DEPARTMENT OF HOMELAND SECURITY

[Docket ID: CISA-2022-0010]

Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

AGENCY: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

ACTION: Request for information.

SUMMARY: The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this Request for Information (RFI) to receive input from the public as CISA develops proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Among other things, CIRCIA directs CISA to develop and oversee implementation of regulations requiring covered entities to submit to CISA reports detailing covered cyber incidents and ransom payments. CIRCIA requires CISA to publish a Notice of Proposed Rulemaking (NPRM) within 24 months of the date of enactment of CIRCIA as part of the process for developing these regulations. CISA is interested in receiving public input on potential aspects of the proposed regulation prior to publication of the NPRM and is issuing this RFI as a means to receive that input. While CISA welcomes input on other aspects of CIRCIA's regulatory requirements, CISA is particularly interested in input on definitions for and interpretations of the terminology to be used in the proposed regulations; the form, manner, content, and procedures for submission of reports required under CIRCIA; information regarding other incident reporting requirements including the requirement to report a description of the vulnerabilities exploited; and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulations.

DATES: Written comments are requested on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Submissions received after that date may not be considered.

ADDRESSES: You may submit comments, identified by Docket ID: CISA-2022-0010, through the *Federal eRulemaking Portal: http://www.regulations.gov*. Follow the instructions contained therein and below for submitting comments. Please note that this RFI period is not rulemaking,

and the Federal Rulemaking Portal is being utilized only as a mechanism for receiving comments.

FOR FURTHER INFORMATION CONTACT: Todd Klessman, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Rulemaking Team Lead, Cybersecurity and Infrastructure Security Agency, circia@cisa.dhs.gov, 202-964-6869.

SUPPLEMENTARY INFORMATION:

I. Public Participation

Interested persons are invited to comment on this notice by submitting written data, views, or arguments using the method identified in the **ADDRESSES** section. All members of the public, including but not limited to specialists in the field, academic experts, industry, public interest groups, and those with relevant economic expertise, are invited to comment.

Instructions: All submissions must include the agency name and Docket ID for this notice. Comments may be submitted electronically via the Federal e-Rulemaking Portal. To submit comments electronically:

1. Go to www.regulations.gov and enter CISA-2022-0010 in the search field,
2. Click the ‘‘Comment Now!’’ icon, complete the required fields, and
3. Enter or attach your comments.

All submissions, including attachments and other supporting materials, will become part of the public record and may be subject to public disclosure. The Cybersecurity and Infrastructure Security Agency (CISA) reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information or otherwise sensitive or protected information. All comments received will be posted to *http://www.regulations.gov*. Commenters are encouraged to identify the number of the specific topic or topics that they are addressing.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* and search for the Docket ID.

II. Background

The growing number of cyber incidents, including ransomware attacks, is one of the most serious economic and national security threats our nation faces. From the theft of private,

financial, or other sensitive data, to cyber-attacks that damage computer networks or facilitate the manipulation of operational or other control systems, cyber incidents are capable of causing significant, lasting harm.

Reporting cyber incidents and ransom payments to the government has many benefits. An organization that is a victim of a cyber incident, including those that result in ransom payments, can receive assistance from government agencies that are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents through analysis and sharing of cyber threat information. CISA and our federal law enforcement partners have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident, and providing technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. Timely reporting of incidents also allows CISA to share information about indicators of compromise, tactics, techniques, procedures, and best practices to reduce the risk of a cyber incident propagating within and across sectors.

Recognizing the importance of cyber incident and ransom payment reporting, in March 2022, Congress passed and President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, Div. Y (2022) (to be codified at 6 U.S.C. 681—681g). Enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, requiring CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA. These reports will allow CISA, in conjunction with other federal partners, to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks, and quickly share that information with network defenders to warn other potential victims.

Some of these new authorities are regulatory in nature and require CISA to complete rulemaking activities before the reporting requirements go into effect. CIRCIA requires that CISA develop and publish a Notice of Proposed Rulemaking (NPRM), which will be open to public comment, and a Final Rule. CIRCIA also mandates that CISA consult with various entities, including Sector Risk Management Agencies, the Department of Justice, and the DHS-chaired Cyber Incident Reporting Council, throughout the rulemaking process. CISA is working to complete these activities within the statutorily mandated timeframes. In addition to the

consultations required by CIRCIA, CISA is interested in receiving input from the public on the best approaches to implementing various aspects of this new regulatory authority.

III. Request for Input

A. Importance of Public Feedback

CISA is committed to obtaining public input in the development of its approach to implementation of the cyber incident and ransom payment reporting requirements of CIRCIA. Owners and operators of entities in critical infrastructure sectors will have particularly useful information, data, and perspectives on the different approaches to reporting requirements given the potential impact that these requirements may have on their organizations and industries. Accordingly, CISA is seeking specific public feedback to inform its proposed regulations to implement CIRCIA's regulatory requirements. All members of the public, including but not limited to specialists in the field, academic experts, industry, public interest groups, and those with relevant economic expertise, are invited to comment.

This notice contains a list of topics on which CISA believes inputs would be particularly useful in developing a balanced approach to implementation of the regulatory authorities Congress assigned to CISA under CIRCIA. CISA encourages public comment on these topics and any other topics commenters believe may be useful to CISA in the development of regulations implementing the CIRCIA authorities. The type of feedback that is most useful to the agency will identify specific approaches the agency may want to consider and provide information supporting why the approach would foster a cost-effective and balanced approach to cyber incident and ransom payment reporting requirements. Feedback that contains specific information, data, or recommendations is more useful to CISA than generic feedback that omits these components. For comments that contain any numerical estimates, CISA encourages the commenter to provide any assumptions made in calculating the numerical estimates.

B. List of Topics for Commenters

The below non-exhaustive list of topics is meant to assist members of the public in the formulation of comments and is not intended to restrict the issues that commenters may address:

(1) Definitions, Criteria, and Scope of Regulatory Coverage

a. The meaning of "covered entity," consistent with the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).

b. The number of entities, either overall or in a specific industry or sector, likely to be "covered entities" under the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).

c. The meaning of "covered cyber incident," consistent with the definition provided in section 2240(4), taking into account the requirements, considerations, and exclusions in section 2242(c)(2)(A), (B), and (C), respectively. Additionally, the extent to which the definition of "covered cyber incident" under CIRCIA is similar to or different from the definition used to describe cyber incidents that must be reported under other existing federal regulatory programs.

d. The number of covered cyber incidents likely to occur on an annual basis either in total or within a specific industry or sector.

e. The meaning of "substantial cyber incident."

f. The meaning of "ransom payment" and "ransomware attack," consistent with the definitions provided in section 2240(13) and (14).

g. The number of ransom payments likely to be made by covered entities on an annual basis.

h. The meaning of "supply chain compromise," consistent with the definition in section 2240(17).

i. The criteria for determining if an entity is a multi-stakeholder organization that develops, implements, and enforces policies concerning the Domain Name System (as described in section 2242(a)(5)(C)).

j. Any other terms for which a definition, or clarification of the definition for the term contained in CIRCIA, would improve the regulations and proposed definitions for those terms, consistent with any definitions provided for those terms in CIRCIA.

(2) Report Contents and Submission Procedures

a. How covered entities should submit reports on covered cyber incidents, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(4)), any specific

format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), any specific information that should be included in reports to facilitate appropriate sharing of reports among federal partners, and any other aspects of the process, manner, form, content, or other items related to covered cyber incident reporting that would be beneficial for CISA to clarify in the regulations.

b. What constitutes "reasonable belief" that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline for reporting covered cyber incidents under section 2242(a)(1).

c. How covered entities should submit reports on ransom payments, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(5)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), and any other aspects of the process, manner, form, content, or other items related to ransom payments that would be beneficial for CISA to clarify in the regulations.

e. When should the time for the 24-hour deadline for reporting ransom payments begin (i.e., when a ransom payment is considered to have been "made").

f. How covered entities should submit supplemental reports, what specific information should be included in supplemental reports, any specific format or manner in which supplemental report information should be submitted, the criteria by which a covered entity determines "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved," and any other aspects of the process, manner, form, content, or other items related to supplemental reports that would be beneficial for CISA to clarify in the regulations.

g. The timing for submission of supplemental reports and what constitutes "substantial new or different information," taking into account the considerations in section 2242(c)(7)(B) and (C).

h. What CISA should consider when "balanc[ing] the need for situational awareness with the ability of the covered entity to conduct cyber incident

response and investigations" when establishing deadlines and criteria for supplemental reports.

i. Guidelines or procedures regarding the use of third-party submitters, consistent with section 2242(d).

j. Covered entity information preservation requirements, such as the types of data to be preserved, how covered entities should be required to preserve information, how long information must be preserved, allowable uses of information preserved by covered entities, and any specific processes or procedures governing covered entity information preservation.

k. To clarify or supplement the examples provided in section 2242(d)(1), what constitutes a third-party entity who may submit a covered cyber incident report or ransom payment report on behalf of a covered entity.

l. How a third party can meet its responsibility to advise an impacted covered entity of its ransom payment reporting responsibilities under section 2242(d)(4).

(3) Other Incident Reporting Requirements and Security Vulnerability Information Sharing

a. Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements.

b. What federal departments, agencies, commissions, or other federal entities receive reports of cyber incidents or ransom payments from critical infrastructure owners and operators.

c. The amount it typically costs and time it takes, including personnel salary costs (with associated personnel titles if possible), to compile and report information about a cyber incident under existing reporting requirements or voluntary sharing, and the impact that the size or type of cyber incident may have on the estimated cost of reporting.

d. The amount it costs per incident to use a third-party entity to submit a covered cyber incident report or ransom payment report on behalf of a covered entity.

e. The amount it typically costs to retain data related to cyber incidents.

f. Criteria or guidance CISA should use to determine if a report provided to another federal entity constitutes "substantially similar reported information."

g. What constitutes a "substantially similar timeframe" for submission of a report to another federal entity.

h. Principles governing the timing and manner in which information relating to security vulnerabilities may be shared, including any common industry best practices and United States or international standards.

(4) Additional Policies, Procedures, and Requirements

a. Policies, procedures, and requirements related to the enforcement of regulatory requirements, to include the issuance of requests for information, subpoenas, and civil actions consistent with section 2244.

b. Information on protections for reporting entities under section 2245.

c. Any other policies, procedures, or requirements that it would benefit the regulated community for CISA to address in the proposed rule.

CISA notes that this RFI is issued solely for information and program-planning purposes. Responses to this RFI do not bind CISA to any further actions.

Jennie M. Easterly,
Director,
Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2022-19551 Filed: 9/9/2022 8:45 am; Publication Date: 9/12/2022]