WHAT WOULD BE A COVERED CYBER INCIDENT UNDER CIRCIA AS PROPOSED IN 6 CFR § 226.1?

DISCLAIMER: This is an unofficial, informational resource summarizing key aspects of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Notice of Proposed Rulemaking (NPRM) and is only intended to highlight major requirements proposed in the NPRM and to assist stakeholders in reviewing the NPRM. While CISA has taken steps to ensure the accuracy of this resource, it does not supplement, supersede, or modify any of the proposals included in the NPRM. This resource is not a substitute for reviewing the NPRM which is available on the Federal Register at www.federalregister.gov. If any conflict exists between this resource and the NPRM, the document published in the Federal Register is the controlling document. Additionally, this resource is based upon the proposed rulemaking and should not be relied upon for compliance purposes after publication of the final rule. CISA may also revise this resource to clarify or update content. For additional and latest information, consult cisa.gov/CIRCIA.

OVERVIEW

Under the CIRCIA NPRM, a covered entity that experiences a ***covered cyber incident*** is required to report.[i] A covered cyber incident is a substantial cyber incident experienced by a covered entity.[ii]

COVERED CYBER INCIDENT

=

SUBSTANTIAL CYBER INCIDENT

IF...

A cyber incident is a substantial cyber incident if it leads to one of the following impacts:[iii]

a. Substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;[iv]

b. Serious impact on the safety and resilience of a covered entity's operational systems and processes;[v]

c. Disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;[vi] 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 a

- **i)** Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
- **ii)** Supply chain compromise.[vii]

UNLESS

a. It is lawfully authorized activity of a Federal or SLTT government entity;[viii]

b. It is perpetrated in good faith in response to a specific request by the system owner/operator;[ix] or

c. It involves a threat to disrupt as extortion.[x]

+

EXPERIENCED BY A COVERED ENTITY

The incident must actually result in one or more of the impacts described above. Cyber incidents that put a covered entity at imminent risk of any of the threshold impacts, but do not actually result in an impact would not meet the definition of a substantial cyber incident.

EXAMPLES OF SUBSTANTIAL CYBER INCIDENTS

Whether a particular incident will be substantial for a particular covered entity is likely to be fact-dependent, but the following is a non-exhaustive illustrative list of incidents that likely would qualify as substantial cyber incidents:

1. A distributed denial-of-service (DDoS) attack that renders services unavailable to customers for an extended period of time.
2. A cyber incident that:
   a. encrypts a core business or information systems;
   b. significantly increases the potential for release of a hazardous material;
   c. compromises or disrupts a bulk electric system that performs a reliability task; or
   d. disrupts the ability of a communications service provider to transmit or delivery emergency alerts or 911 calls, or results in the transmission of false alerts or calls.
3. Exploitation of a vulnerability resulting in extended system or network downtime.
4. A ransomware attack that locks a covered entity out of its industrial control system.
5. Unauthorized access to a covered entity's business system:
   a. Caused by automated download of a tampered software update; or
   b. Using compromised credentials from a managed service provider.
6. Intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose.

EXAMPLES OF INCIDENTS UNLIKELY TO QUALIFY AS SUBSTANTIAL CYBER INCIDENTS

CISA encourages reporting or sharing of information about all cyber incidents, even if it would not be required under CIRCIA. The following is a non-exhaustive, illustrative list of incidents unlikely to qualify as substantial cyber incidents:

1. A DDoS attack or other incident that only results in a brief period of unavailability of a public-facing website that does not provide critical functions or services to customers or the public.
2. A cyber incident that results in minor disruption, 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 multi-factor authentication) are in place to preclude use of those credentials.
4. Malicious software is downloaded but antivirus software successfully quarantines the software and precludes it from executing.
5. A malicious actor exploits a known vulnerability, which the covered entity has not been able to patch but has instead deployed increased monitoring for tactics, techniques, and procedures associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.
6. Blocked phishing attempts.
7. Failed attempts to gain access to systems.
8. Credentials reported missing that have not been used to access a system and have since been rendered inactive.
9. Routine scanning that presents no evidence of penetration.

---

[i] § 226.3(a).
[ii] § 226.1 (definition of covered cyber incident).
[iii] § 226.1 (definition of substantial cyber incident). See further discussion on assessing whether an impact level is met at 89 FR 23,664-65.
[iv] See further discussion of "Impact 1" at 89 FR 23,662.
[v] See further discussion of "Impact 2" at 89 FR 23,662-63.
[vi] See further discussion of "Impact 3" at 89 FR 23,663.
[vii] See further discussion of "Impact 4" at 89 FR 23,663-64.
[viii] See further discussion of this exclusion at 89 FR 23,666-67.
[ix] See further discussion of this exclusion at 89 FR 23,667.
[x] See further discussion of this exclusion at 89 FR 23,667-68.