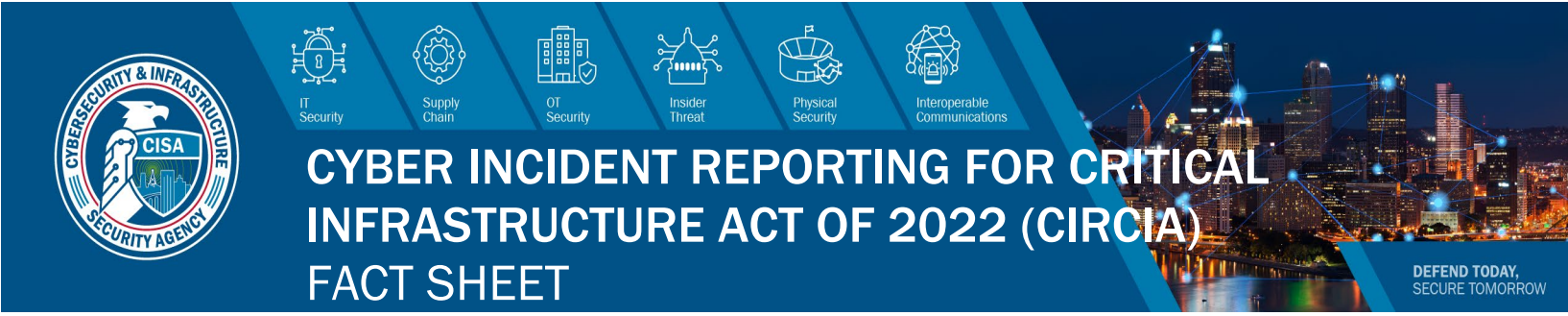

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA) FACT SHEET

ORGANIZATIONS CAN SHARE INFORMATION ABOUT UNUSUAL CYBER ACTIVITY AND/OR CYBER INCIDENTS TO REPORT@CISA.GOV OR (888) 282-0870.

BACKGROUND

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 to CISA covered cyber incidents and ransom payments. 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.

CYBER INCIDENT REPORTING INITIATIVES

CIRCIA includes a number of requirements related to the required reporting and sharing of covered cyber incidents, to include the following:

- Cyber Incident Reporting Requirements: CIRCIA requires CISA to develop and issue regulations requiring covered entities to report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred.
- Federal Incident Report Sharing: Any federal entity receiving a report on a cyber incident after the effective date of the final rule must share that report with CISA within 24 hours. CISA will also have to make information received under CIRCIA available to certain federal agencies within 24 hours.
- Cyber Incident Reporting Council: DHS must establish and Chair an intergovernmental Cyber Incident Reporting Council (Council) to coordinate, deconflict, and harmonize federal incident reporting requirements.

RANSOMWARE INITIATIVES

CIRCIA additionally authorizes or requires a number of initiatives related to combatting ransomware, to include the following:

- Ransom Payment Reporting Requirements: CIRCIA requires CISA to develop and issue regulations requiring covered entities to report to CISA within 24 hours of making any ransom payments made as a result of a ransomware attack. CISA must share such reports with federal agencies, similar to above.
- Ransomware Vulnerability Warning Pilot Program: CISA must establish a pilot to identify systems with vulnerabilities to ransomware attacks and may notify the owners of those systems.
- Joint Ransomware Task Force: CISA has announced the launch of the Joint Ransomware Task Force in accordance with the statute to build on the important work that has already begun to coordinate an ongoing nationwide campaign against ransomware attacks. CISA will continue working closely with the Federal Bureau of Investigation and the National Cyber Director to build the task force.

IMPLEMENTING CIRCIA'S REPORTING REQUIREMENT

- Some of the new authorities are regulatory in nature and require CISA to complete rulemaking activities before the reporting requirements go into effect.
- As part of the rulemaking process, CIRCIA requires CISA to publish a Notice of Proposed Rulemaking (NPRM) within 24 months of the enactment of CIRCIA, and to issue a Final Rule setting forth the regulatory requirements within 18 months of the publication of the NPRM.
- CIRCIA also mandates that CISA consult with various entities throughout the rulemaking process, including Sector Risk Management Agencies (SRMAs), the Department of Justice (DOJ), other appropriate Federal agencies, and the Council.
- As CISA wants to ensure that the proposed rule benefits from the perspectives of our broad partner community, CISA will also be publishing a Request for Information later this year in the Federal Register, and will also be hosting a series of listening sessions where stakeholders will be able to provide thoughts on the statutory requirements directly to members of CISA.

SHARING INFORMATION WITH CISA ABOUT CYBER INCIDENTS OR RANSOM PAYMENTS

- Until the effective date of the Final Rule, organizations are not required to submit cyber incident or ransom payment reports under CIRCIA.
- However, CISA strongly encourages organizations to continue voluntarily sharing cyber event information with CISA throughout the rulemaking period prior to the Final Rule's effective date.
- When information about cyber incidents is shared quickly, we 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.

HOW TO SHARE INFORMATION ABOUT A CYBER INCIDENT

- When information about cyber incidents is shared quickly, we 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.
- Organizations can share information about unusual cyber activity and/or cyber incidents to report@cisa.gov or (888) 282-0870.
- Additional information on sharing information about unusual cyber activity or incidents can be found here.

LEARN MORE ABOUT CIRCIA

Visit cisa.gov/CIRCIA or contact CIRCIA@cisa.dhs.gov. For media inquiries, please contact CISA Media at CISAMedia@cisa.dhs.gov.