 12 presents the combined industry and government costs over the period of analysis. Based on the primary estimates for industry's costs presented throughout Section 4 of the Preliminary RIA and the government costs presented in Section 5 of the Preliminary RIA, CISA estimates an undiscounted cost to industry and government over the period of analysis of $2.6 billion. Discounted at 2%, the estimated cost of this proposed rule over the period of analysis is $2.4 billion, with an annualized cost of $244.7 million.

Table 12: Combined Industry and Government Cost, Primary Estimate ($ Millions)

Year	Industry	Government	Total, Undiscounted	Total, Discounted 2%
2023	$0.0	$34.5	$34.5	$34.5
2024	$0.0	$97.7	$97.7	$95.8
2025	$467.0	$115.9	$582.9	$560.3
2026	$506.6	$115.9	$622.5	$586.6
2027	$65.6	$115.9	$181.5	$167.7
2028	$66.2	$115.9	$182.1	$164.9
2029	$66.7	$115.9	$182.6	$162.2
2030	$67.3	$115.9	$183.2	$159.5
2031	$67.8	$115.9	$183.7	$156.8
2032	$68.4	$115.9	$184.3	$154.2
2033	$69.0	$115.9	$184.9	$151.6
Total	**$1,444.5**	**$1,175.3**	**$2,619.8**	**$2,394.0**
Annualized				***$244.6***

Note. Totals may not sum due to rounding.

Table 13 presents the cost range for combined industry and government costs, discounted at 2%. The costs over the period of analysis range from a low estimate of $2.2

billion to a high estimate of $4.1 billion, and an annualized range of $225.4 million to $415.4 million., discounted at 2%[425]

Table 13: Combined Industry and Government Cost Range, ($ Millions)

Year	Low Estimate	Primary Estimate	High Estimate
2023	$34.5	$34.5	$34.5
2024	$95.8	$95.8	$95.8
2025	$560.3	$560.3	$1,237.5
2026	$569.1	$586.6	$1,281.8
2027	$141.8	$167.7	$212.9
2028	$139.5	$164.9	$209.2
2029	$137.3	$162.2	$205.6
2030	$135.1	$159.5	$202.1
2031	$132.9	$156.8	$198.6
2032	$130.7	$154.2	$195.2
2033	$128.6	$151.6	$191.8
Total	**$2,205.6**	**$2,394.0**	**$4,065.1**
Annualized	***$225.4***	***$244.6***	***$415.4***

Note. Totals may not sum due to rounding.

v. Benefits

The primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety. The provisions included in this proposed rule would support that purpose in a number of ways, providing several benefits. In this analysis, CISA discusses the qualitative benefits of the proposed rule.

Over the last decade, the United States has seen an exponential increase in cyber incidents, with nation-states, criminal actors, and other malicious cyber threat actors targeting entities across all of the critical infrastructure sectors with ever-evolving tactics, techniques, and procedures. Addressing this growing, dynamic threat requires a better understanding of the threat and the vulnerabilities being exploited, and the timely sharing of that information with owners and operators of internet-connected information systems so that they can take steps to better secure themselves from potential cyber incidents. As

[425] This analysis uses 2023 as the base year for costs estimates.

noted by the Cyberspace Solarium Commission, "The government's cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its risk identification and assessment efforts rely on comprehensive data. However, there are insufficient federal and state laws and policies requiring companies to report incidents that impact or threaten to impact business operations."[426] As discussed in greater detail below, CIRCIA would help the Federal government address this shortcoming by helping the Federal government understand the cyber threat landscape and enabling the timely sharing of information to enhance cyber resilience.

Under this proposed rule, covered entities would be required to report covered cyber incidents and ransom payments to CISA within the timeframes and other requirements described in the proposed rule. Collecting this information in a timely fashion (within 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred or 24 hours after a ransom payment has been disbursed) would provide the Federal government with enhanced cross-sector visibility into the cyber threat landscape and support the aggregation, analysis, and sharing of incident data in a way that heretofore has been unavailable to the cybersecurity community. This, in turn, would facilitate a better understanding by both Federal and non-Federal entities of who is causing cyber incidents; what types of entities malicious cyber actors are targeting; what tactics, techniques, and procedures malicious cyber actors are using to compromise entities in critical infrastructure sectors; what vulnerabilities are being exploited; what security defenses are effective at stopping the incidents; and what mitigation measures are successful in reducing the consequences of an incident.

While not part of the proposed rule,[427] CIRCIA recognizes the value of these activities and imposes upon CISA a number of requirements related to the analysis and

---

[426] *Cyberspace Solarium Commission Report*, *supra* note 23, at 103-04.
[427] As Congress imposed these obligations solely on Federal departments and agencies, they are not included in the CIRCIA proposed rule itself.

sharing of information received through CIRCIA Reports to ensure their value is reasonably maximized. These obligations include:

- Aggregating and analyzing reports to assess the effectiveness of security controls; identify tactics, techniques, and procedures adversaries use to overcome these controls; assess potential impact of cyber incidents on public health and safety; and enhance situational awareness of cyber threats across critical infrastructure sectors;[428]
- Coordinating and sharing information with appropriate Federal departments and agencies to identify and track ransom payments;[429]
- Leveraging information gathered about cyber incidents to provide appropriate entities, including Sector Coordinating Councils, Information Sharing and Analysis Organizations, SLTT governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures;[430]
- For significant cyber incidents, reviewing the details surrounding the incident or group of incidents and identifying and disseminating ways to prevent or mitigate similar cyber incidents in the future;[431]
- Publishing quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations;[432]

[428] 6 U.S.C. 681a(a)(1).
[429] 6 U.S.C. 681a(a)(2).
[430] 6 U.S.C. 681a(a)(3)(B).
[431] 6 U.S.C. 681a(a)(6).
[432] 6 U.S.C. 681a(a)(8).

- Proactively identifying opportunities to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations;[433] and
- Making information received in CIRCIA Reports available to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.[434]

By requiring CISA to perform these analytical activities and share information and analytical the findings with Federal and non-Federal stakeholders—an obligation CISA intends to fulfill through a variety of information sharing mechanisms, including through the development, maintenance, and issuance of publicly available alerts, advisories, a known exploited vulnerabilities catalog, and other products that can be leveraged by both covered entities and non-covered entities— CIRCIA will indirectly enhance the nation's overall level of cybersecurity and resiliency, resulting in direct, tangible benefits to the nation. For example:

- By supporting CISA's ability to share information that will enable non-Federal and Federal partners to detect and counter sophisticated cyber campaigns earlier with the potential for significant avoided or mitigated negative impacts to critical infrastructure or national security, CIRCIA's mandatory reporting requirements reduce the risks associated with those campaigns.[435]
- By facilitating the identification and sharing of information on exploited vulnerabilities and measures that can be taken to address those vulnerabilities,

---

[433] 6 U.S.C. 681a(a)(9).
[434] 6 U.S.C. 681a(a)(10).
[435] See, e.g., *Stakeholder Perspectives Hearing*, *supra* note 17, at 17-18 (statement of FireEye Mandiant Vice President Ronald Bushar) ("Timely reporting of incidents within and across sectors allow[s] for earlier detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or National security implications. Technical indicators, along with contextual information, provide a more robust data set to conduct faster and more accurate attribution in adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a time frame that has a high probability of successful countermeasures or deterrence."). See also Mandiant, *Analysis of Time-to-Exploit Trends: 2021-2022* (Sept. 28, 2023), available at https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022.

incident reporting enables entities with unremediated and unmitigated vulnerabilities on their systems to take steps to remedy those vulnerabilities before the entity also falls victim to cyberattack.[436]

- By supporting sharing information about common threat actor tactics, techniques, and procedures with the IT community, cyber incident reporting will enable software developers and vendors to develop more secure products or send out updates to add security to existing products, better protecting end users.[437]
- By enabling rapid identification of ongoing incidents and increased understanding of successful mitigation measures, incident reporting increases the ability of impacted entities and the Federal government to respond to ongoing campaigns faster and mitigate the consequences that could result from them.[438]

---

[436] See, e.g., *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack: Hearing Before the Subcomms. on Cybersecurity, Infrastructure Protection, and Innovation & Transportation and Maritime Security of the H. Comm. on Homeland Security*, 117th Cong. 21 (June 15, 2021) (testimony of CISA Cybersecurity Division Executive Assistant Director Eric Goldstein) ("With increased visibility, we are able to better identify adversary activity across sectors, which allows us to produce more targeted guidance . . . ."), available at https://www.congress.gov/event/117th-congress/joint-event/LC69050/text (hereinafter "*CHS June 15, 2021 Hearing*"); Bitsight Security Research, *A Mere Five Percent of Vulnerable Enterprises Fix Their Issues Every Month: How to Help Them Do Better?* (May 3, 2023), available at https://www.bitsight.com/blog/mere-five-percent-vulnerable-enterprises-fix-their-issues-every-month-how-help-them-do-better (noting that CISA alerts and advisories can increase the likelihood of rapid cybersecurity vulnerability remediation by nearly five times the likelihood of rapid remediation for cybersecurity vulnerabilities for which there is no CISA alert or advisory).

[437] See, e.g., *Open Hearing: Hack of U.S. Networks by a Foreign Adversary Before the S. Select Comm. on Intelligence*, 117th Cong. (Feb. 23, 2021) (written testimony of SolarWinds CEO Sudhakar Ramakrishna) ("Indicators of compromise associated with [cybersecurity] events shared with software vendors in an anonymized way enriches the understanding of prevailing threat actor techniques and target sets, enabling software providers to improve defenses and better protect users."), available at https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

[438] See, e.g., *id.* (written testimony of Microsoft President Brad Smith) ("A private sector disclosure obligation will foster greater visibility, which can in turn strengthen a national coordination strategy with the private sector which can increase responsiveness and agility."); *Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. (Mar. 18, 2021) (opening statement of Sen. Gary Peters, Chairman) ("In order to adapt to the evolving cybersecurity threat, both the public and private sector need a centralized, transparent, and streamlined process for sharing information. In the event of a future attack[], this will be critical to mitigating the damage."), available at https://www.hsgac.senate.gov/hearings/understanding-and-responding-to-the-solarwinds-supply-chain-attack-the-federal-perspective/ (hereinafter "*HSGAC March 18, 2021 Hearing*").

- Law enforcement entities can use the information submitted in reports to investigate, identify, capture, and prosecute perpetrators of cybercrime, getting malicious cyber actors off the street and deterring future actors.[439]
- By contributing to a more accurate and comprehensive understanding of the cyber threat environment, incident reporting allows for CISA's Federal and non-Federal stakeholders to more efficiently and effectively allocate resources to prevent, deter, defend against, respond to, and mitigate significant cyber incidents.[440] Please also see the discussion of market failure associated with the current patchwork system of cyber incident reporting that exists today and why a centralized regulatory system to collect incident reports is needed to correct this failure, in Section 1.2 of the Preliminary RIA.

Even before CIRCIA, one of the core mechanisms through which CISA achieves its cybersecurity mission is producing and widely sharing timely and actionable operational alerts and advisories on known threats, incidents, and vulnerabilities. The broad sharing of timely information enables CISA to make an impact at scale and buy down broad swaths of risk. CISA leverages many information sharing mechanisms and partnership communities to ensure that relevant information is reaching the targeted audience.[441] There are many ways in which CISA ensures that alerts, advisories, analysis,

---

[439] See, e.g., *HSGAC March 18, 2021 Hearing*, *supra* note 438 (statement of FBI Cyber Division Acting Assistant Director Tonya Ugoretz) ("[The SolarWinds attack] highlighted how vital private sector cooperation is to our broader work protecting America from cyber threats. The virtuous cycle we can drive when we work together has been on display in the SolarWinds response: information from the private sector fuels our investigations, allows us to identify evidence and adversary infrastructure, and enables us to hand off leads to intelligence and law enforcement partners here and abroad. Our partners then put that information to work and hand us back more than we started with, which we can then use to arm the private sector to harden itself against the threat. By leaning into our partnerships, all of us who are combating malicious cyber activity become stronger while we weaken the perpetrators together.").

[440] See, e.g., *CHS June 15, 2021 Hearing*, *supra* note 436, at 15 (statement of TSA Assistant Administrator for Surface Operations Sonya Proctor) ("By requiring the reporting of cybersecurity incidents, the Federal Government is better positioned to understand the changing threat of cyber events and the current and evolving risks to pipelines."); *Stakeholder Perspectives Hearing*, *supra* note 17, at 20 (statement of FireEye Mandiant Vice President Ronald Bushar) ("[R]obust and centralized collection of incident information provides the Government with a much more accurate cyber risk picture and enables more effective and efficient investments and support before, during, and after major cyber attacks.").

and specific vulnerability or threat information is widely shared to the broadest appropriate audience, including:

- Working to prioritize stakeholder awareness of actively exploited vulnerabilities through maintenance of a known exploited vulnerability (KEV) catalog which is available on CISA's website. Members of the public can also subscribe to the GovDelivery notification subscription to receive email notifications whenever the KEV catalog is updated.
- Leveraging several communities to ensure broadest appropriate dissemination of guidance to specific communities of interest, such as through Sector Risk Management Agencies, Information Sharing & Analysis Centers (ISACs), and CISA regional personnel to engage state and local governments, critical infrastructure, and other communities directly.
- Depending on the severity of the threat, vulnerability, or threat actor campaign, CISA may reach out directly to potentially impacted entities to try to ensure their awareness and recommended mitigations, if available.
- CISA shares cyber threat indicators, based on information shared with CISA by CISA partners or generated through CISA's own analysis and engagements, via the Automated Indicator Sharing platform.
- Working with other federal and industry partners, as appropriate, who will also disseminate alerts/advisories through their information sharing mechanisms.

Through CIRCIA reporting, CISA would be able to gather more time-sensitive threat and vulnerability data regarding covered cyber incidents or ransomware attacks. This timely collection of specific data elements, fed into CISA's existing robust

---

[441] CISA shares and disseminates information in myriad ways, including via the CISA.gov website and/or the StopRansomware.gov website, various social media platforms, and the GovDelivery email notification subscription. Information is also shared with the Homeland Security Information Network (HSIN), U.S. Cyber Centers, and through direct stakeholder engagement.

communication channels, described above, would allow for sharing of a higher volume of actionable information that is more timely and could be used to reduce risk and mitigate against losses associated with covered cyber incidents and ransom payments. The reporting of covered cyber incidents by impacted entities would provide information that could reduce the number of incidents with consequences through increased awareness of attack vectors and vulnerabilities, leading to more informed covered entities (and non-covered entities) taking preventative or protective measures based on the shared information. This would allow entities to either reduce the losses associated with incidents for which they have been a victim, or for entities to take protective measures prevent an incident altogether. Through early identification and warning of threat actor tactics, cyber incidents, or vulnerabilities, CISA would be able to help entities recognize potential weaknesses and implement protective measures to prevent cyber incidents or limit the consequences of cyber incidents.

By creating a centralized regulatory incident reporting system, CIRCIA can help the Federal government develop a comprehensive understanding of known incidents and ransom payments. Under the current patchwork reporting system, many incidents go unreported, other incidents are reported with limited technical information that results in limited ability to use the reports to help prevent other incidents, and there is no reliable mechanism to ensure that reports are being shared broadly enough across the Federal government or between the Federal government and non-Federal partners to make the reported information actionable to mitigate against negative impacts. A robust, rich, and consolidated incident reporting program, facilitated by the proposed rule, would make the realization of the benefits listed above far more likely, comprehensive, useful, and timely.

These benefits, which stem from the reporting of cyber incidents for aggregation, analysis, and information sharing, directly contribute to a reduction in economic, health, safety, and security consequences associated with cyber incidents by reducing the

likelihood of cyber incidents successfully perpetrated and mitigating the consequences of those cyber incidents that are successful by catching them earlier. For example, incident reporting to CISA within 72 hours and CISA's sharing of that information has a number of benefits associated with rapid vulnerability remediation. For example: (1) vendors that receive earlier warning of previously undisclosed vulnerabilities can begin to develop patches sooner, reducing the likelihood of an incident resulting from their exploitation;, (2) entities that remediate a vulnerability rapidly can reduce the likelihood of a known vulnerability being exploited by reducing the period of time during which their systems are vulnerable to exploitation of that vulnerability; (3) entities that remediate a vulnerability rapidly can reduce the likelihood of the propagation of a threat within their systems, which would reduce the impact of a vulnerability that has already been exploited (i.e., reducing the severity of an incident); and (4) awareness that a vulnerability is being actively exploited by threat actors can help entities effectively prioritize their remediation and patching efforts (as entities often have more patches in the queue than their personnel can realistically remediate in a timely fashion). In an analysis of its proprietary dataset of cyber claims, the Marsh McLennan Cyber Risk Analytics Center compared cyber controls in terms of their effectiveness in reducing the likelihood of an organization experiencing a cyber event. Although patching was identified as one of the most effective controls, tied for fourth, it was found to have one of the lowest implementation rates.[442] However, a recent study suggests that information put out by CISA is meaningfully shaping how entities are implementing this highly effective control. Bitsight Security Research found that CISA alerts and advisories can increase the likelihood of rapid cybersecurity vulnerability remediation by nearly five times the likelihood of rapid

[442] Marsh McLennan, *Using data to prioritize cybersecurity investments* (2023), available at https://www.marsh.com/us/services/cyber-risk/insights/using-cybersecurity-analytics-to-prioritize-cybersecurity-investments.html.

remediation for vulnerabilities for which there is no CISA alert or advisory, outpacing the impact of even sustained social media coverage:

> Further, strategic coverage of vulnerabilities in CISA briefings (Alerts and Current Activity advisories) can accelerate the pace of their remediation, boosting the probability of rapid remediation by around 4.7x. Even greater impacts may be possible, which would be highly desirable. Sustained coverage of vulnerabilities on social media, e.g. Twitter, is associated with boosting their prospects of rapid remediation by roughly 2.7x.[443]

By identifying a vulnerability through CIRCIA reporting, and disseminating that information quickly and broadly, CISA can provide earlier disclosure to vendors of zero-day vulnerabilities and early warning to potentially impacted entities to take preventative or protective measures to remediate known vulnerabilities before they become exploited.[444] CISA requests comment on the potential impact of reporting requirements for preventing or mitigating cybersecurity incidents.

It is worth noting that these benefits are not limited to covered entities required to report under CIRCIA, but also inure to entities not subject to CIRCIA's reporting requirements as they too will receive the downstream benefits of enhanced information sharing, more secure technology products, and an ability to better defend their networks based on sector-specific and cross-sector understandings of the threat landscape.

CISA also anticipates qualitative benefits stemming from the data and record preservation requirements of this proposed rule. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom. Access to forensic data, such as records and logs, can help analysts uncover how malicious cyber activity was conducted, what vulnerabilities were exploited, what tactics were used, and so on. This information can be essential to

---

[443] Bitsight Security Research, *A Mere Five Percent of Vulnerable Enterprises Fix Their Issues Every Month: How to Help Them Do Better?* (May 3, 2023), available at https://www.bitsight.com/blog/mere-five-percent-vulnerable-enterprises-fix-their-issues-every-month-how-help-them-do-better.

[444] See also Mandiant, *Analysis of Time-to-Exploit Trends: 2021-2022* (Sept. 28, 2023), available at https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022.

preventing others from falling victim to similar incidents in the future. How an incident was perpetrated may not be immediately identifiable upon discovery of an incident, and the failure to properly preserve data or records during the period of initial incident response can render it difficult to subsequently perform this analysis. This can especially be true in incidents involving zero-day vulnerabilities or highly complex malicious cyber activity by nation state threat actors, such as the "SUNBURST" malware that compromised legitimate updates of customers using SolarWinds products or the Hafnium campaign on Exchange servers, with the full extent, cause, or attribution of an incident often not being known until months after the initial discovery.[445]

In designing the proposed rule, CISA sought the approach that would provide the best balance between qualitative benefits and the costs associated with implementation of the rule. For instance, in determining the proposed scope of the covered entity population, CISA attempted to balance the need for sufficient reporting necessary to achieve the benefits described in this section with the recognition that the larger the covered entity population, the greater the costs associated with the rule would be.[446] In light of that, as described in Section IV.B, CISA worked closely with its Federal partners to carefully target specific types of entities from each critical infrastructure sector for inclusion after consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) and the entities' ability to manage the reporting requirements. Based on that, CISA is proposing to cover only a small portion of the millions of entities "in a critical infrastructure sector" that could have been included in the description of covered entities.

Another example of where CISA looked to maximize qualitative benefits relative to costs is in the content that a covered entity is required to submit when making a Covered Cyber Incident Report. CISA generally focused on requiring content that was

---

[445] See, e.g., *Evidence Preservation*, *supra* note 370.
[446] See Section III.C.ii for a discussion of why a sufficient number of reports is needed to achieve the purposes of CIRCIA.

either specifically enumerated as required content in the CIRCIA legislation or that CISA believes is necessary for CISA to accomplish an obligation imposed upon CISA by the legislation.

Similarly, as described in Section IV.F, regarding data preservation, CISA felt that there are significant benefits from requiring entities to retain data for an extended period of time. When determining the data preservation timeframe, CISA considered existing best practices regarding preservation of information related to cyber incidents, data retention or preservation requirements from comparable regulatory programs, and comments received on this issue from stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions. Based on the above, CISA believes that a data preservation requirement lasting anywhere between two and three years would be consistent with existing best practices, would be implementable by the regulated community, and would achieve the purposes for which data preservation is intended under CIRCIA. Recognizing that the costs for preserving data increase the longer the data must be retained, and wanting to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the intended purposes, CISA is proposing a length at the lower end of the spectrum of best practices for data preservation. While many regulatory regimes require data to be preserved for three years or more, CISA has elected to propose a two-year reporting period. CISA believes the two-year period would provide the best balance between qualitative benefits and costs by balancing the incremental costs of continued data retention against the benefits of having incident data available for an extended period of time following an incident.

In addition to identifying the qualitative benefits discussed above, CISA considered a break-even analysis. Break-even analysis is useful when it is not possible to quantify the benefits of a regulatory action. OMB Circular A-4 recommends a "threshold" or "break-even" analysis when non-quantified benefits are important to

evaluating the benefits of a regulation. Threshold or break-even analysis answers the question, "How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?"[447] OMB Circular A-4 notes that "It may be useful to focus a break even analysis on whether the action under consideration will change the probability of events occurring or the potential magnitude of those events. For example, there may be instances when you have estimates of the expected outcome of a type of catastrophic event, but assessing the change in the probability of such an event may be difficult. Your break-even analysis could demonstrate how much a regulatory alternative would need to reduce the probability of a catastrophic event occurring in order to yield positive net benefits or change which regulatory alternative is most net beneficial."[448]

In the past, DHS has used a break-even analysis to compare the costs of a proposed rule to the expected impacts of a terrorist attack, or other extremely rare, high consequence event. This analysis would differ for CIRCIA, as this proposed rule would help prevent or mitigate far more common cybersecurity incidents that, as discussed in Section 1.1 of the Preliminary RIA, occur more often, and with an increased frequency since 2018.

Agencies typically use break-even to produce a conditional justification for the proposed rule. While this conditional justification does not resolve whether or not a rule would break-even, or reach net-zero benefits, it serves to highlight what information is missing and what kind of assumptions would be necessary to provide a basis for the proposed rule to break-even.[449] According to Sunstein, break-even analysis helps agencies "…to specify the source of uncertainty, and what they would need to know in

---

[447] OMB, Circular A-4 (Sept. 17, 2003), available at https://obamawhitehouse.archives.gov/omb/circulars_a004_a-4/.
[448] *Id.*
[449] Cass R. Sunstein, "The Limits of Quantification," 102 *California Law Review* 102, no. 6 (2014).

order to reduce it. Conditional justifications have the advantage of transparency, because they specify the factual assumptions that would have to be made for the benefits to justify the costs. That specification is exceedingly important, because it can promote accountability, promote consideration of the plausibility of the underlying assumptions, and promote testing and revisiting over time as new information becomes available."[450]

CISA expects this proposed rule to reduce the risk of loss of critical services or financial losses due to a covered cyber incident in the critical infrastructure sectors. As described above, upon receiving a Covered Cyber Incident Report or Ransom Payment Report, the statute requires CISA to undertake a number of analytical and information-sharing efforts. The development and sharing of actionable information about cyber threats, security vulnerabilities, and defensive measures can help other entities to avoid the costs of a cyber incident in two ways.

First, the information would allow some entities to take actions that prevent the incident from occurring. For example, this could lead to discovery of a zero-day vulnerability earlier in time, resulting in earlier vendor development and customer deployment of a patch; recognition that a previously identified vulnerability is one being actively exploited by threat actors, resulting in its remediation being prioritized;[451] or identification of a new threat actor tactic, technique, or procedure, for which companies can deploy enhanced network or end-point scanning and blocking.

Second, even where an incident is not prevented, the information would allow other entities to mitigate the impacts of the incident (e.g., by reducing the propagation of the incident throughout the organization). Incidents occur in different stages (often referred to as the "lifecycle" of a cyber incident); the earlier in the lifecycle a network defender can identify an incident, the more likely network defenders can negate or

---

[450] *Id.*

[451] CISA, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, https://www.cisa.gov/known-exploited-vulnerabilities (last visited Nov. 28, 2023).

impede the adversary from achieving their goals.[452] This means that earlier detection of incidents minimizes both the impact to systems and data (and the associated damage from that impact) and the cost of containment, remediation, and recovery.

CISA requests comment on the potential use of a break-even analysis in this case, specifically on what the consequences of a substantial cyber incident would be, and the number of substantial cyber incidents expected in a given year. Additionally, CISA requests comment on how effective early notification of cyber incidents would be in mitigating expected consequences of an incident.

When thinking about benefits, CISA considered estimates of the cost of a covered cyber incident from the Information Risk Insights Study (IRIS) 2022 by the Cyentia Institute, which was sponsored by CISA. The Cyentia Institute analyzed Advisen's Cyber Loss Data, which is widely used and presents the most comprehensive list of historical cyber incidents. From the July 2022 Advisen dataset, the Cyentia Institute analyzed the 1,893 cyber events with reported loss data, from the 10-year period ranging from 2012 to 2021. These predominately U.S. events impacted firms across all 20 NAICS sectors at the two-digit level and were assigned to one of eight patterns: Denial of Service Attack, Accidental Disclosure, Scam or Fraud, System Intrusion, Insider Misuse, Physical Threats, Ransomware, and System Failure. Of these eight pattern types, System Intrusion was found to be both the most frequent (49.6% of all types) and to have the highest financial impact (60.2% of the total impact across all types). Table 14 presents summary statistics associated with these 1,893 cyber events.[453]

Table 14: Summary of Cyber Event Losses and Counts, IRIS 2022

Measure	Loss	Number of Events (2012–2021) [a]	Average Annual Number of Events

[452] See, e.g., MITRE, *Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle* (2015), available at http://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf.
[453] Cyentia Institute, *Information Risk Insights Study 2022*, tbl. 3, Loss Summary, available at https://www.cyentia.com/iris-2022/.

Minimum	$32	0	0
First Quartile	$29,000	474	47.4
Geometric Mean	$266,000	479	47.9
Third Quartile	$2,000,000	458	45.8
95th Percentile	$52,000,000	386	38.6
Maximum	$12,000,000,000	96	9.6

Note. Data is based on data from the Cyentia Institute's IRIS 2022 study.

[a] These are the number of events that resulted in losses between the breakpoints of each of the following loss bin: [$0, $32), [$32, $29,000), [$29,000, $266,000), [$266,000, $ 2 million), [$2 million, $52 million), and [$52 million, $12 billion]. Since the minimum value of $32 is the single lowest loss that occurred among the 1,893 events, there are no events associated with it in this column. Instead, there are 474 events which had losses from $32 up to $29,000, 479 events from $29,000 up to $266,000, and so on.

As noted in the Cyentia Institute IRIS 2022 report, the typical cost of a security incident is close to the geometric mean of $266,000, and the average, or arithmetic mean, is over $25 million. Rather than require reporting of any cyber incident, this rule proposes to require reporting only of covered cyber incidents, which means a substantial cyber incident experienced by a covered entity. Under the proposed rule, a substantial cyber incident means a Cyber Incident that leads to any of the following:

1. Substantial loss of confidentiality, integrity, or availability;
2. Serious impact on safety and resiliency of operational systems and processes;
3. Disruption of ability to engage in business or industrial operations, or deliver goods or services; or
4. Unauthorized access facilitated through or caused by a: (1) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider, or (2) supply chain compromise.[454]

Although none of these impacts is defined in terms of event loss, in its report "IRIS 20/20 Xtreme," Cyentia Institute describes losses associated with business interruptions, which are included in the third type of impact for substantial cyber

[454] See § 226.1 of the proposed rule.

events.[455] Cyentia Institute finds that business interruptions are the most numerous event category, with over half of all total losses attributable to business interruption, and have high median losses of $82 million. Because this rule proposes to require incident reporting only for covered cyber incidents, which must by definition be substantial cyber incidents, CISA considered comparing the cost of this proposed rule to the 95th percentile loss value of $52 million, which is closer to the estimate of $82 million and perhaps more representative of what a substantial cyber incident may cost. CISA again welcomes comment on the potential application of these and other estimates.

vi. Accounting Statement

The OMB A-4 Accounting Statement (Table 15) presents annualized costs and qualitative benefits of the proposed rule in 2022 dollars.

Table 15: OMB A-4 Accounting Statement ($ Millions, 2022 dollars)

Category	Estimates			Units			Notes
	Primary Estimate	Low Estimate	High Estimate	Year Dollar	Discount Rate	Period Covered	
Cost Savings							
Quantitative Annualized Monetized ($ millions/year)	N/A	N/A	N/A	N/A	2%	N/A	
Qualitative	Qualitative benefits include (a) improved incident reporting and response and (b) improved cybersecurity posture through improved ability to prevent or mitigate events through information sharing, early warning, threat analysis, and incident response. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of (a) analysts and investigators to understand how a cyber incident was perpetrated and by whom and (b) law enforcement to capture and prosecute perpetrators of cyber incidents and recover ill-gotten proceeds from the criminal activity.						
Costs							
Annualized Monetized ($ millions/year)	$244.6	$225.4	$415.4	2023	2%	10 years	NPRM RIA
Transfers							
From/To	From: N/A			To: N/A			
Other Annualized Monetized ($ millions/year)	N/A	N/A	N/A	N/A	2%	N/A	

[455] Cyentia Institute, *Information Risk Insights Study IRIS 20/20 Xtreme* (2020), tbl. 4, Event Top Level Category, available at https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf.

From/To	From:	N/A		To:	N/A		
Effects							
State, Local, and/or Tribal Government - Annualized Monetized ($ millions/year)	$10.1				2%	10 years	NPRM RIA (Section 11.2.1)
Small Business	Conducted Initial Regulatory Flexibility Analysis (IRFA)						IRFA (Section 9)
Wages	None						
Growth	Not measured						

vii. Alternatives

As part of this analysis, CISA considered alternatives to the proposed rule. Below, CISA presents the four alternatives considered for this rulemaking along with the estimated costs. When comparing alternatives, CISA reviewed the cost of each alternative as well as the objective of the rulemaking effort and the benefits associated with each alternative. While CISA did not estimate quantitative benefits for each alternative, the qualitative benefits for each alternative provide context as to why the NPRM alternative is the preferred choice for CISA.

1. The Preferred Alternative – The NPRM

The analysis for this alternative was discussed above, as it is the proposed alternative. As presented in Section V.A.iv, CISA estimates a combined industry and government cost of $2.6 billion over the period of analysis, and an annualized cost of $244.6 million, discounted at 2%.

CISA selected this alternative as the preferred alternative, as it would provide the best balance between qualitative benefits and costs while being responsive to the statutorily mandated requirements of CIRCIA. While there are potential lower cost alternatives, the scoping of the population of covered entities in the preferred alternative allows CISA to capture adequate reporting populations from not just the sector-based

criteria, but also from entities in multiple critical infrastructure sectors and subsectors using a single threshold.

As discussed above in Section IV.B.iv.1, there are several benefits to including the size-based criterion in the population of covered entities. CISA believes that substantial cyber incidents at larger entities routinely will have a higher likelihood of disrupting the reliable operation of critical infrastructure, making timely knowledge by CISA of any covered cyber incidents affecting larger entities in critical infrastructure sectors essential for potential mitigation of negative consequences. Also, larger entities are more likely to identify early signs of compromise than smaller entities because larger entities also are likely to have more mature cybersecurity capabilities or be better situated to bring in outside experts to assist during an incident.[456] By including large entities in the description of covered entity, the likelihood that an incident is noticed and reported is increased, while the timeframe between initiation of an incident and its reporting is likely to be decreased, making any potential mitigation efforts more effective. CISA also believes that large entities would be better situated to simultaneously report and respond to or mitigate an incident. Because large entities represent a disproportionate percent of the impacts of covered cyber incidents on critical infrastructure, are more likely to be able to identify a cover cyber incident earlier, and respond more quickly while mitigating an incident, CISA believes that the inclusion of the size-based criterion will materially improve the content and volume of reports that CISA receives.

Additionally, the data and record preservation requirements put forth in the preferred alternative are consistent with existing best practices, help ensure the ability to assess and analyze an incident as new information comes to light related to this specific incident or type of incident, support eventual attribution of an incident that may not be known in the immediate aftermath of the incident, and increase the likelihood that

[456] *Verizon 2022 DBIR*, *supra* note 181, at 65.

necessary data and records are preserved long enough to support investigation and prosecution of the threat actors responsible for carrying out the incident. Any reduction in these provisions, while reducing burden, would not justify the sacrifice in benefits. In the following sections for each alternative, CISA more fully explains why each proposed alternative was rejected.

2. Alternative 1 – Reduce the Data and Record Preservation Period

For this alternative, CISA reduces the proposed data and record preservation period from two years to six months. A six-month period would align with existing FBI Letters of Preservation, which allow for an initial 90-day duration, with the option to request preservation for another 90-day period, if needed. Under this alternative, there would be no change to the CIRCIA reporting requirements and therefore, no changes to the costs estimated for becoming familiar with the rule, reporting, help desk, or enforcement of CIRCIA.

Under this alternative, we estimate the costs only for six months of storage, which is the equivalent of multiplying the number of reports per year by $500, without accounting for storage costs after the year the report was submitted.

Table 16 presents the industry cost for Alternative 1 (based on the primary estimates presented in Section V.A.ii), which CISA estimated would be $1.2 billion over the period of analysis and $129.2 million annualized at a 2% discount rate.

Table 16: Alternative 1 Industry Cost, Primary Estimate ($ Millions)

Year	Familiarization Costs	Reporting Costs	Data & Record Preservation Costs	Help Desk Costs	Enforcement Costs	Total	
						Undiscounted	Discounted 2%
2024	$0.0	$0.0	$0.0	$0.00	$0.00	**$0.0**	**$0.0**
2025	$467.0	$0.0	$0.0	$0.00	$0.00	**$467.0**	**$448.9**
2026	$475.1	$9.7	$12.5	$0.44	$0.03	**$497.8**	**$469.1**
2027	$16.2	$9.7	$12.7	$0.44	$0.03	**$39.1**	**$36.1**
2028	$16.2	$9.8	$12.8	$0.44	$0.03	**$39.3**	**$35.6**
2029	$16.2	$9.9	$13.0	$0.45	$0.03	**$39.5**	**$35.1**
2030	$16.2	$9.9	$13.2	$0.45	$0.03	**$39.7**	**$34.6**
2031	$16.2	$10.0	$13.3	$0.46	$0.03	**$40.0**	**$34.1**

2032	$16.2	$10.0	$13.5	$0.46	$0.03	**$40.2**	**$33.6**
2033	$16.2	$10.1	$13.6	$0.46	$0.03	**$40.4**	**$33.2**
Total	**$1,055.5**	**$79.1**	**$104.6**	**$3.59**	**$0.24**	**$1,243.0**	**$1,160.2**
Annualized							***$129.2***

Note. Totals may not sum due to rounding.

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain $1.2 billion, discounted at 2%, over the period of analysis for government costs (see Table 11). The combined costs for industry and government under Alternative 1 are presented in Table 17. CISA estimates a combined 11-yearcost of $2.2 billion and an annualized cost of $226.7 million, discounted at 2%.

Table 17: Alternative 1 Combined Industry and Government Cost, Primary Estimate, ($ Millions)

Year	Industry Cost	Government Cost	Total Cost	
			Undiscounted	Discounted 2%
2023	$0.0	$34.5	$34.5	$34.5
2024	$0.0	$97.7	$97.7	$95.8
2025	$467.0	$115.9	$582.9	$560.3
2026	$497.8	$115.9	$613.7	$578.3
2027	$39.1	$115.9	$155.0	$143.2
2028	$39.3	$115.9	$155.2	$140.6
2029	$39.5	$115.9	$155.4	$138.0
2030	$39.7	$115.9	$155.6	$135.5
2031	$40.0	$115.9	$155.9	$133.0
2032	$40.2	$115.9	$156.1	$130.6
2033	$40.4	$115.9	$156.3	$128.2
Total	**$1,243.0**	**$1,175.3**	**$2,418.3**	**$2,218.0**
Annualized				***$226.6***

Note. Totals may not sum due to rounding.

Alternative 1 represents a cost savings compared to the Preferred Alternative of $176.0 million over the period of analysis, all of which is realized due to the reduction of the data and record preservation period. While Alternative 1 would implement CIRCIA at a lower cost than the Preferred Alternative, CISA rejects this alternative because it would not convey the full benefits associated with the data and record preservation requirements. The data and record preservation requirements can support the ability of

analysts and investigators to understand how a cyber incident was perpetrated and by whom as well as enable data and trend analysis and the investigation of incidents. This could lead to a reduction or mitigation of the risk of future cyber incidents.

The reduction in the data and record preservation requirements would weaken the ability for CISA and other agencies to assess and analyze an incident as new information that may come to light related to this specific incident or type of incident, support eventual attribution of an incident that may not be known in the immediate aftermath of the incident. Reducing the data and records preservation period would also decrease the likelihood that necessary data and records are preserved long enough to support investigation and prosecution of the threat actors responsible for carrying out the incident. Any reduction in these provisions, while reducing burden, would not justify the sacrifice in benefits.

3. Alternative 2 – Remove Size-Based Criterion

For this alternative, CISA would decrease the affected population of covered entities by removing the size-based criterion for covered entities. This change would reduce the population of covered entities by 35,152 (see Section 8.3 of the Preliminary RIA) to 284,607 covered entities, which would be approximately a 12% reduction from the Preferred Alternative. Although this alternative estimates the cost savings for the removal of all 35,152 covered entities identified under the size-based criterion, it is unlikely that the removal of this criterion would result in the removal of all covered entities in the size-based criterion. CISA, however, does not have an estimate for the number of covered entities that would be removed from the affected population of covered entities based on the removal of the size-based standard. As discussed in Section IV.B.iv, CISA recognizes that additional sector-based criteria would be developed in lieu of the size-based standard, however, CISA has not yet developed the thresholds that would be necessary to define these additional criteria. For this alternative, CISA

conducted the analysis using the same methodology as presented in the Preferred Alternative.

Table 18 presents the industry cost for Alternative 2. CISA estimated all costs using the methodology for obtaining the primary estimates presented in Section V.A.ii above and Section 4 of the Preliminary RIA, but based on the reduced population of covered entities. CISA estimated the total cost to industry would be $1.1 billion over the period of analysis and $119.7 million annualized at a 2% discount rate.

Table 18: Alternative 2 Industry Cost, Primary Estimate ($ Millions)

Year	Familiarization	Reporting Costs	Data & Record Preservation Costs	Help Desk Costs	Enforcement Costs	Total	Discounted 2%
2024	$0.0	$0.0	$0.0	$0.0	$0.0	**$0.0**	**$0.0**
2025	$395.3	$0.0	$0.0	$0.0	$0.0	**$395.3**	**$380.0**
2026	$401.0	$7.0	$9.2	$0.3	$0.0	**$417.6**	**$393.5**
2027	$11.5	$7.0	$29.0	$0.3	$0.0	**$47.9**	**$44.2**
2028	$11.5	$7.1	$29.5	$0.3	$0.0	**$48.4**	**$43.9**
2029	$11.5	$7.2	$30.0	$0.3	$0.0	**$49.0**	**$43.5**
2030	$11.5	$7.2	$30.5	$0.3	$0.0	**$49.5**	**$43.1**
2031	$11.5	$7.3	$31.0	$0.3	$0.0	**$50.1**	**$42.8**
2032	$11.5	$7.3	$31.5	$0.3	$0.0	**$50.7**	**$42.4**
2033	$11.5	$7.5	$32.0	$0.3	$0.0	**$51.3**	**$42.1**
Total	**$876.6**	**$50.2**	**$190.6**	**$2.3**	**$0.21**	**$1,159.8**	**$1,075.4**
Annualized							***$119.7***

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain $1.2 billion over the 11-year period of analysis for government costs. CISA assumes no change in government cost due to the relatively small impact associated with the removal of the size-based criterion. Additionally, since government costs are based on expected budget requests, there is a high degree of uncertainty regarding how this change would impact that request. The combined costs for industry and government under Alternative 2 are presented in Table 19. CISA estimates a combined 11-year cost of $2.1 billion and an annualized cost of $218.0 million, discounted at 2%.

Table 19: Alternative 2 Combined Industry and Government Cost, Primary Estimate ($ Millions)

Year	Industry Cost	Government Cost	Total Cost	
			Undiscounted	Discounted 2%
2023	$0.0	$34.5	$34.5	$34.5
2024	$0.0	$97.7	$97.7	$95.8
2025	$395.3	$115.9	$511.2	$491.4
2026	$417.6	$115.9	$533.5	$502.7
2027	$47.9	$115.9	$163.8	$151.3
2028	$48.4	$115.9	$164.3	$148.8
2029	$49.0	$115.9	$164.9	$146.4
2030	$49.5	$115.9	$165.4	$144.0
2031	$50.1	$115.9	$166.0	$141.7
2032	$50.7	$115.9	$166.6	$139.4
2033	$51.3	$115.9	$167.2	$137.2
Total	**$1,159.8**	**$1,175.3**	**$2,335.1**	**$2,133.1**
Annualized				***$218.0***

While Alternative 2 would present a lower cost than the Preferred Alternative, there are several reasons why it was rejected in favor of the Preferred Alternative. As discussed in Section IV.B, there are a wide variety of types of entities that are active participants in critical infrastructure sectors and communities and are considered "in a critical infrastructure sector." Rather than develop sector-based criteria for each of these potential categories of covered entities, CISA relies on the size-based criterion to capture entities in these sectors and subsectors that are not otherwise covered in the sector-based criteria and for which CISA considered that requiring reporting only from large entities was sufficient to meet CIRCIA's purposes. Including these entities is critical for the following reasons, as described in further detail in section IV.B.iv.1:

- While size is not alone indicative of criticality, larger entities' larger customer bases, market shares, number of employees, and other similar size-based characteristics mean that cyber incidents affecting them typically have greater potential to result in consequences impacting national security, economic

security, or public health and safety than cyber incidents affecting smaller companies.

- Large entities disproportionately experience cyber incidents.
- Non-small entities are likely to own or operate a disproportionate percentage of the nation's critical infrastructure.
- In light of the interconnectedness of the world today, incidents at entities in critical infrastructure sectors that are not themselves owners and operators of critical infrastructure can have cascading effects that end up impacting critical infrastructure. Based on this, CISA believes that substantial cyber incidents at larger entities routinely will have a high likelihood of disrupting the reliable operation of critical infrastructure.

Removing the size-based criterion would limit CISA's ability to collect valuable information from a broader set of entities than relying on the sector-based criteria would allow. Furthermore, removing the size-based criterion would require CISA to develop additional sector-based criteria to capture entities from certain critical sectors or subsectors, such as Food and Agriculture Sector entities, Commercial Facilities, Oil and Natural Gas Subsector entities, and medical laboratories that currently are included in the description of covered entity primarily or solely based on the size-based criterion. Covering these additional entities is much more in line with the purpose of the regulation for CISA to learn about new or novel vulnerabilities, trends, or tactics sooner and be able to share early warnings before additional entities within the sector, critical or non-critical, can fall victim to them.

Contrary to the minimum benefits (in terms of industry cost savings) likely to be gained by elimination of the size-based criterion, CISA believes there are significant reasons to include the criterion in the proposal. First, as described at length in Section IV.B.iv.1, there are a number of reasons why CISA believes requiring reporting from

large entities is beneficial. This includes the belief that substantial cyber incidents at larger entities routinely will have a high likelihood of disrupting the reliable operation of critical infrastructure, making timely knowledge by CISA of any covered cyber incidents affecting larger entities in critical infrastructure sectors essential for potential mitigation of negative consequences; larger entities are more likely to identify early signs of compromise than smaller entities; large entities would be better situated to simultaneously report and respond to or mitigate an incident; and the inclusion of the size-based criterion will materially improve the content and volume of reports that CISA receives. Second, the size-based criterion allows CISA to capture adequate reporting from multiple sectors and subsectors using a single threshold. As noted above, without the size-based criterion, CISA likely would need to establish one or more new sector-based criteria for each of at least five critical infrastructure sectors or subsectors, and has included alternative proposed sector-based criteria in the proposed rulemaking for this purpose. In total, while CISA believes it could achieve the purposes of the CIRCIA statute without a size-based criterion, CISA believes that the benefits of including the size-based criterion far exceed the almost certainly minimal cost savings associated with an alternative where additional sector-based criteria are used in lieu of the size-based criterion.

4. Alternative 3 – Reduce the Data and Record Preservation Requirement and Remove Size-Based Criterion

For this alternative, CISA would combine the cost reductions presented in Alternative 1 and Alternative 2 to present the lowest cost alternative.

Table 20 presents the industry cost for Alternative 3. CISA estimated all costs, with the exception of the data and record preservation costs, using the methodology for obtaining the primary estimates presented in Section V.A.ii. CISA estimated the data and records preservation costs using the same methodology used under Alternative 1 as

presented in Section V.A.vii.a. CISA estimated the total cost to industry would be $950.0 million over the period of analysis and $105.7 million annualized at a 2% discount rate.

Table 20: Alternative 3 Industry Cost, Primary Estimate ($ Millions)

Year	Familiarization Costs	Reporting Costs	Data & Record Preservation Costs	Help Desk Costs	Enforcement Costs	Total	
						Undiscounted	Discounted 2%
2024	$0.0	$0.0	$0.0	$0.0	$0.00	**$0.0**	**$0.0**
2025	$395.3	$0.0	$0.0	$0.0	$0.00	**$395.3**	**$380.0**
2026	$401.0	$7.0	$9.2	$0.3	$0.03	**$417.6**	**$393.5**
2027	$11.5	$7.0	$9.4	$0.3	$0.03	**$28.3**	**$26.1**
2028	$11.5	$7.1	$9.6	$0.3	$0.03	**$28.5**	**$25.8**
2029	$11.5	$7.2	$9.7	$0.3	$0.03	**$28.7**	**$25.5**
2030	$11.5	$7.2	$9.9	$0.3	$0.03	**$28.9**	**$25.2**
2031	$11.5	$7.3	$10.0	$0.3	$0.03	**$29.2**	**$24.9**
2032	$11.5	$7.3	$10.2	$0.3	$0.03	**$29.4**	**$24.6**
2033	$11.5	$7.5	$10.4	$0.3	$0.03	**$29.7**	**$24.4**
Total	**$876.6**	**$57.7**	**$78.4**	**$2.7**	**$0.24**	**$1,015.5**	**$949.9**
Annualized							***$105.7***

Note. Totals may not sum due to rounding.

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain $1.2 billion over the 11-year period of analysis for government costs. The combined costs for industry and government under Alternative 3 are presented in Table 21. CISA estimates a 11-year cost of $2.0 billion and an annualized cost of $205.1 million, discounted at 2%.

Table 21: Alternative 3 Combined Industry and Government Cost, Primary Estimate ($ Millions)

Year	Industry Cost	Government Cost	Total Cost	
			Undiscounted	Discounted 2%
2023	$0.0	$34.5	$34.5	$34.5
2024	$0.0	$97.7	$97.7	$95.8
2025	$395.3	$115.9	$511.2	$491.4
2026	$417.6	$115.9	$533.5	$502.7
2027	$28.3	$115.9	$144.2	$133.2
2028	$28.5	$115.9	$144.4	$130.8
2029	$28.7	$115.9	$144.6	$128.4
2030	$28.9	$115.9	$144.8	$126.1
2031	$29.2	$115.9	$145.1	$123.8
2032	$29.4	$115.9	$145.3	$121.6

2033	$29.7	$115.9	$145.6	$119.4
Total	**$1,015.5**	**$1,175.3**	**$2,190.8**	**$2,007.6**
Annualized				***$205.1***

Note. Totals may not sum due to rounding.

Alternative 3 estimates the lowest cost alternative in this analysis, which presents a lower burden based on changes to discretionary elements in two required provisions – a reduction in the data and records preservation requirements and a reduction in the number of covered entities through the removal of the size-based criterion. As discussed in Sections V.A.vii.b and c, the reduction in the data preservation period and the removal of the size-based criterion, while reducing costs, would sacrifice benefits as compared to Preferred Alternative.

5. Alternative 4 – Increase the Affected Population to All Critical Infrastructure Entities

For this alternative, CISA widened the description of covered entity to include all entities operating in the 16 critical infrastructure sectors.[457] Under this alternative, the affected population would increase from 316,244 covered entities to 13,180,483 covered entities. This population was estimated by using the manner of determining whether an entity is in a critical infrastructure sector as explained in Section IV.B.ii. As discussed above, the SSPs for each critical infrastructure sector include a sector profile of entities in the sector.[458] The number of covered entities within each sector, was based on information in the SSPs, as well as populations based on NAICS codes for the affected industries, which was estimated using U.S. Census County Business Patterns data. Table 22 presents the affected population for each of the 16 critical infrastructure sectors. This

[457] The 16 critical infrastructure sectors listed by Presidential Policy Directive 21. See https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/ (last visited Nov. 28, 2023).

[458] The list of 16 Critical Infrastructure Sectors can be found at https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Nov. 28, 2023).

affected population would include small and not small businesses, based on SBA size standards, within the 16 critical infrastructure sectors.

Table 22: Affected Population by Critical Infrastructure Sector

Criteria	Affected Population	Percentage of Affected Population		
		2%	5%	10%
Chemical Sector	31,717	634	1,586	3,172
Commercial Facilities Sector	7,980,640	159,613	399,032	798,064
Communications Sector	92,861	1,857	4,643	9,286
Critical Manufacturing Sector	46,259	925	2,313	4,626
Dams Sector	107,054	2,141	5,353	10,705
Defense Industrial Base Sector	60,000	1,200	3,000	6,000
Emergency Services	118,098	2,362	5,905	11,810
Energy Sector	36,069	721	1,803	3,607
Financial Services Sector	294,794	5,896	14,740	29,479
Food and Agriculture Sector	3,239,083	64,782	161,954	323,908
Government Facilities Sector	89,626	1,793	4,481	8,963
Healthcare and Public Health Sector	142,806	2,856	7,140	14,281
Information Technology Sector	557,000	11,140	27,850	55,700
Nuclear Reactors, Materials, and Waste Sector	143	3	7	14
Transportation Systems Sector	214,833	4,297	10,742	21,483
Water and Wastewater Sector	169,500	3,390	8,475	16,950
Total	**13,180,483**	**263,610**	**659,024**	**1,318,048**

Using all of the same assumptions for the primary estimates presented in Sections V.A.i and ii, this would increase the number of expected CIRCIA Reports from 210,525

to 5,292,818 over the period of analysis. This would significantly increase the cost to industry, which is estimated to be $31.8 billion over the period of analysis, or $3.5 billion annualized, discounted at 2%, as presented in Table 23.

Table 23: Alternative 4 Industry Cost, Primary Estimate ($ Millions)

Year	Familiarization Costs	Reporting Costs	Data & Record Preservation Costs	Help Desk Costs	Enforcement Costs	Total Cost	
						Undiscounted	Discounted 2%
2024	$0.0	$0.0	$0.0	$0.0	$0.00	**$0.0**	**$0.0**
2025	$10,461.9	$0.0	$0.0	$0.0	$0.00	**$10,461.9**	**$10,055.7**
2026	$10,799.4	$384.3	$235.6	$11.3	$0.03	**$11,430.6**	**$10,771.3**
2027	$675.0	$384.4	$732.8	$11.3	$0.03	**$1,803.5**	**$1,666.1**
2028	$675.0	$384.4	$733.3	$11.3	$0.03	**$1,804.0**	**$1,634.0**
2029	$675.0	$384.5	$733.8	$11.3	$0.03	**$1,804.6**	**$1,602.4**
2030	$675.0	$384.5	$734.3	$11.3	$0.03	**$1,805.1**	**$1,571.5**
2031	$675.0	$384.6	$734.8	$11.3	$0.03	**$1,805.7**	**$1,541.1**
2032	$675.0	$384.7	$735.3	$11.3	$0.03	**$1,806.3**	**$1,511.4**
2033	$675.0	$384.8	$735.8	$11.3	$0.03	**$1,806.9**	**$1,482.3**
Total	**$25,986.1**	**$3,076.2**	**$5,375.8**	**$90.3**	**$0.24**	**$34,528.6**	**$31,835.8**
Annualized							***$3,544.2***

Note. Totals may not sum due to rounding.

In addition to increased industry cost, CISA assumes that the substantial increase in volume of CIRCIA Reports submitted would lead to increased Federal government costs necessary to manage a much larger CIRCIA program. For the purposes of this alternatives analysis, CISA assumes a 10X (900%) increase in government cost in response to the 4,967% increase in the affected population. As presented in Table 24, CISA estimates a combined 11-year cost of $42.1 billion, with an annualized cost of $4.3 billion, discounted at 2%, for Alternative 4.

Table 24: Alternative 4 Combined Industry and Government Costs, Primary Estimate ($ Millions)

Year	Industry Cost	Government Cost	Total Cost	
			Undiscounted	Discounted 2%
2023	$0.0	$34.5	$34.5	$34.5
2024	$0.0	$977.0	$977.0	$957.8
2025	$10,461.9	$1,159.0	$11,620.9	$11,169.7
2026	$11,430.6	$1,159.0	$12,589.6	$11,863.5
2027	$1,803.5	$1,159.0	$2,962.5	$2,736.8
2028	$1,804.0	$1,159.0	$2,963.0	$2,683.7

2029	$1,804.6	$1,159.0	$2,963.6	$2,631.6
2030	$1,805.1	$1,159.0	$2,964.1	$2,580.5
2031	$1,805.7	$1,159.0	$2,964.7	$2,530.3
2032	$1,806.3	$1,159.0	$2,965.3	$2,481.2
2033	$1,806.9	$1,159.0	$2,965.9	$2,433.1
Total	**$34,528.6**	**$11,442.5**	**$45,971.1**	**$42,102.7**
Annualized				***$4,302.0***

Note. Totals may not sum due to rounding.

While Alternative 4 would capture a significantly larger affected population, and therefore provide CISA with additional data to use in its efforts to prevent, or mitigate the impact of, covered cyber incidents, this alternative is rejected due to its high cost. CISA would not anticipate additional benefits comparable to the cost increase from expanding the population, as the Preferred Alternative focuses the affected population on the highest-risk population within the critical infrastructure sectors and is expected to provide sufficient reporting for CISA to identify cyber incident threats and trends.

6. Alternative Comparison

In this analysis, CISA considered four regulatory alternatives to the Preferred Alternative. Table 25 presents the cost comparison for the Preferred Alternative and the four additional alternatives discussed.

Table 25: Alternatives Summary, Combined Industry and Government Cost, Primary Estimate ($ Millions)

Alternative	Description	11-Year Cost		Annualized Cost
		Undiscounted	Discounted 2%	Discounted 2%
Preferred	Proposed Rulemaking	$2,619.8	$2,394.0	$244.6
1	Reduces the data and record preservation period	$2,418.3	$2,218.0	$226.6

2	Remove Size Based Criterion for Covered Entities[459]	$2,335.1	$2,133.1	$218.0
3	Reduces the data and record preservation period and removes the size-based criterion	$2,190.8	$2,007.6	$205.1
4	Increases the affected population to all critical infrastructure entities	$45,971.1	$42,102.7	$4,302.0

B. Small Entities

The Regulatory Flexibility Act (RFA), 5 U.S.C. 603, requires agencies to consider the impacts of its rules on small entities. In accordance with the RFA, CISA has prepared an initial regulatory flexibility analysis (IRFA) that examines the impacts of the proposed rule on small entities. The IRFA is included in the Preliminary RIA that is available in the docket for this rulemaking. The term "small entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of fewer than 50,000.

CISA is publishing the IRFA in the rulemaking docket to aid the public in commenting on the potential small entity impacts of the requirements in this proposed rule. CISA invites all interested parties to submit data and information regarding the potential economic impact on small entities that would result from the adoption of the proposed requirements in this proposed rule. Under section 603(b) and (c) of the RFA, an

[459] In this proposed rule, CISA proposes several criteria in § 226.2 to describe entities that would be considered covered entities, and one criterion would include entities that exceed the SBA small business size standard. Alternatives 2 and 3 would remove that as a criterion for determining covered entities.

IRFA must describe the impact of the proposed rule on small entities and contain the following:

- A description of the reasons why action by the agency is being considered.
- A succinct statement of the objectives of, and legal basis for, the proposed rule.
- A description of and, where feasible, an estimate of the number of small entities to which the proposed rule would apply.
- A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities which would be subject to the requirements and the type of professional skills necessary for preparation of the report or record.
- An identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with the proposed rule.
- A description of any significant alternatives to the proposed rule that accomplish the stated objectives of applicable statutes and may minimize any significant economic impact of the proposed rule on small entities.

CISA has discussed many of these issues in other sections of the preamble to the NPRM and in the Preliminary RIA, which is published in the rulemaking docket. CISA welcomes comment from the public on the Preliminary RIA.

An estimated 316,244 covered entities would be subject to requirements proposed in this NPRM and potentially incur costs as a result of this proposed rule. These covered entities include businesses, government entities, and organizations—some of which are considered to be small entities as defined by the RFA.

CISA does not have a complete list of the entities that would be subject to the requirements of this proposed rule. Therefore, as discussed in Section 9.4 of the Preliminary RIA, CISA conducted an analysis to review the NAICS codes that would most likely have entities affected by the proposed rule. Using the SBA size standards,

CISA estimated the number of small entities within each of the 280 relevant NAICS codes. CISA then performed an IRFA to assess the impacts on small entities resulting from this proposed rule using the estimated cost per covered entity.

Based on the IRFA, CISA found:

- Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities.
- Of the 264 NAICS codes with available revenue data, 99.2% had a revenue impact of less than or equal to 1%.
- CISA estimated that the average cost per non-covered entity would be $33.58 and the average cost per covered entity experiencing a single covered cyber incident would be $4,139.60.

CISA has discussed many of these issues in other sections of the NPRM and in the Preliminary RIA, which is published in the rulemaking docket. CISA welcomes comment from the public on the Preliminary RIA and the IRFA.

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104-121), CISA wants to assist small entities in understanding this proposed rule so that they can better evaluate its effects on them and participate in the rulemaking. If this proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please contact the person in the FOR FURTHER INFORMATION CONTACT section of this NPRM. CISA will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the CISA.

D. Collection of Information

Under the Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. 3501-3520, agencies are required to submit to OMB, for review and approval, any reporting

requirements inherent in a rule. This proposed rule would call for a new collection of information under PRA. CIRCIA also includes a broad exemption to PRA, which provides that: "Sections 3506(c), 3507, 3508, and 3509 of title 44 shall not apply to any action to carry out this section." 6 U.S.C. 681b(f). CISA interprets the phrase "this section" as referring to 6 U.S.C. 681b for the purposes of the PRA exemption. Therefore, CISA understands the scope of this PRA exemption as applying to all information collection related to CIRCIA's reporting requirements under 6 U.S.C. 681b(a)(1)-(3) as wholly exempt from compliance with the PRA, regardless of whether that information must be required under this proposed rule or is voluntarily provided in response to an optional question in a CIRCIA Report.

covered entities will also have the opportunity to submit additional data and information to enhance situational awareness of cyber threats, as authorized under 6 U.S.C. 681c(b), via an open text box and/or the ability to upload information as part of a covered entity's CIRCIA Report. Because CISA does not plan to require covered entities to submit this data and information, nor will it pose identical questions that must be responded to in any particular form or time period to covered entities, this additional information does not constitute a "collection of information" under the Paperwork Reduction Act. See 5 CFR 1320.3(c).

Accordingly, information collected through CIRCIA Reports, including additional information collected in an ad hoc manner that is incorporated into CIRCIA Reports, is exempt from compliance with PRA requirements. Information collected by CISA entirely pursuant to 6 U.S.C. 681c is outside of the scope of this rulemaking and not exempt from compliance with PRA requirements.

E. Federalism

Under Executive Order 13132, Federalism, 64 FR 43255 (Aug. 10, 1999), agencies must adhere to fundamental federalism principles, policymaking criteria, and in

some cases follow additional requirements when promulgating federal regulations. While it is possible that the regulations proposed through this notice may have some impact on SLTT governments, CISA believes that this rule would not trigger the additional requirements contained in Executive Order 13132 for rules that have federalism impacts.

Depending on the type of rule under development, Executive Order 13132 may require an agency to: 1) provide the State and local government with funds to pay for the direct costs they incur in complying with the regulation; 2) consult with State and local officials early in the process of developing the proposed regulation; 3) provide a federalism summary impact statement in the preamble of the rule; and/or 4) provide the Director of OMB with written communications submitted to the agency by State and local officials. Under Section 6 of the Executive Order, agencies must meet these additional requirements for two categories of rules. Section 6(b) describes the first category as rules that have federalism implications, impose substantial direct compliance costs on State and local governments, and that are not required by statute. Because the regulations proposed through this notice are required by statute, this proposed rule is not the sort of action contemplated by Section 6(b). The second category, described in Section 6(c) is a rule that would have federalism implications and that would preempt state law. While the regulations proposed through this notice may have some impact on SLTT governments, the rule would not have federalism implications as defined in Executive Order 13132, nor would the majority of this rule preempt state law.

A rule has implications for federalism under Executive Order 13132 if it has a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. While this proposed rule describes covered entity to include State and local government entities and entities like emergency service or education providers that may be considered part of a State, the requirement to file a

CIRCIA Report is not a substantial direct effect under Executive Order 13132. Congress explicitly prohibited CISA from pursuing enforcement against a State or local government for failure to report a covered cyber incident or ransom payment as otherwise required under the statute's implementing regulations. See 6 U.S.C. 681d(f). Thus, even though these proposed regulations require some State and local governments and government entities to report covered cyber incidents and ransom payments to CISA, this requirement is unenforceable. CISA believes that an unenforceable requirement to submit an informational report to a federal agency is not the type of government action that results in a substantial direct effect on States, the relationship between the States and the national government, or the distribution of power or responsibilities among the various levels of government. Accordingly, CISA believes that this proposed rule would not have sufficient federalism implications that require under Executive Order 13132 preparation of a federalism summary impact statement, nor require further consultation with State and local government officials.

Similarly, the majority of this rule would not preempt State and/or local government law. Congress did not include any express preemption provision in the CIRCIA statute, and CISA does not assert through this rulemaking that the Federal government so fully occupies the field of cyber incident reporting that States or local governments cannot also regulate in this space. To CISA's knowledge, no State or local laws directly conflict with the incident reporting requirements set forth by this regulation, but CISA welcomes comment from stakeholders explaining otherwise.

One exception to this general lack of preemption is the set of statutory provisions included in CIRCIA, replicated in the proposed rulemaking for clarity in § 226.18(a)(5)(A) and (b)(2), that places limits on a State and/or local government's ability to use information obtained solely through a CIRCIA Report, and disclose the CIRCIA Reports themselves. Similar to the restriction placed on federal regulatory use of

information obtained through reporting to CISA under CIRCIA, CIRCIA prohibits SLTT governments from using information about a covered cyber incident or ransom payment obtained solely through reporting directly to CISA under CIRCIA to regulate the activities of the covered entity or entity that made the ransom payment, unless the SLTT expressly permitted the entity to submit a CIRCIA Report to comply with its SLTT reporting obligations. See 6 U.S.C. 681e(a)(5).[460] Similarly, in addition to exemption from disclosure under the Federal FOIA, CIRCIA also exempts CIRCIA Reports from disclosure under SLTT freedom of information laws or similar laws requiring disclosure of information or records. See U.S.C. 681e(b)(3). CISA believes, however, that incorporation of these provisions into the proposed rule does not result in a rule that implicates federalism as contemplated under Executive Order 13132 for several reasons. First, these two information protection provisions, are a small, supportive aspect of the CIRCIA regulations and will only actually be implicated if and when SLTT governments receive CIRCIA Reports, or information included therein. Unless the SLTT government is in possession of a CIRCIA Report or information obtained solely through a CIRCIA Report after it has been submitted to CISA, these restrictions do not apply. Further, regarding the regulatory use restrictions, SLTT governments are not prohibited from taking regulatory actions based on information they receive from another source, even if that very same information was submitted to CISA as part of a CIRCIA Report. Congress prohibited from using the information obtained *solely* through a CIRCIA Report for such regulatory purposes, unless the submission of a CIRCIA Report is expressly permitted to meet SLTT reporting requirements. In other words, the rule would only place limits on SLTT governments' use and disclosure of information that they would not have otherwise obtained (and therefore, as a practical matter, would not have had in their

[460] A CIRCIA Report may, consistent with State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems. 6 U.S.C. 681e(a)(5)(B).

possession to use or disclose) but for the rule itself. Second, these provisions are expected to inure to the benefit of SLTT governments by making it possible for CIRCIA Reports and/or information contained in those reports that is provided to the Federal government to be shared with the States, which CISA would not otherwise be able to do without risking the important confidentiality and other stakeholder protections required by CIRCIA. This ultimately means that SLTT governments will have more information (e.g., to protect their own information systems) than they would have had without the rule. Accordingly, CISA does not believe that this rule contains federalism implications and preempts state law in the manner that would trigger additional steps required for certain regulatory actions under Executive Order 13121.

Although CISA believes that Executive Order 13132 does not require adherence to the additional steps otherwise necessary for rules that have federalism implications and which preempt state law, CISA notes that representatives from several State and local government entities were consulted early in the development of this proposed rule. CISA hosted several listening sessions between September and November 2022 to obtain input from those entities who may be impacted by the proposed regulations once they have been finalized. Representatives from various State and local government entities were invited to and attended these listening sessions. In some cases, representatives from State and local entities provided input on the proposed regulations during the listening session, for example, during the Emergency Services Sector and Government Facilities Sector sector-specific listening sessions. Transcripts of those listening sessions are available in the docket for this rulemaking.

CISA welcomes public comments on Executive Order 13132 federalism implications.

F. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 or UMRA, 2 U.S.C. 1531-1538, directs Federal agencies to assess the effects of regulatory actions on State, local, and tribal governments, and the private sector. UMRA's requirements apply when any Federal mandate may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100,000,000 (which is now $177,000,000 when adjusted for inflation) or more in any one year. [461] This proposed rule does not impose an unfunded Federal mandate on State, local, or tribal governments because the proposed reporting requirements are unenforceable against SLTT Government Entities.[462] Although this proposed rulemaking would not impose an unfunded mandate on State, local, or tribal governments, the estimates for years 2 and 3 show an unfunded mandate in excess of $177 million on the private sector primarily due to the estimated familiarization costs with the final rule. The regulatory impact assessment prepared in conjunction with this proposed rule satisfies UMRA's requirements under 2 U.S.C. 1532.

G. Taking of Private Property

This proposed rule would not cause a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights, 53 FR 8863 (Mar. 18, 1988).

H. Civil Justice Reform

---

[461] $100 million in 1995 dollars adjusted for inflation to 2022 using the GDP implicit price deflator for the U.S. economy. Federal Reserve Bank of St. Louis, "GDP Implicit Price Deflator in United States," available at https://fred.stlouisfed.org/series/USAGDPDEFAISMEI#0, last accessed on July 21, 2023.

[462] See Memorandum for the Heads of Executive Departments and Agencies, *Guidance for Implementing Title II of S. 1*, from Alice Rivlin, OMB Director (Mar. 31, 1995) ("As a general matter, a Federal mandate includes Federal regulations that impose enforceable duties on State, local, and tribal governments, or on the private sector . . . ."), available at https://obamawhitehouse.archives.gov/omb/memoranda_1998 (last accessed Oct. 13, 2023). See also 5 U.S.C. 1555 which defines a federal mandate as "…any provision in statute or regulation or any Federal court ruling that imposes *an enforceable duty* upon State, local, or tribal governments…" (emphasis added).

This proposed rule meets the applicable standards set forth in section 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, 61 FR 4729 (Feb. 5, 1996) to minimize litigation, eliminate ambiguity, and reduce burden.

I. Protection of Children

This proposed rule, while "economically significant" under Executive Order 12866 as amended by Executive Order 14094, does not concern an environmental health risk or safety risk that an agency has reason to believe may disproportionately affect children. Accordingly, no further analysis is needed under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks, 62 FR 19885 (Apr. 21, 1997).

J. Indian Tribal Governments

This rule does not have "tribal implications" under Executive Order 13175, Consultation and Coordination With Indian Tribal Governments, 65 FR 67249 (Nov. 6, 2000), because it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal government and Indian tribes, or on the distribution of power and responsibilities between the Federal government and Indian tribes. As with State and local governments, this proposed rule describes "covered entity," to include tribal government entities and entities like emergency service providers that may be considered part of a tribal government. The requirement to file a CIRCIA Report, however, is not a substantial direct effect under Executive Order 13175. Further, Congress explicitly prohibited CISA from pursuing enforcement against a tribal government for failure to report a covered cyber incident or ransom payment as otherwise required under the statute's implementing regulations. See 6 U.S.C. 681d(f). Accordingly, CISA believes that this rule does not have tribal implications, and therefore Executive Order 13175 requires no further agency action or analysis. CISA welcomes public comments on Executive Order 13175 tribal implications.

K. Energy Effects

CISA has analyzed this proposed rule under Executive Order 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use, 66 FR 28355 (May 18, 2001). CISA has determined that it is not a "significant energy action" under that order because even though it is a "significant regulatory action" under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy, and it has not been designated by the Administrator of the Office of Information and Regulatory Affairs as a "significant energy action." Accordingly, the provisions of Executive Order 13211 to not apply to this proposed rule.

L. Technical Standards

The National Technology Transfer and Advancement Act, codified as a note to 15 U.S.C. 272, directs agencies to use voluntary consensus standards in their regulatory activities unless the agency provides Congress, through OMB, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (e.g., specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies. This proposed rule does not use technical standards. Therefore, CISA did not consider the use of voluntary consensus standards.

M. National Environmental Policy Act

Section 102 of the National Environmental Policy Act of 1969 (NEPA), 42 U.S.C. 4321 *et seq*., requires Federal agencies to evaluate the impact of any proposed major Federal action significantly affecting the human environment, consider alternatives to the proposed action, provide public notice and opportunity for comment, and properly document its analysis. See 40 CFR parts 1501, 1502, 1506.6. DHS and its component

agencies analyze proposed actions to determine whether NEPA applies and, if so, what level of analysis and documentation is required. See 40 CFR 1501.3.

DHS Directive 023-01 Rev. 01 (Directive) and Instruction Manual 023-01-001-01 Rev. 01 (Instruction Manual) together establish the policies and procedures DHS and its component agencies use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations for implementing the procedural requirements of NEPA, codified at 40 CFR parts 1500 through 1508.

The CEQ regulations allow Federal agencies to establish in their NEPA implementing procedures, with CEQ review and concurrence, categories of actions ("categorical exclusions") that experience has shown do not, individually or cumulatively, have a significant effect on the human environment and, therefore, do not require preparation of an Environmental Assessment or Environmental Impact Statement. 40 CFR 1507.3(e)(2)(ii), 1501.4. Appendix A of the Instruction Manual lists the DHS categorical exclusions. Under DHS NEPA implementing procedures, for a proposed action to be categorically excluded it must satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect. Instruction Manual section V.B(2)(a)-(c).

This proposed rule implements the authority in CIRCIA to develop and codify requirements for covered entities to report covered cyber incidents, ransom payments, and substantial new or different information from what was previously reported regarding such cyber incidents and ransom payments. The proposed rules will be codified at 6 CFR §§ 226.1 through 226.20.

DHS has determined that this proposed rule will have no significant effect on the human environment and clearly fits within categorical exclusion A3 in Appendix A of the

Instruction Manual established for promulgation of rules of a strictly administrative or procedural nature and that implement statutory requirements without substantive change.

This proposed rule is not part of a larger action and presents no extraordinary circumstances creating the potential for significant environmental effects. Therefore, this proposed rule is categorically excluded from further NEPA review.

VI. Proposed Regulation

List of Subjects in 6 CFR Part 226

Computer Technology, Critical Infrastructure, Cybersecurity, Internet, Reporting and Recordkeeping Requirements.

For the reasons stated in the preamble, and under the authority of 6 U.S.C. 681 through 681e and 6 U.S.C. 681g, the Department of Homeland Security proposes to add chapter II, consisting of part 226 to title 6 of the Code of Regulations to read as follows:

CHAPTER II--DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

PART 226—COVERED CYBER INCIDENT AND RANSOM PAYMENT REPORTING

Sec.

AUTHORITY: 6 U.S.C. 681 – 681e, 6 U.S.C. 681g; Sections 2240-2244 and 2246 of the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135, as amended by Pub. L. 117-103 and Pub. L. 117-263 (Dec. 23, 2022).

§ 226.1 Definitions.

For the purposes of this part:

CIRCIA means the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended, in 6 U.S.C. 681 – 681g.

CIRCIA Agreement means an agreement between CISA and another Federal agency that meets the requirements of § 226.4(a)(2), has not expired or been terminated, and, when publicly posted by CISA in accordance with § 226.4(a)(5), indicates the availability of a substantially similar reporting exception for use by a covered entity.

CIRCIA Report means a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report, as defined under this part.

Cloud service provider means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in Nat'l Inst. of Standards & Tech., NIST Special Publication 800-145, and any amendatory or superseding document relating thereto.

Covered cyber incident means a substantial cyber incident experienced by a covered entity.

Covered Cyber Incident Report means a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident as required by this part. A Covered Cyber Incident Report also includes any responses to optional questions and additional information voluntarily submitted as part of a Covered Cyber Incident Report.

Covered entity means an entity that meets the criteria set forth in § 226.2 of this part.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or actually jeopardizes, without lawful authority, an information system.

Cybersecurity and Infrastructure Security Agency or CISA means the Cybersecurity and Infrastructure Security Agency as established under section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 and subsequent laws, or any successor organization.

Cybersecurity threat means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. This term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Director means the Director of CISA, any successors to that position within the Department of Homeland Security, or any designee.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including, but not limited to, operational technology systems such as industrial control systems, supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

Joint Covered Cyber Incident and Ransom Payment Report means a submission made by a covered entity or a third party on behalf of a covered entity to simultaneously report both a covered cyber incident and ransom payment related to the covered cyber

incident being reported, as required by this part. A Joint Covered Cyber Incident and Ransom Payment Report also includes any responses to optional questions and additional information voluntarily submitted as part of the report.

Managed service provider means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity, such as hosting, or in a third-party data center.

Personal information means information that identifies a specific individual or nonpublic information associated with an identified or identifiable individual. Examples of personal information include, but are not limited to, photographs, names, home addresses, direct telephone numbers, social security numbers, medical information, personal financial information, contents of personal communications, and personal web browsing history.

Ransom payment means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

Ransom Payment Report means a submission made by a covered entity or a third party on behalf of a covered entity to report a ransom payment as required by this part. A Ransom Payment Report also includes any responses to optional questions and additional information voluntarily submitted as part of a Ransom Payment Report.

Ransomware attack means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or that actually or imminently jeopardizes, without lawful authority, an information system that involves, but need not be limited to, the following:

(1) The use or the threat of use of:

(i) Unauthorized or malicious code on an information system; or

(ii) Another digital mechanism such as a denial-of-service attack;

(2) To interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system; and

(3) To extort a ransom payment.

(4) *Exclusion.* A ransomware attack does not include any event where the demand for a ransom payment is:

(i) Not genuine; or

(ii) Made in good faith by an entity in response to a specific request by the owner or operator of the information system.

State, Local, Tribal, or Territorial Government entity or SLTT Government entity means an organized domestic entity which, in addition to having governmental character, has sufficient discretion in the management of its own affairs to distinguish it as separate from the administrative structure of any other governmental unit, and which is one of the following or a subdivision thereof:

(1) A State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States;

(2) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regardless of whether the council of governments is incorporated as a nonprofit corporation under State law, regional or interstate government entity, or agency or instrumentality of a Local government;

(3) An Indian tribe, band, nation, or other organized group or community, or other organized group or community, including any Alaska Native village or regional or village corporation as defined in or established pursuant to 43 U.S.C. 1601 *et seq.*, which is

recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians; and

(4) A rural community, unincorporated town or village, or other public entity.

Substantial cyber incident means a cyber incident that leads to any of the following:

(1) A substantial loss of confidentiality, integrity or availability of a covered entity's information system or network;

(2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

(3) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

(4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:

(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

(ii) Supply chain compromise.

(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

(6) The term "substantial cyber incident" does not include:

(i) Any lawfully authorized activity of a United States Government entity or SLTT Government entity, including activities undertaken pursuant to a warrant or other judicial process;

(ii) Any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or

(iii) The threat of disruption as extortion, as described in 6 U.S.C. 650(22).

Supplemental report means a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required by this part. A supplemental report also includes any responses to optional questions and additional information voluntarily submitted as part of a supplemental report.

Supply chain compromise means a cyber incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

Virtual currency means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value. Virtual currency includes a form of value that substitutes for currency or funds.

§ 226.2 Applicability.

This part applies to an entity in a critical infrastructure sector that either:

(a) *Exceeds the small business size standard.* Exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the U.S. Small Business Administration's Small Business Size Regulations as set forth in 13 CFR part 121; or

(b) *Meets a sector-based criterion.* Meets one or more of the sector-based criteria provided below, regardless of the specific critical infrastructure sector of which the entity considers itself to be part:

(1) *Owns or operates a covered chemical facility.* The entity owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards pursuant to 6 CFR part 27;

(2) *Provides wire or radio communications service*. The entity provides communications services by wire or radio communications, as defined in 47 U.S.C. 153(40), 153(59), to the public, businesses, or government, as well as one-way services and two-way services, including but not limited to:

(i) Radio and television broadcasters;

(ii) Cable television operators;

(iii) Satellite operators;

(iv) Telecommunications carriers;

(v) Submarine cable licensees required to report outages to the Federal Communications Commission under 47 CFR 4.15;

(vi) Fixed and mobile wireless service providers;

(vii) Voice over Internet Protocol providers; or

(viii) Internet service providers;

(3) *Owns or operates critical manufacturing sector infrastructure*. The entity owns or has business operations that engage in one or more of the following categories of manufacturing:

(i) Primary metal manufacturing;

(ii) Machinery manufacturing;

(iii) Electrical equipment, appliance, and component manufacturing; or

(iv) Transportation equipment manufacturing;

(4) *Provides operationally critical support to the Department of Defense or processes, stores, or transmits covered defense information.* The entity is a contractor or subcontractor required to report cyber incidents to the Department of Defense pursuant to

the definitions and requirements of the Defense Federal Acquisition Regulation Supplement 48 CFR 252.204-7012;

(5) *Performs an emergency service or function*. The entity provides one or more of the following emergency services or functions to a population equal to or greater than 50,000 individuals:

(i) Law enforcement;

(ii) Fire and rescue services;

(iii) Emergency medical services;

(iv) Emergency management; or

(v) Public works that contribute to public health and safety;

(6) *Bulk electric and distribution system entities.* The entity is required to report cybersecurity incidents under the North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to the Department of Energy;

(7) *Owns or operates financial services sector infrastructure*. The entity owns or operates any legal entity that qualifies as one or more of the following financial services entities:

(i) A banking or other organization regulated by:

(A) The Office of the Comptroller of the Currency under 12 CFR parts 30 and 53, which includes all national banks, Federal savings associations, and Federal branches and agencies of foreign banks;

(B) The Federal Reserve Board under:

(1) 12 CFR parts 208, 211, 225, or 234, which includes all U.S. bank holding companies, savings and loans holding companies, state member banks, the U.S.

operations of foreign banking organizations, Edge and agreement corporations, and certain designated financial market utilities; or

(2) 12 U.S.C. 248(j), which includes the Federal Reserve Banks;

(C) The Federal Deposit Insurance Corporation under 12 CFR part 304, which includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations;

(ii) A Federally insured credit union regulated by the National Credit Union Administration under 12 CFR part 748;

(iii) A designated contract market, swap execution facility, derivatives clearing organization, or swap data repository regulated by the Commodity Futures Trading Commission under 17 CFR parts 37, 38, 39, and 49;

(iv) A futures commission merchant or swap dealer regulated by the Commodity Futures Trading Commission under 17 CFR parts 1 and 23;

(v) A systems compliance and integrity entity, security-based swap dealer, or security-based swap data repository regulated by the Securities and Exchange Commission under Regulation Systems Compliance and Integrity or Regulation Security-Based Swap Regulatory Regime, 17 CFR part 242;

(vi) A money services business as defined in 31 CFR 1010.100(ff); or

(vii) Fannie Mae and Freddie Mac as defined in 12 CFR 1201.1;

(8) *Qualifies as a State, local, Tribal, or territorial government entity.* The entity is a State, local, Tribal, or territorial government entity for a jurisdiction with a population equal to or greater than 50,000 individuals;

(9) *Qualifies as an education facility*. The entity qualifies as any of the following types of education facilities:

(i) A local educational agency, educational service agency, or state educational agency, as defined under 20 U.S.C. 7801, with a student population equal to or greater than 1,000 students; or

(ii) An institute of higher education that receives funding under Title IV of the Higher Education Act, 20 U.S.C. 1001 *et seq*., as amended;

(10) *Involved with information and communications technology to support elections processes.* The entity manufactures, sells, or provides managed services for information and communications technology specifically used to support election processes or report and display results on behalf of State, Local, Tribal, or Territorial governments, including but not limited to:

(i) Voter registration databases;

(ii) Voting systems; and

(iii) Information and communication technologies used to report, display, validate, or finalize election results;

(11) *Provides essential public health-related services*. The entity provides one or more of the following essential public health-related services:

(i) Owns or operates a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1);

(ii) Manufactures drugs listed in appendix A of the *Essential Medicines Supply Chain and Manufacturing Resilience Assessment* developed pursuant to section 3 of E.O. 14017; or

(iii) Manufactures a Class II or Class III device as defined by 21 U.S.C. 360c;

(12) *Information technology entities.* The entity meets one or more of the following criteria:

(i) Knowingly provides or supports information technology hardware, software, systems, or services to the Federal government;

(ii) Has developed and continues to sell, license, or maintain any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

(A) Is designed to run with elevated privilege or manage privileges;

(B) Has direct or privileged access to networking or computing resources;

(C) Is designed to control access to data or operational technology;

(D) Performs a function critical to trust; or

(E) Operates outside of normal trust boundaries with privileged access;

(iii) Is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components;

(iv) Performs functions related to domain name operations;

(13) *Owns or operates a commercial nuclear power reactor or fuel cycle Facility.* The entity owns or operates a commercial nuclear power reactor or fuel cycle facility licensed to operate under the regulations of the Nuclear Regulatory Commission, 10 CFR chapter I;

(14) *Transportation system entities*. The entity is required by the Transportation Security Administration to report cyber incidents or otherwise qualifies as one or more of the following transportation system entities:

(i) A freight railroad carrier identified in 49 CFR 1580.1(a)(1), (4), or (5);

(ii) A public transportation agency or passenger railroad carrier identified in 49 CFR 1582.1(a)(1)-(4);

(iii) An over-the-road bus operator identified in 49 CFR 1584.1;

(iv) A pipeline facility or system owner or operator identified in 49 CFR 1586.101;

(v) An aircraft operator regulated under 49 CFR part 1544;

(vi) An indirect air carrier regulated under 49 CFR part 1548;

(vii) An airport operator regulated under 49 CFR part 1542; or

(viii) A Certified Cargo Screening Facility regulated under 49 CFR part 1549;

(15) *Subject to regulation under the Maritime Transportation Security Act.* The entity owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106; or

(16) *Owns or operates a qualifying community water system or publicly owned treatment works.* The entity owns or operates a community water system, as defined in 42 U.S.C. 300f(15), or a publicly owned treatment works, as defined in 40 CFR 403.3(q), for a population greater than 3,300 people.

§ 226.3 Required reporting on covered cyber incidents and ransom payments.

(a) *Covered cyber incident.* A covered entity that experiences a covered cyber incident must report the covered cyber incident to CISA in accordance with this part.

(b) *Ransom payment.* A covered entity that makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, as the result of a ransomware attack against the covered entity must report the ransom payment to CISA in accordance with this part. This reporting requirement applies to a covered entity even if the ransomware attack that resulted in a ransom payment is not a covered cyber incident subject to the reporting requirements of this part. If a covered entity makes a ransom payment that relates to a covered cyber incident that was previously reported in accordance with paragraph (a) of this section, the covered entity must instead submit a supplemental report in accordance with paragraph (d)(1)(ii) of this section.

(c) *Covered cyber incident and ransom payment.* A covered entity that experiences a covered cyber incident and makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, that is related to that covered cyber incident may report both events to CISA in a Joint Covered Cyber Incident and Ransom Payment Report in accordance with this part. If a covered entity, or a third party

acting on the covered entity's behalf, submits a Joint Covered Cyber Incident and Ransom Payment Report in accordance with this part, the covered entity is not required to also submit reports pursuant to paragraph (a) and (b) of this section.

(d) *Supplemental Reports*--(1) *Required Supplemental Reports.* A covered entity must promptly submit Supplemental Reports to CISA about a previously reported covered cyber incident in accordance with this part unless and until such date that the covered entity notifies CISA that the covered cyber incident at issue has concluded and has been fully mitigated and resolved. Supplemental Reports must be promptly submitted by the covered entity if:

(i) Substantial new or different information becomes available. Substantial new or different information includes but is not limited to any information that the covered entity was required to provide as part of a Covered Cyber Incident Report but did not have at the time of submission; or

(ii) The covered entity makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, that relates to a covered cyber incident that was previously reported in accordance with paragraph (a) of this section.

(2) *Optional notification that a covered cyber incident has concluded.* A covered entity may submit a Supplemental Report to inform CISA that a covered cyber incident previously reported in accordance with paragraph (a) of this section has concluded and been fully mitigated and resolved.

§ 226.4 Exceptions to required reporting on covered cyber incidents and ransom payments.

(a) *Substantially similar reporting exception*--(1) *In general.* A covered entity that reports a covered cyber incident, ransom payment, or information that must be submitted to CISA in a supplemental report to another Federal agency pursuant to the terms of a CIRCIA Agreement will satisfy the covered entity's reporting obligations under § 226.3.

A covered entity is responsible for confirming that a CIRCIA Agreement is applicable to the covered entity and the specific reporting obligation it seeks to satisfy under this part, and therefore, qualifies for this exemption.

(2) *CIRCIA Agreement requirements*. A CIRCIA Agreement may be entered into and maintained by CISA and another Federal agency in circumstances where CISA has determined the following:

(i) A law, regulation, or contract exists that requires one or more covered entities to report covered cyber incidents or ransom payments to the other Federal agency;

(ii) The required information that a covered entity must submit to the other Federal agency pursuant to a legal, regulatory, or contractual reporting requirement is substantially similar information to that which a covered entity is required to include in a CIRCIA Report as specified in §§ 226.7 through 226.11, as applicable;

(iii) The applicable law, regulation, or contract requires covered entities to report covered cyber incidents or ransom payments to the other Federal agency within a substantially similar timeframe to those for CIRCIA Reports specified in § 226.5; and

(iv) CISA and the other Federal agency have an information sharing mechanism in place.

(3) *Substantially similar information determination*. CISA retains discretion to determine what constitutes substantially similar information for the purposes of this part. In general, in making this determination, CISA will consider whether the specific fields of information reported by the covered entity to another Federal agency are functionally equivalent to the fields of information required to be reported in CIRCIA Reports under §§ 226.7 through 226.11, as applicable.

(4) *Substantially similar timeframe.* Reporting in a substantially similar timeframe means that a covered entity is required to report covered cyber incidents, ransom payments, or supplemental reports to another Federal agency in a timeframe that enables

the report to be shared by the Federal agency with CISA by the applicable reporting deadline specified for each type of CIRCIA Report under § 226.5.

(5) *Public posting of CIRCIA Agreements.* CISA will maintain an accurate catalog of all CIRCIA Agreements on a public-facing website and will make CIRCIA Agreements publicly available, to the maximum extent practicable. An agreement will be considered a CIRCIA Agreement for the purposes of this section when CISA publishes public notice concerning the agreement on such website and until notice of termination or expiration has been posted as required under § 226.4(a)(6).

(6) *Termination or expiration of a CIRCIA Agreement*. CISA may terminate a CIRCIA Agreement at any time. CISA will provide notice of the termination or expiration of CIRCIA Agreements on the public-facing website where the catalog of CIRCIA Agreements is maintained.

(7) *Continuing supplemental reporting requirement*. Covered entities remain subject to the supplemental reporting requirements specified under § 226.3(d), unless the covered entity submits the required information to another Federal agency pursuant to the terms of a CIRCIA Agreement.

(8) *Communications with CISA*. Nothing in this section prevents or otherwise restricts CISA from contacting any entity that submits information to another Federal agency, nor is any entity prevented from communicating with, or submitting a CIRCIA Report to, CISA.

(b) *Domain Name System exception.* The following entities, to the degree that they are considered a covered entity under § 226.2, are exempt from the reporting requirements in this part:

(1) The Internet Corporation for Assigned Names and Numbers;

(2) The American Registry for Internet Numbers;

(3) Any affiliates controlled by the covered entities listed in paragraphs (b)(1) and (2) of this section; and

(4) The root server operator function of a covered entity that has been recognized by the Internet Corporation for Assigned Names and Numbers as responsible for operating one of the root identities and has agreed to follow the service expectations established by the Internet Corporation for Assigned Names and Numbers and its Root Server System Advisory Committee.

(c) *FISMA report exception.* Federal agencies that are required by the Federal Information Security Modernization Act, 44 U.S.C. 3551 *et seq.*, to report incidents to CISA are exempt from reporting those incidents as covered cyber incidents under this part.

§ 226.5 CIRCIA Report submission deadlines.

Covered entities must submit CIRCIA Reports in accordance with the submission deadlines specified in this section.

(a) *Covered Cyber Incident Report deadline.* A covered entity must submit a Covered Cyber Incident Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred.

(b) *Ransom Payment Report deadline*. A covered entity must submit a Ransom Payment Report to CISA no later than 24 hours after the ransom payment has been disbursed.

(c) *Joint Covered Cyber Incident and Ransom Payment Report deadline.* A covered entity that experiences a covered cyber incident and makes a ransom payment within 72 hours after the covered entity reasonably believes a covered cyber incident has occurred may submit a Joint Covered Cyber Incident and Ransom Payment Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred.

(d) *Supplemental Report Deadline.* A covered entity must promptly submit supplemental reports to CISA. If a covered entity submits a supplemental report on a ransom payment made after the covered entity submitted a Covered Cyber Incident Report, as required by § 226.3(d)(1)(ii), the covered entity must submit the Supplemental Report to CISA no later than 24 hours after the ransom payment has been disbursed.

§ 226.6 Required manner and form of CIRCIA Reports.

A covered entity must submit CIRCIA Reports to CISA through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director.

§ 226.7 Required information for CIRCIA Reports.

A covered entity must provide the following information in all CIRCIA Reports to the extent such information is available and applicable to the event reported:

(a) Identification of the type of CIRCIA Report submitted by the covered entity;

(b) Information relevant to establishing the covered entity's identity, including the covered entity's:

(1) Full legal name;

(2) State of incorporation or formation;

(3) Affiliated trade names;

(4) Organizational entity type;

(5) Physical address;

(6) Website;

(7) Internal incident tracking number for the reported event;

(8) Applicable business numerical identifiers;

(9) Name of the parent company or organization, if applicable; and

(10) The critical infrastructure sector or sectors in which the covered entity considers itself to be included;

(c) Contact information, including the full name, email address, telephone number, and title for:

(1) The individual submitting the CIRCIA Report on behalf of the covered entity;

(2) A point of contact for the covered entity if the covered entity uses a third party to submit the CIRCIA Report or would like to designate a preferred point of contact that is different from the individual submitting the report; and

(3) A registered agent for the covered entity, if neither the individual submitting the CIRCIA Report, nor the designated preferred point of contact are a registered agent for the covered entity; and

(d) If a covered entity uses a third party to submit a CIRCIA Report on the covered entity's behalf, an attestation that the third party is expressly authorized by the covered entity to submit the CIRCIA Report on the covered entity's behalf.

§ 226.8 Required information for Covered Cyber Incident Reports.

A covered entity must provide all the information identified in § 226.7 and the following information in a Covered Cyber Incident Report, to the extent such information is available and applicable to the covered cyber incident:

(a) A description of the covered cyber incident, including but not limited to:

(1) Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the covered cyber incident, including but not limited to:

(i) Technical details and physical locations of such networks, devices, and/or information systems; and

(ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require

protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);

(2) A description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;

(3) Dates pertaining to the covered cyber incident, including but not limited to:

(i) The date the covered cyber incident was detected;

(ii) The date the covered cyber incident began;

(iii) If fully mitigated and resolved at the time of reporting, the date the covered cyber incident ended;

(iv) The timeline of compromised system communications with other systems; and

(v) For covered cyber incidents involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting; and

(4) The impact of the covered cyber incident on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and information to enable CISA's assessment of any known impacts to national security or public health and safety;

(b) The category or categories of any information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person or persons;

(c) A description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;

(d) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident;

(e) A description of the type of incident and the tactics, techniques, and procedures used to perpetrate the covered cyber incident, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;

(f) Any indicators of compromise, including but not limited to those listed in § 226.13(b)(1)(ii), observed in connection with the covered cyber incident;

(g) A description and, if possessed by the covered entity, a copy or samples of any malicious software the covered entity believes is connected with the covered cyber incident;

(h) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the covered cyber incident;

(i) A description of any mitigation and response activities taken by the covered entity in response to the covered cyber incident, including but not limited to:

(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;

(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident;

(3) Identification of any law enforcement agency that is engaged in responding to the covered cyber incident, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and any law enforcement agency that the covered entity otherwise believes may be involved in investigating the covered cyber incident; and

(4) Whether the covered entity requested assistance from another entity in responding to the covered cyber incident and, if so, the identity of each entity and a description of the type of assistance requested or received from each entity;

(j) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.

§ 226.9 Required information for Ransom Payment Reports.

A covered entity must provide all the information identified in § 226.7 and the following information in a Ransom Payment Report, to the extent such information is available and applicable to the ransom payment:

(a) A description of the ransomware attack, including but not limited to:

(1) Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the ransomware attack, including but not limited to:

(i) Technical details and physical locations of such networks, devices, and/or information systems; and

(ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);

(2) A description of any unauthorized access, regardless of whether the ransomware attack involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;

(3) Dates pertaining to the ransomware attack, including but not limited to:

(i) The date the ransomware attack was detected;

(ii) The date the ransomware attack began;

(iii) If fully mitigated and resolved at the time of reporting, the date the ransomware attack ended;

(iv) The timeline of compromised system communications with other systems; and

(v) For ransomware attacks involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting; and

(4) The impact of the ransomware attack on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and any known or suspected impacts to national security or public health and safety;

(b) A description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;

(c) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the ransomware attack;

(d) A description of the tactics, techniques, and procedures used to perpetrate the ransomware attack, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;

(e) Any indicators of compromise the covered entity believes are connected with the ransomware attack, including, but not limited to, those listed in section 226.13(b)(1)(ii), observed in connection with the ransomware attack;

(f) A description and, if possessed by the covered entity, a copy or sample of any malicious software the covered entity believes is connected with the ransomware attack;

(g) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the ransomware attack;

(h) The date of the ransom payment;

(i) The amount and type of assets used in the ransom payment;

(j) The ransom payment demand, including but not limited to the type and amount of virtual currency, currency, security, commodity, or other form of payment requested;

(k) The ransom payment instructions, including but not limited to information regarding how to transmit the ransom payment; the virtual currency or physical address where the ransom payment was requested to be sent; any identifying information about the ransom payment recipient; and information related to the completed payment, including any transaction identifier or hash;

(l) Outcomes associated with making the ransom payment, including but not limited to whether any exfiltrated data was returned or a decryption capability was provided to the covered entity, and if so, whether the decryption capability was successfully used by the covered entity;

(m) A description of any mitigation and response activities taken by the covered entity in response to the ransomware attack, including but not limited to:

(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;

(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the ransomware attack;

(3) Identification of any law enforcement agency that is engaged in responding to the ransomware attack, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and

any law enforcement agency that the covered entity otherwise believes may be involved in investigating the ransomware attack; and

(4) Whether the covered entity requested assistance from another entity in responding to the ransomware attack or making the ransom payment and, if so, the identity of such entity or entities and a description of the type of assistance received from each entity;

(n) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.

§ 226.10 Required information for Joint Covered Cyber Incident and Ransom Payment Reports.

A covered entity must provide all the information identified in §§ 226.7, 226.8, and 226.9 in a Joint Covered Cyber Incident and Ransom Payment Report to the extent such information is available and applicable to the reported covered cyber incident and ransom payment.

§ 226.11 Required information for Supplemental Reports.

(a) *In general.* A covered entity must include all of the information identified as required in § 226.7 and the following information in any Supplemental Report:

(1) The case identification number provided by CISA for the associated Covered Cyber Incident Report or Joint Covered Cyber Incident and Ransom Payment Report;

(2) The reason for filing the Supplemental Report;

(3) Any substantial new or different information available about the covered cyber incident, including but not limited to information the covered entity was required to provide as part of a Covered Cyber Incident Report but did not have at the time of submission and information required under § 226.9 if the covered entity or another entity on the covered entity's behalf has made a ransom payment after submitting a Covered Cyber Incident Report; and

(4) Any other data or information required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.

(b) *Required information for a Supplemental Report providing notice of a ransom payment made following submission of a Covered Cyber Incident Report.* When a covered entity submits a Supplemental Report to notify CISA that the covered entity has made a ransom payment after submitting a related Covered Cyber Incident Report, the supplemental report must include the information required in § 226.9.

(c) *Optional information to provide notification that a covered cyber incident has concluded.* Covered entities that choose to submit a notification to CISA that a covered cyber incident has concluded and has been fully mitigated and resolved may submit optional information related to the conclusion of the covered cyber incident.

§ 226.12 Third party reporting procedures and requirements.

(a) *General*. A covered entity may expressly authorize a third party to submit a CIRCIA Report on the covered entity's behalf to satisfy the covered entity's reporting obligations under § 226.3. The covered entity remains responsible for ensuring compliance with its reporting obligations under this part even when the covered entity has authorized a third party to submit a CIRCIA Report on the covered entity's behalf.

(b) *Procedures for third party submission of CIRCIA Reports*. CIRCIA Reports submitted by third parties must comply with the reporting requirements and procedures for covered entities set forth in this part.

(c) *Confirmation of express authorization required.* For the purposes of compliance with the covered entity's reporting obligations under this part, upon submission of a CIRCIA Report, a third party must confirm that the covered entity expressly authorized the third party to file the CIRCIA Report on the covered entity's behalf. CIRCIA Reports submitted by a third party without an attestation from the third party that the third party has the express authorization of a covered entity to submit a

report on the covered entity's behalf will not be considered by CISA for the purposes of compliance of the covered entity's reporting obligations under this part.

(d) *Third party ransom payments and responsibility to advise a covered entity*. A third party that makes a ransom payment on behalf of a covered entity impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for the ransom payment. When a third party knowingly makes a ransom payment on behalf of a covered entity, the third party must advise the covered entity of its obligations to submit a Ransom Payment Report under this part.

§ 226.13 Data and records preservation requirements.

(a) *Applicability*. (1) A covered entity that is required to submit a CIRCIA Report under § 226.3 or experiences a covered cyber incident or makes a ransom payment but is exempt from submitting a CIRCIA Report pursuant to § 226.4(a) is required to preserve data and records related to the covered cyber incident or ransom payment in accordance with this section.

(2) A covered entity maintains responsibility for compliance with the preservation requirements in this section regardless of whether the covered entity submitted a CIRCIA Report or a third party submitted the CIRCIA Report on the covered entity's behalf.

(b) *Covered data and records.* (1) A covered entity must preserve the following data and records:

(i) Communications with any threat actor, including copies of actual correspondence, including but not limited to emails, texts, instant or direct messages, voice recordings, or letters; notes taken during any interactions; and relevant information on the communication facilities used, such as email or Tor site;

(ii) Indicators of compromise, including but not limited to suspicious network traffic; suspicious files or registry entries; suspicious emails; unusual system logins; unauthorized accounts created, including usernames, passwords, and date/time stamps

and time zones for activity associated with such accounts; and copies or samples of any malicious software;

(iii) Relevant log entries, including but not limited to, Domain Name System, firewall, egress, packet capture file, NetFlow, Security Information and Event Management/Security Information Management, database, Intrusion Prevention System/Intrusion Detection System, endpoint, Active Directory, server, web, Virtual Private Network, Remote Desktop Protocol, and Window Event;

(iv) Relevant forensic artifacts, including but not limited to live memory captures; forensic images; and preservation of hosts pertinent to the incident;

(v) Network data, including but not limited to NetFlow or packet capture file, and network information or traffic related to the incident, including the Internet Protocol addresses associated with the malicious cyber activity and any known corresponding dates, timestamps, and time zones;

(vi) Data and information that may help identify how a threat actor compromised or potentially compromised an information system, including but not limited to information indicating or identifying how one or more threat actors initially obtained access to a network or information system and the methods such actors employed during the incident;

(vii) System information that may help identify exploited vulnerabilities, including but not limited to operating systems, version numbers, patch levels, and configuration settings;

(viii) Information about exfiltrated data, including but not limited to file names and extensions; the amount of data exfiltration by byte value; category of data exfiltrated, including but not limited to, classified, proprietary, financial, or personal information; and evidence of exfiltration, including but not limited to relevant logs and screenshots of exfiltrated data sent from the threat actor;

(ix) All data or records related to the disbursement or payment of any ransom payment, including but not limited to pertinent records from financial accounts associated with the ransom payment; and

(x) Any forensic or other reports concerning the incident, whether internal or prepared for the covered entity by a cybersecurity company or other third-party vendor.

(2) A covered entity is not required to create any data or records it does not already have in its possession based on this requirement.

(c) *Required preservation period.* Covered entities must preserve all data and records identified in paragraph (b) of this section:

(1) Beginning on the earliest of the following dates:

(i) The date upon which the covered entity establishes a reasonable belief that a covered cyber incident occurred; or

(ii) The date upon which a ransom payment was disbursed; and

(2) For no less than two years from the submission of the most recently required CIRCIA Report submitted pursuant to § 226.3, or from the date such submission would have been required but for the exception pursuant to § 226.4(a).

(d) *Original data or record format.* Covered entities must preserve data and records set forth in paragraph (b) of this section in their original format or form whether the data or records are generated automatically or manually, internally or received from outside sources by the covered entity, and regardless of the following:

(1) Form or format, including hard copy records and electronic records;

(2) Where the information is stored, located, or maintained without regard to the physical location of the information, including stored in databases or cloud storage, on network servers, computers, other wireless devices, or by a third-party on behalf of the covered entity; and

(3) Whether the information is in active use or archived.

(e) *Storage, protection, and allowable use of data and records*. (1) A covered entity may select its own storage methods, electronic or non-electronic, and procedures to maintain the data and records that must be preserved under this section.

(2) Data and records must be readily accessible, retrievable, and capable of being lawfully shared by the covered entity, including in response to a lawful government request.

(3) A covered entity must use reasonable safeguards to protect data and records against unauthorized access or disclosure, deterioration, deletion, destruction, and alteration.

§ 226.14 Request for information and subpoena procedures.

(a) *In general*. This section applies to covered entities, except a covered entity that qualifies as a State, Local, Tribal, or Territorial Government entity as defined in § 226.1.

(b) *Use of authorities*. When determining whether to exercise the authorities in this section, the Director or designee will take into consideration:

(1) The complexity in determining if a covered cyber incident has occurred; and

(2) The covered entity's prior interaction with CISA or the covered entity's awareness of CISA's policies and procedures for reporting covered cyber incidents and ransom payments.

(c) *Request for information*--(1) *Issuance of request*. The Director may issue a request for information to a covered entity if there is reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with § 226.3. Reason to believe that a covered entity failed to submit a CIRCIA Report in accordance with § 226.3 may be based upon public reporting or other information in possession of the Federal Government, which includes but is not limited to analysis performed by CISA. A request for information will be

served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(2) *Form and contents of the request*. At a minimum, a request for information must include:

(i) The name and address of the covered entity;

(ii) A summary of the facts that have led CISA to believe that the covered entity has failed to submit a required CIRCIA Report in accordance with § 226.3. This summary is subject to the nondisclosure provision in paragraph (f) of this section;

(iii) A description of the information requested from the covered entity. The Director, in his or her discretion, may decide the scope and nature of information necessary for CISA to confirm whether a covered cyber incident or ransom payment occurred. Requested information may include electronically stored information, documents, reports, verbal or written responses, records, accounts, images, data, data compilations, and tangible items;

(iv) A date by which the covered entity must reply to the request for information; and

(v) The manner and format in which the covered entity must provide all information requested to CISA.

(3) *Response to request for information*. A covered entity must reply in the manner and format, and by the deadline, specified by the Director. If the covered entity does not respond by the date specified in paragraph (c)(2)(iv) of this section or the Director determines that the covered entity's response is inadequate, the Director, in his or her discretion, may request additional information from the covered entity to confirm whether a covered cyber incident or ransom payment occurred, or the Director may issue a subpoena to compel information from the covered entity pursuant to paragraph (d) of this section.

(4) *Treatment of information received*. Information provided to CISA by a covered entity in a reply to a request for information under this section will be treated in accordance with §§ 226.18 and 226.19.

(5) *Unavailability of Appeal*. A request for information is not a final agency action within the meaning of 5 U.S.C. 704 and cannot be appealed.

(d) *Subpoena*--(1) *Issuance of subpoena*. The Director may issue a subpoena to compel disclosure of information from a covered entity if the entity fails to reply by the date specified in paragraph (c)(2)(iv) of this section or provides an inadequate response, to a request for information. The authority to issue a subpoena is a nondelegable authority. A subpoena will be served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(2) *Timing of subpoena*. A subpoena to compel disclosure of information from a covered entity may be issued no earlier than 72 hours after the date of service of the request for information.

(3) *Form and contents of subpoena*. At a minimum, a subpoena must include:

(i) The name and address of the covered entity;

(ii) An explanation of the basis for issuance of the subpoena and a copy of the request for information previously issued to the covered entity, subject to the nondisclosure provision in paragraph (f) of this section;

(iii) A description of the information that the covered entity is required to produce. The Director, in his or her discretion, may determine the scope and nature of information necessary to determine whether a covered cyber incident or ransom payment occurred, obtain the information required to be reported under § 226.3, and to assess the potential impacts to national security, economic security, or public health and safety. Subpoenaed information may include electronically stored information, documents,

reports, verbal or written responses, records, accounts, images, data, data compilations, and tangible items;

(iv) A date by which the covered entity must reply; and

(v) The manner and format in which the covered entity must provide all information requested to CISA.

(4) *Reply to the Subpoena*. A covered entity must reply in the manner and format, and by the deadline, specified by the Director. If the Director determines that the information received from the covered entity is inadequate to determine whether a covered cyber incident or ransom payment occurred, does not satisfy the reporting requirements under § 226.3, or is inadequate to assess the potential impacts to national security, economic security, or public health and safety, the Director may request or subpoena additional information from the covered entity or request civil enforcement of a subpoena pursuant to § 226.15.

(5) *Authentication requirement for electronic subpoenas*. Subpoenas issued electronically must be authenticated with a cryptographic digital signature of an authorized representative of CISA or with a comparable successor technology that demonstrates the subpoena was issued by CISA and has not been altered or modified since issuance. Electronic subpoenas that are not authenticated pursuant to this subparagraph are invalid.

(6) *Treatment of information received in response to a subpoena*--(i) *In general.* Information obtained by subpoena is not subject to the information treatment requirements and restrictions imposed within § 226.18 and privacy and procedures for protecting privacy and civil liberties in § 226.19; and

(ii) *Provision of certain information for criminal prosecution and regulatory enforcement proceedings.* The Director may provide information submitted in response to a subpoena to the Attorney General or the head of a Federal regulatory agency if the

Director determines that the facts relating to the cyber incident or ransom payment may constitute grounds for criminal prosecution or regulatory enforcement action. The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making any such determination. Information provided by CISA under this paragraph (d)(6)(ii) may be used by the Attorney General or the head of a Federal regulatory agency for criminal prosecution or a regulatory enforcement action. Any decision by the Director to exercise this authority does not constitute final agency action within the meaning of 5 U.S.C. 704 and cannot be appealed.

(7) *Withdrawal and appeals of subpoena issuance*--(i) *In general.* CISA, in its discretion, may withdraw a subpoena that is issued to a covered entity. Notice of withdrawal of a subpoena will be served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(ii) *Appeals of subpoena issuance.* A covered entity may appeal the issuance of a subpoena through a written request that the Director withdraw it. A covered entity, or a representative on behalf of the covered entity, must file a Notice of Appeal within seven (7) calendar days after service of the subpoena. All Notices of Appeal must include:

(A) The name of the covered entity;

(B) The date of subpoena issuance;

(C) A clear request that the Director withdraw the subpoena;

(D) The covered entity's rationale for requesting a withdrawal of the subpoena; and

(E) Any additional information that the covered entity would like the Director to consider as part of the covered entity's appeal.

(iii) *Director's final decision*. Following receipt of a Notice of Appeal, the Director will issue a final decision and serve it upon the covered entity. A final decision made by the Director constitutes final agency action. If the Director's final decision is to

withdraw the subpoena, a notice of withdrawal of a subpoena will be served on the covered entity in accordance with the procedures in § 226.14(e).

(e) *Service*--(1) *covered entity point of contact.* A request for information, subpoena, or notice of withdrawal of a subpoena may be served by delivery on an officer, managing or general agent, or any other agent authorized by appointment or law to receive service of process on behalf of the covered entity.

(2) *Method of service.* Service of a request for information, subpoena, or notice of withdrawal of a subpoena will be served on a covered entity through a reasonable electronic or non-electronic attempt that demonstrates receipt, such as certified mail with return receipt, express commercial courier delivery, or electronically.

(3) *Date of service*. The date of service of any request for information, subpoena, or notice of withdrawal of a subpoena shall be the date on which the document is mailed, electronically transmitted, or delivered in person, whichever is applicable.

(f) *Nondisclosure of certain information*. In connection with the procedures in this section, CISA will not disclose classified information as defined in Section 1.1(d) of E.O. 12968 and reserves the right to not disclose any other information or material that is protected from disclosure under law or policy.

§ 226.15 Civil enforcement of subpoenas.

(a) *In general.* If a covered entity fails to comply with a subpoena issued pursuant to § 226.14(d), the Director may refer the matter to the Attorney General to bring a civil action to enforce the subpoena in any United States District Court for the judicial district in which the covered entity resides, is found, or does business.

(b) *Contempt.* A United States District Court may order compliance with the subpoena and punish failure to obey a subpoena as a contempt of court.

(c) *Classified and protected information*. In any review of an action taken under § 226.14, if the action was based on classified or protected information as described in §

226.14(f), such information may be submitted to the reviewing court *ex parte* and *in camera*. This paragraph does not confer or imply any right to review in any tribunal, judicial or otherwise.

§ 226.16 Referral to the Department of Homeland Security Suspension and Debarment Official.

The Director must refer all circumstances concerning a covered entity's noncompliance that may warrant suspension and debarment action to the Department of Homeland Security Suspension and Debarment Official.

§ 226.17 Referral to Cognizant Contracting Official or Attorney General.

The Director may refer information concerning a covered entity's noncompliance with the reporting requirements in this part that pertain to performance under a federal procurement contract to the cognizant contracting official or the Attorney General for civil or criminal enforcement.

§ 226.18 Treatment of information and restrictions on use.

(a) *In general*. The protections and restrictions on use enumerated in this section apply to CIRCIA Reports and information included in such reports where specified in this section, as well as to all responses provided to requests for information issued under § 226.14(c). This section does not apply to information and reports submitted in response to a subpoena issued under § 226.14(d) or following Federal government action under §§ 226.15-226.17.

(b) *Treatment of information*--(1) *Designation as commercial, financial, and proprietary information.* A covered entity must clearly designate with appropriate markings at the time of submission a CIRCIA Report, a response provided to a request for information issued under § 226.14(c), or any portion of a CIRCIA Report or a response provided to a request for information issued under § 226.14(c) that it considers to be commercial, financial, and proprietary information. CIRCIA Reports, responses

provided to a request for information issued under § 226.14(c), or designated portions thereof, will be treated as commercial, financial, and proprietary information of the covered entity upon designation as such by a covered entity.

(2) *Exemption from disclosure under the Freedom of Information Act*. CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and under any State, Local, or Tribal government freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. If CISA receives a request under the Freedom of Information Act to which a CIRCIA Report, response to a request for information under § 226.14(c), or information contained therein is responsive, CISA will apply all applicable exemptions from disclosure, consistent with 6 CFR part 5.

(3) *No Waiver of Privilege*. A covered entity does not waive any applicable privilege or protection provided by law, including trade secret protection, as a consequence of submitting a CIRCIA Report under this part or a response to a request for information issued under § 226.14(c).

(4) *Ex parte communications waiver*. CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are not subject to the rules or procedures of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) *Restrictions on use*--(1) *Prohibition on use in regulatory actions*. Federal, State, Local, and Tribal Government entities are prohibited from using information obtained solely through a CIRCIA Report submitted under this part or a response to a request for information issued under § 226.14(c) to regulate, including through an

enforcement proceeding, the activities of the covered entity or the entity that made a ransom payment on the covered entity's behalf, except:

(i) If the Federal, State, Local, or Tribal Government entity expressly allows the entity to meet its regulatory reporting obligations through submission of reports to CISA; or

(ii) Consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, a CIRCIA Report or response to a request for information issued under § 226.14(c) may inform the development or implementation of regulations relating to such systems.

(2) *Liability protection*--(i) *No cause of action.* No cause of action shall lie or be maintained in any court by any person or entity for the submission of a CIRCIA Report or a response to a request for information issued under § 226.14(c) and must be promptly dismissed by the court. This liability protection only applies to or affects litigation that is solely based on the submission of a CIRCIA Report or a response provided to a request for information issued under § 226.14(c).

(ii) *Evidentiary and discovery bar for reports*. CIRCIA Reports submitted under this part, responses provided to requests for information issued under § 226.14(c), or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting CIRCIA Reports or responses to requests for information issued under § 226.14(c), may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof. This bar does not create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report under this part or a response to a request for information issued under § 226.14(c).

(iii) *Exception*. The liability protection provided in paragraph (c)(2)(i) of this section does not apply to an action taken by the Federal government pursuant to § 226.15.

(3) *Limitations on authorized uses.* Information provided to CISA in a CIRCIA Report or in a response to a request for information issued under § 226.14(c) may be disclosed to, retained by, and used by any Federal agency or department, component, officer, employee, or agent of the Federal Government, consistent with otherwise applicable provisions of Federal law, solely for the following purposes:

(i) A cybersecurity purpose;

(ii) The purpose of identifying a cybersecurity threat, including the source of the cybersecurity threat, or a security vulnerability;

(iii) The purpose of responding to, or otherwise preventing or mitigating, a specific threat of:

(A) Death;

(B) Serious bodily harm; or

(C) Serious economic harm;

(iv) The purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) The purpose of preventing, investigating, disrupting, or prosecuting an offense:

(A) Arising out of events required to be reported in accordance with § 226.3;

(B) Described in 18 U.S.C. 1028 through 1030 relating to fraud and identity theft;

(C) Described in 18 U.S.C. chapter 37 relating to espionage and censorship; or

(D) Described in 18 U.S.C. 90 relating to protection of trade secrets.

§ 226.19 Procedures for protecting privacy and civil liberties.

(a) *In general*. The use of personal information received in CIRCIA Reports and in responses provided to requests for information issued under § 226.14(c) is subject to the procedures described in this section for protecting privacy and civil liberties. CISA will ensure that privacy controls and safeguards are in place at the point of receipt, retention, use, and dissemination of a CIRCIA Report. The requirements in this section do not apply to personal information submitted in response to a subpoena issued under § 226.14(d) or following Federal government action under §§ 226.15 through 226.17.

(b) *Instructions for submitting personal information.* A covered entity should only include the personal information requested by CISA in the web-based CIRCIA Incident Reporting Form or in the request for information and should exclude unnecessary personal information from CIRCIA Reports and responses to requests for information issued under § 226.14(c).

(c) *Assessment of personal information.* CISA will review each CIRCIA Report and response to request for information issued under § 226.14(c) to determine if the report contains personal information other than the information requested by CISA and whether the personal information is directly related to a cybersecurity threat. Personal information directly related to a cybersecurity threat includes personal information that is necessary to detect, prevent, or mitigate a cybersecurity threat.

(1) If CISA determines the personal information is not directly related to a cybersecurity threat, nor necessary for contacting a covered entity or report submitter, CISA will delete the personal information from the CIRCIA Report or response to request for information. covered entity or report submitter contact information, including information of third parties submitting on behalf of an entity, will be safeguarded when retained and anonymized prior to sharing the report outside of the federal government unless CISA receives the consent of the individual for sharing personal information and

the personal information can be shared without revealing the identity of the covered entity.

(2) If the personal information is determined to be directly related to a cybersecurity threat, CISA will retain the personal information and may share it consistent with § 226.18 of this part and the guidance described in paragraph (d) of this section.

(d) *Privacy and civil liberties guidance.* CISA will develop and make publicly available guidance relating to privacy and civil liberties to address the retention, use, and dissemination of personal information contained in Covered Cyber Incident Reports and Ransom Payment Reports by CISA. The guidance shall be consistent with the need to protect personal information from unauthorized use or disclosure, and to mitigate cybersecurity threats.

(1) One year after the publication of the guidance, CISA will review the effectiveness of the guidance to ensure that it appropriately governs the retention, use, and dissemination of personal information pursuant to this part and will perform subsequent reviews periodically.

(2) The Chief Privacy Officer of CISA will complete an initial review of CISA's compliance with the privacy and civil liberties guidance approximately one year after the effective date of this part and subsequent periodic reviews not less frequently than every three years.

§ 226.20 Other procedural measures.

(a) *Penalty for false statements and representations*. Any person that knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, response to a request for information, or response to an administrative subpoena is subject to the penalties under 18 U.S.C. 1001.

(b) *Severability.* CISA intends the various provisions of this part to be severable from each other to the extent practicable, such that if a court of competent jurisdiction were to vacate or enjoin any one provision, the other provisions are intended to remain in effect unless they are dependent upon the vacated or enjoined provision.

Jennie M. Easterly,

Director,

Cybersecurity and Infrastructure Security Agency,

Department of Homeland Security.

[FR Doc. 2024-06526 Filed: 3/27/2024 8:45 am; Publication Date: 4/4/2024]