America's Credit Unions

Regulatory Comment: Summary and Feedback Request Cyber Incident Reporting

THE ISSUE:

On April 4, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) published a notice of proposed rulemaking to implement cyber incident and ransom payment reporting requirements adopted in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). 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.

IMPACT TO CREDIT UNIONS:

The proposal applies to covered entities operating in critical infrastructure sectors, including all federally insured credit unions (FICUs). While CISA's proposed reporting framework generally aligns with the cyber incident notification rules adopted by the National Credit Union Administration (NCUA) in 12 CFR Part 748, certain aspects of the proposal are new (i.e., ransom payments) and may require more detailed forensic assessments. To the extent reporting procedures differ between the NCUA and CISA, FICUs may face duplicative and potentially more burdensome reporting obligations unless CISA recognizes the NCUA's cyber incident notification framework as "substantially similar."

KEY POINTS:

- A covered cyber incident subject to reporting requirements would be defined as "substantial cyber incident." As proposed, the term substantial cyber incident is functionally similar to what the NCUA has adopted in 12 CFR § 748(c)(1); however, CISA's

proposed, multi-part definition could be construed as broader in some areas when compared to equivalent NCUA language.

- The preamble includes a list of cyber incidents that would likely qualify as substantial and therefore reportable, as well as those that would not qualify. Reportable events include any cyber incident that encrypts one of a covered entity's core business systems or information systems, the exploitation of a vulnerability resulting in the extended downtime a system or network, and intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, among others.
- CISA expects to publish a final rule in late 2025 and anticipates that covered entities will likely not begin submitting CIRCIA reports until 2026.

ACTION NEEDED: Deadlines and contacts

Please use the comment link below to respond to America's Credit Unions' survey. This will help shape the discussion and better address your needs in our comment letters.

- Comments due to America's Credit Unions: May 20, 2024 — **Submit here**
- Comments due to the CISA by June 3, 2024.
- Questions? Contact Andrew Morris, Senior Counsel for Research and Policy, America's Credit Unions
- Agency contact: Todd Klessman, CIRCIA Rulemaking Team Lead, 202-964-6869

QUESTIONS TO CONSIDER:

1. In certain cases, CISA's reporting framework may demand more forensic detail than the NCUA's cyber incident notification standard. How long does it generally take to assemble a preliminary forensic assessment of a cyber incident? Is 72 hours a realistic timeframe for assembling a report that meets CISA's requirements?
2. Comparing CISA's standard for reporting with the NCUA's notification rule in Part 748, would you anticipate needing to report a wider range of cyber incidents to CISA?

BACKGROUND:

Enacted in March 2022, the CIRCIA assigns to CISA the responsibility for implementing by 2025 a cyber reporting framework for critical infrastructure owners (covered entities). The statutory parameters for this framework require covered entities to report "substantial" cyberattacks to CISA within 72 hours after forming a "reasonable belief" that a covered incident has occurred, and supplemental reports as new information becomes available. In addition, covered entities must report any ransomware payments to CISA within 24 hours of payment.

The CIRCIA applies to covered entities that operate in critical infrastructure sectors, such as the financial sector. CISA's director is granted some discretion in terms of interpreting the scope of coverage and the CIRCIA's baseline definition of a substantial cyber incident.

In September 2023, the NCUA adopted new cyber incent notification rules in Part 748 of its regulations in response to CIRCIA's enactment. Under the NCUA's rule, a FICU that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the FICU reasonably believes that it has experienced such an incident. In general, the NCUA's rule is closely aligned with the CIRCIA's standard for what qualifies as a "substantial" and therefore reportable. However, the NCUA's rules do not adopt a separate ransom payment reporting requirement, which is a distinct component of the CIRCIA.

In general, the NCUA has characterized its current reporting framework as an early alert to the agency that does not demand a lengthy assessment of an incident. By contrast, CISA's proposal reaches further in terms of seeking more detailed forensic information and supplemental reporting. This discrepancy in terms of scope and intent could complicate FICUs' ability to utilize CIRCIA's exception for substantially similar reporting, a feature that would theoretically accommodate a single line of reporting to the NCUA and alleviate the burden of contacting CISA separately.

SECTION-BY-SECTION ANALYSIS:

A. Definitions

Section 226.1 of the proposal outlines key definitions, the most important of which are included below along with accompanying annotations. For a complete list, and the full text of the regulatory proposal, credit unions should consult the notice published on the Federal Register.

Covered entity means an entity that meets the criteria set forth in proposed § 226.2.

> NOTE: This term encompasses all FICUs per § 226.2(b)(7)(ii).

***C*overed cyber incident** means a *substantial cyber incident* experienced by a covered 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.
> >
> > > NOTE: *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.

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.

(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.

NOTE: *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.

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.

(6) The term "substantial cyber incident" **does not** include:

(i) Any lawfully authorized activity of a United States Government entity or [state, local, tribal, or territorial] 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).

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.

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.

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.

> NOTE**:** *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.

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.

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.

B. When to Report

For each of the reports covered in the proposal (collectively, CIRCIA Reports), certain timing and trigger requirements apply. These are discussed below:

Covered Cyber Incident Report. 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.

Ransom Payment Report. A covered entity must submit a Ransom Payment Report to CISA no later than 24 hours after the ransom payment has been disbursed.

Joint Covered Cyber Incident and Ransom Payment Report. 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.

Supplemental Reports. A covered entity must promptly submit Supplemental Reports to CISA about a previously reported covered cyber incident 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:

a. Substantial new or different information becomes available.
b. 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

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.

If a covered entity submits a supplemental report on a ransom payment made after the covered entity submitted a Covered Cyber Incident Report, the covered entity must submit the Supplemental Report to CISA no later than 24 hours after the ransom payment has been disbursed.

C. Content of Reports

In general, all CIRCIA Reports must include information sufficient to identify the covered entity, and any agent or third party submitting a report on the covered entity's behalf. This includes the following items:

§226.7 Required information for CIRCIA Reports.

(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.

In addition to general identifying information, a covered entity must also include specific information to the extent it is available and applicable to the type of cyber incident being reported. The chart below shows how certain categories of information are common across different reports.

§226.8 - Covered Cyber Incident	**§226.9 - Ransom Payment Report**	**§226.11 - Supplemental Report**
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;	Same categories, but specific to ransomware attack.	(a) 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

(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;		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.
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	Same but specific to ransomware attack.	
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	No similar category.	
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	Same but specific to ransomware attack.	

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	Same but specific to ransomware attack.	
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	Same but specific to ransomware attack.	
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	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	
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	Same but specific to ransomware attack.	
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;	Same but specific to ransomware attack.	
A description of any mitigation and response activities taken by the covered entity in response to the covered cyber incident	Same but specific to ransomware attack.	
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	Same but specific to ransomware attack.	

For Joint Covered Cyber Incident and Ransom 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.

§226.12 - Third party reporting procedures and requirements.

A covered entity may expressly authorize a third party to submit a CIRCIA Report on the covered entity's behalf to satisfy its 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 report on its behalf. 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.

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.

D. Comparison with NCUA Cyber Incident Notification Rule

The NCUA's cyber incident notification rule in 12 CFR § 784.1(c) is far less prescriptive than CISA's proposed reporting framework. The NCUA has provided guidance to FICUs regarding the content of cyber incident reports in Letter to Credit Unions 23-CU-07.

Each FICU 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. The NCUA must receive this notification as soon as possible but no later than 72 hours after a federally insured credit union reasonably believes that it has experienced a reportable cyber incident or, if reporting pursuant to paragraph (c)(1)(i)(C) of this section, within 72 hours of being notified by a third-party

Notably, the substantive contents of cyber incident reports sent to the NCUA are comparatively lighter than what CISA is proposing. NCUA guidance states that FICUs should be prepared to provide as much of the following information as is known at the time of reporting, including:

- When the credit union reasonably believed a reportable cyber incident took place; and

- A basic description of the reportable cyber incident, including what functions were, or are reasonably believed to have been affected or if sensitive information was compromised.

The NCUA also specifies in its guidance that at the time of initial notification, FICUs should not send the NCUA:

- Sensitive personally identifiable information;
- Indicators of compromise;
- Specific vulnerabilities; or
- Email attachments.

In effect, the NCUA's reporting framework operates more as an early warning mechanism rather than a detailed assessment, whereas CISA's proposal appears to demand more investigative rigor. However, CISA's reporting requirements are contingent on information being "available and applicable."

With respect to questions concerning vulnerabilities, defenses, or tactics, techniques and procedures, CISA recognizes that not all of this information will be immediately available. In the proposed rule's preamble, CISA recognizes that good faith answers of "unknown at this time" or something similar generally will be acceptable 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. As discussed in the proposed rule's preamble, 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.

E. Exception for Substantially Similar Reporting

The CIRCIA grants an exception for direct reporting to CISA if a covered entity 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. However, the exception would only apply if CISA has an information sharing agreement and mechanism in place with that Federal agency. For FICUs, the availability of the exception would depend on five conditions:

(1) the report must be required to contain substantially similar information to that required to be included in the applicable CIRCIA report;

> NOTE: The substantive reporting required by the NCUA in response to covered cyber incidents under Part 748 is not completely aligned with CISA's proposed rule.

(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;

> NOTE: 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.
>
> In the NCUA's case, a 72 hour period applies with respect to covered cyber incidents that are reportable under Part 748, but there is no 24-hour deadline or reporting requirements specific to ransom payments.

(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.

F. Record Keeping

A covered entity must comply with record preservation requirements in § 226.13 regardless of whether the covered entity submitted a CIRCIA Report or a third party submitted the CIRCIA Report on the covered entity's behalf. A covered entity is not required to create any data or records it does not already have in its possession based on this requirement.

In general, a covered entity must preserve the following data and records, to the extent they are available, for a period of two years:

(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.

Covered entities must preserve all data and records identified in the preceding paragraphs (§ 226.13(b)) for no less than two years from the submission of the most recently required CIRCIA Report submitted pursuant to § 226.3, 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.

G. Requests for Information and Subpoena Procedures

Under proposed § 226.14, CISA's 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 ransom payment.

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 would be served on a covered entity in accordance with the procedures in proposed § 226.14(e). In this event, the covered entity would need to 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 proposed §226.14(c)(2)(iv) or the Director determines that the covered entity's response is inadequate, the Director could request additional information from the covered entity to confirm whether a covered cyber incident or ransom payment occurred, or the Director could issue a subpoena to compel information from the covered entity.

A request for information would not be treated as a final agency action within the meaning of 5 U.S.C. 704 and could not be appealed.

The Director would also be permitted to issue a subpoena to compel disclosure of information from a covered entity if the entity fails to reply or provides an inadequate response to a request for information. 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. A covered entity would need to reply in the manner and format, and by the deadline, specified by the Director.

A covered entity could, however, appeal the issuance of a subpoena through a written request that the Director withdraw it. To do so, a covered entity, or a representative on behalf of the covered entity, would need to file a Notice of Appeal within seven (7) calendar days after service of the subpoena, and satisfy certain filing requirements outlined in proposed § 226.14(d)(7).

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.

Separately, under proposed § 226.20, CISA could apply criminal penalties under 18 U.S.C § 1001 (generally relating to false statements made to an agent of the government) if any person 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.

H. Confidentiality of Reports

CIRCIA Reports and responses provided to requests for information issued under § 226.14(c) would be treated as exempt from disclosure under the Freedom of Information Act (FOIA), 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.

Under the proposed rule, a covered entity would need to clearly designate with appropriate markings any responses 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, would be treated as commercial, financial, and proprietary information upon designation as such by a covered entity. If CISA receives a FOIA request to which a CIRCIA Report, response to a request for information under § 226.14(c), or information contained therein is responsive, CISA would apply all applicable exemptions from disclosure, consistent with Department of Homeland Security (DHS) rules for processing FOIA requests.

§ 226.18(c)(1) - Prohibition on use in regulatory actions.

Federal, State, Local, and Tribal Government entities would be prohibited from using information obtained solely through a CIRCIA Report 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.

§ 226.18(c)(2) – Liability protection.

In general, covered entities that submit CIRCIA reports would not face liability for the submission of a CIRCIA Report or a response to a request for information issued under § 226.14(c). As proposed, this liability protection would only apply to or affect 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). However, the liability protection would not apply to an action taken by the Federal government that relates to civil enforcement of a subpoena under § 226.15.

§ 226.18(c)(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;

PROPOSED EFFECTIVE DATE

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.