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]