CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA)

All organizations are encouraged to share information about unusual cyber activity and/or cyber incidents 24/7 via report@cisa.gov or (888) 282-0870.

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, requiring the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.

Rulemaking Process

These new authorities are regulatory in nature and require CISA to complete mandatory rulemaking activities before the reporting requirements go into effect. CIRCIA requires CISA to develop and publish a Notice of Proposed Rulemaking (NPRM), which will be open for public comment, and a Final Rule. CIRCIA also mandates that CISA consult with various entities throughout the rulemaking

process, including Sector Risk Management Agencies, the Department of Justice, other appropriate Federal agencies, and a soon-to-be formed, DHS-chaired Cyber Incident Reporting Council. This work is already underway.

CISA is committed to receiving inputs into the NPRM from other stakeholders as well, such as critical infrastructure owners and operators and other members of the potentially regulated community, while maintaining the rulemaking schedule required by statute.

Request for Information

CISA has released a Request for Information (RFI) through which we are soliciting public input for 60 days, starting September 12, 2022, on potential aspects of the proposed regulation prior to publication of the NPRM.

This public input from our critical infrastructure partners will help us understand how we can implement the new cyber incident reporting legislation in the most effective way possible to protect the nation's critical infrastructure.

The RFI has been published in the Federal Register site, along with a notice of public listening sessions.

CISA is particularly interested in input on definitions for and interpretations of the terminology to be used in the proposed regulations, as well as the form, manner, content, and procedures for submission of reports required under CIRCIA.

In addition, CISA is also interested in information regarding other incident reporting requirements and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulations.

There are two ways to provide input on the rulemaking process:

- Provide written comments in response to the Request for Information by November 14, 2022
- Participate in one of the listening sessions that CISA will be hosting around the country

Schedule of Public Listening Sessions

CISA will be hosting in person listening sessions around the country. Dates, times and locations for each of the listening schedules is provided below.

Registration is encouraged for the public listening sessions and priority access will be given to individuals who register. To register for a listening session, please click on the link "Register Here" below and follow the instructions provided. Registration for each session will be accepted until 5:00 p.m. (Eastern Daylight Time) two days before the listening session.

UPDATE: The September 28 session scheduled for Atlanta, GA, has been cancelled due to hurricane preparations at the venue. Participants are encouraged to submit written input via the Request for Information.

REGISTER HERE

City	Date	Time	Location
Salt Lake City, Utah	September 21, 2022	11 a.m. - 3 p.m.	Taylorsville State Office Building, 4315 S 2700 W, Taylorsville, UT 84129
*** CANCELLED* ~~Atlanta, Georgia~~**	~~September 28, 2022~~	~~11 a.m. - 3 p.m.~~	~~Georgia Emergency Management Administration Building, 935 United Ave SE, Atlanta GA, 30316~~
Chicago, Illinois	October 5, 2022	11 a.m. - 3 p.m.	Federal Building, USCIS Auditorium, 536 S. Clark Street, Chicago, IL 60605
Dallas/Fort Worth, Texas	October 5, 2022	11 a.m. - 3 p.m.	Fritz G. Lanham Federal Building, 819 Taylor Street, Fort Worth, TX 76102
New York, New York	October 12, 2022	11 a.m. - 3 p.m.	Alexander Hamilton U.S. Custom House Smithsonian Museum of the American Indian, 1 Bowling Green, New York, NY 10004
Philadelphia, Pennsylvania	October 13, 2022	11 a.m. - 3 p.m.	Federal Reserve Bank 10 N. Independence Mall, W Philadelphia, PA 19106
Oakland, California	October 26, 2022	11 a.m. - 3 p.m.	Ronald V. Dellums Federal Building, 1301 Clay Street, Oakland, CA 94612
Boston, Massachusetts	November 2, 2022	11 a.m. - 3 p.m.	Tip O'Neill Federal Building, 10 Causeway, Boston, MA 02222
Seattle, Washington	November 9, 2022	11 a.m. - 3 p.m.	Henry Jackson Federal Building, 915 2nd Avenue, Seattle, WA 98104
Kansas City, Missouri	November 16, 2022	TB 11 a.m. - 3 p.m. D	Two Pershing Square, 2300 Main Street, Kansas City, MO 64108

City	Date	Time	Location
Washington, DC	October 19, 2022	11 a.m. - 3 p.m.	Metropolitan Washington Council of Governments, 777 North Capitol Street NE, Suite 300, Washington, DC 20002

Voluntary Sharing of Information about Cyber Incidents

While covered cyber incident and ransomware payment reporting under CIRCIA will not be required until the Final Rule implementing CIRCIA's reporting requirements goes into effect, CISA encourages critical infrastructure owners and operators to voluntarily share with CISA information on cyber incidents prior to the effective date of the final rule.

When information about cyber incidents is shared quickly, CISA can use this information to render assistance and provide warning to prevent other organizations from falling victim to a similar incident. This information is also critical to identifying trends that can help efforts to protect the homeland.

CISA encourages all organizations to share information about unusual cyber activity and/or cyber incidents 24/7 via report@cisa.gov or (888) 282-0870. To learn more about how Observe, Act, and Report cyber incidents, view our fact sheet on Sharing Cyber Event Information.

Expand All Sections

Additional Resources:

Background and Facts About CIRCIA

Frequently Asked Questions (FAQ)

For Media Inquiries