DEPARTMENT OF HOMELAND SECURITY

[Docket ID: CISA-2022-0010]

Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions

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

ACTION: Notice of public listening sessions.

SUMMARY: The Cybersecurity and Infrastructure Security Agency (CISA) is announcing a series of public listening sessions to receive input as CISA develops proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CISA is interested in receiving public input on potential aspects of the proposed regulations prior to their publication in a Notice of Proposed Rulemaking (NPRM), and issued a request for information in the *Federal Register* on [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*] (the "RFI") as a means to receive that input. These public listening sessions are intended to serve as an additional means for interested parties to provide input to CISA on the topics identified in the RFI prior to the publication of the NPRM.

DATES: Public listening sessions are scheduled to be held on the following dates at the following locations:

Salt Lake City, Utah—September 21, 2022; Taylorsville State Office Building, 4315 S 2700 W, Taylorsville, UT 84129.

Atlanta, Georgia—September 28, 2022; Georgia Emergency Management Administration Building, 935 United Avenue SE, Atlanta, GA 30316.

Chicago, Illinois—October 5, 2022; 536 S. Clark / 101 W. Ida B. Wells Federal Building, USCIS Auditorium, 536 S. Clark Street / 101 W. Ida B. Wells Drive, Chicago, IL 60605.

Dallas/Fort Worth, Texas—October 5, 2022; Fritz G. Lanham Federal Building, 819 Taylor Street, Fort Worth, TX 76102.

New York, New York—October 12, 2022; Alexander Hamilton U.S. Custom House Smithsonian Museum of the American Indian, 1 Bowling Green, New York, NY 10004.

Philadelphia, Pennsylvania—October 13, 2022; Federal Reserve Bank, 10 N. Independence Mall, W Philadelphia, PA 19106.

Oakland, California—October 26, 2022; Ronald V. Dellums Federal Building, 1301 Clay Street, Oakland, CA 94612.

Boston, Massachusetts—November 2, 2022; Tip O'Neill Federal Building, 10 Causeway, Boston, MA 02222.

Seattle, Washington—November 9, 2022; Henry Jackson Federal Building, 915 2nd Avenue, Seattle, WA 98104.

Kansas City, Missouri—November 16, 2022; Two Pershing Square, 2300 Main Street, Kansas City, MO 64108.

CISA also plans to host a listening session in Washington, D.C.; however, a date and location for that session has not yet been finalized. CISA will publish a supplemental notice in the *Federal Register* containing the date and location of the Washington, D.C. listening session once those details have been finalized.

All of the listening sessions are tentatively scheduled to occur from 11 a.m. – 3 p.m. local time. CISA reserves the right to reschedule, move to virtual, or cancel any of these sessions for any reason, including a health emergency, severe weather, or an incident that impacts the ability of CISA to safely conduct these sessions in person at the proposed date, time, and location. Any changes or updates to dates, locations, or start and end times for these listening sessions, to include the date and location for the Washington, D.C. listening session, will be posted on www.cisa.gov/circia.

CISA is committed to ensuring all participants have equal access to these sessions regardless of disability status. If you require reasonable accommodation due to a disability to fully participate, please contact CISA at circia@cisa.dhs.gov or (202) 964-6869 as soon as possible prior to the session you wish to attend.

Registration is encouraged for these public listening sessions and priority access will be given to individuals who register. To register, please visit www.cisa.gov/circia and follow the instructions available there to complete registration. Registration for each in-person listening session will be accepted until 5 p.m. (eastern daylight time) two days before the listening session.

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. 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. To help support the gathering of this input, on [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], CISA published a Request for Information in the *Federal Register*.

II. Purpose

These public listening sessions are intended to serve as an additional means for interested parties to provide input to CISA on aspects of the proposed regulations prior to the publication of the NPRM. 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. Key areas within these four topical areas on which CISA is particularly interested in receiving stakeholder input are enumerated in section IV below.

III. Public Listening Session Procedures and Participation

As the sole intent of the public listening sessions is to allow the general public to provide input to CISA on aspects of potential approaches to implementing CIRCIA's regulatory requirements, the sessions have been designed to facilitate one-way communication. Outside of introductory and logistical remarks, CISA will not be providing substantive information on CIRCIA or potential content of the NPRM, or responding to comments during the public listening sessions. Each listening session is open to the public and each is expected to last up to a total of four hours. To allow as many members of the public as possible to speak, we are requesting speakers limit their remarks to three minutes. Attendance at these listening sessions will be capped consistent with room capacity limitations at each location. Participants are encouraged to register for their desired session via an on-line registration form available at www.cisa.gov/circia. Registered individuals will be provided priority access to the room and the

opportunity to speak before individuals who did not register. Please note that a public meeting may adjourn early if all commenters present have had the opportunity to speak prior to the scheduled conclusion of the meeting. All comments made during the sessions will be documented and transcribed by CISA. A final transcript of each of these sessions will be provided in the electronic docket for the CIRCIA rulemaking, docket **CISA-2022-0010**, available at http://www.regulations.gov.

CISA also plans on holding sector-specific listening sessions at dates and times to-be-determined. Information about those listening sessions will be available on www.cisa.gov/circia when it becomes available. Feedback from those listening sessions will be added to the rulemaking docket for public consideration. Additionally, written comments on proposed elements of the CIRCIA regulations may also be submitted in response to CISA's RFI via the Federal eRulemaking Portal identified by docket number **CISA-2022-0010** through the duration of the RFI's comment period.

IV. Key Inputs Solicited by the Agency

The below non-exhaustive list of topics, which mirrors those contained in the RFI, 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.

d. 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").

e. 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.

f. 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).

g. 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.

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

i. 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.

j. 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.

k. 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 these public meetings are being held solely for information and program-planning purposes. Inputs provided during the public meetings do not bind CISA to any further actions.

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

[FR Doc. 2022-19550 Filed: 9/9/2022 8:45 am; Publication Date: 9/12/2022]