2023 CHEMICAL SECURITY SUMMIT

August 29-31, 2023

#ChemicalSecurity

CHEMICAL SECURITY SUMMIT

August 31, 2023

Cyber Regulations at Chemical Facilities

Todd Klessman
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking Team Lead, CISA

CAPT Andy Meyers
Chief, Office of Port & Facility Compliance, United States Coast Guard

Ronald Pavlik
Deputy Assistant Administrator
Surface Operations, Transportation Security Administration

Moderator: Annie Hunziker Boyer
Chief, Policy, Rulemaking, and Engagement Branch
CISA Chemical Security

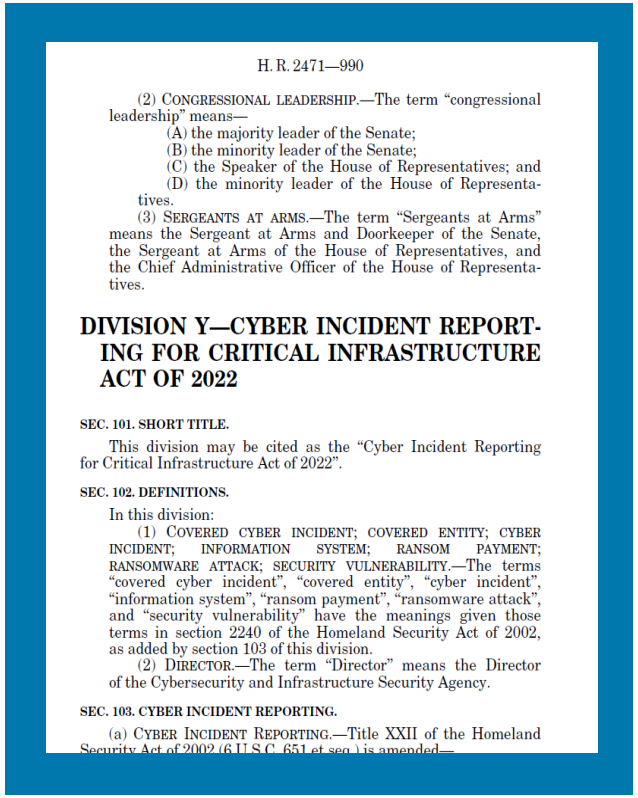
#ChemicalSecurity

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

August 2023

CIRCIA Overview

- In March 2022, Congress enacted the ***Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)***



H. R. 2471—990

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" means—
(A) the majority leader of the Senate;
(B) the minority leader of the Senate;
(C) the Speaker of the House of Representatives; and
(D) the minority leader of the House of Representatives.
(3) SERGEANTS AT ARMS.—The term "Sergeants at Arms" means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 101. SHORT TITLE.

This division may be cited as the "Cyber Incident Reporting for Critical Infrastructure Act of 2022".

SEC. 102. DEFINITIONS.

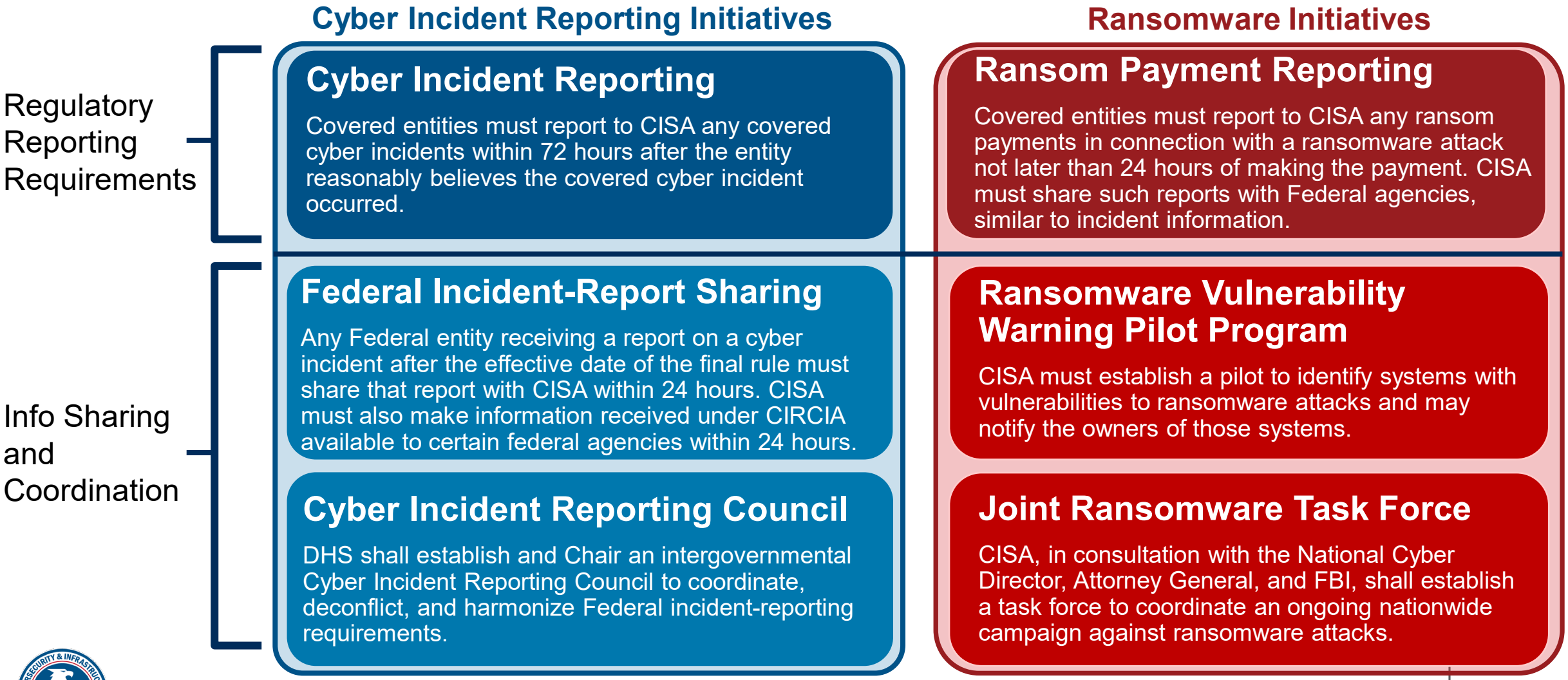
In this division:
(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms "covered cyber incident", "covered entity", "cyber incident", "information system", "ransom payment", "ransomware attack", and "security vulnerability" have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.
(2) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

SEC. 103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

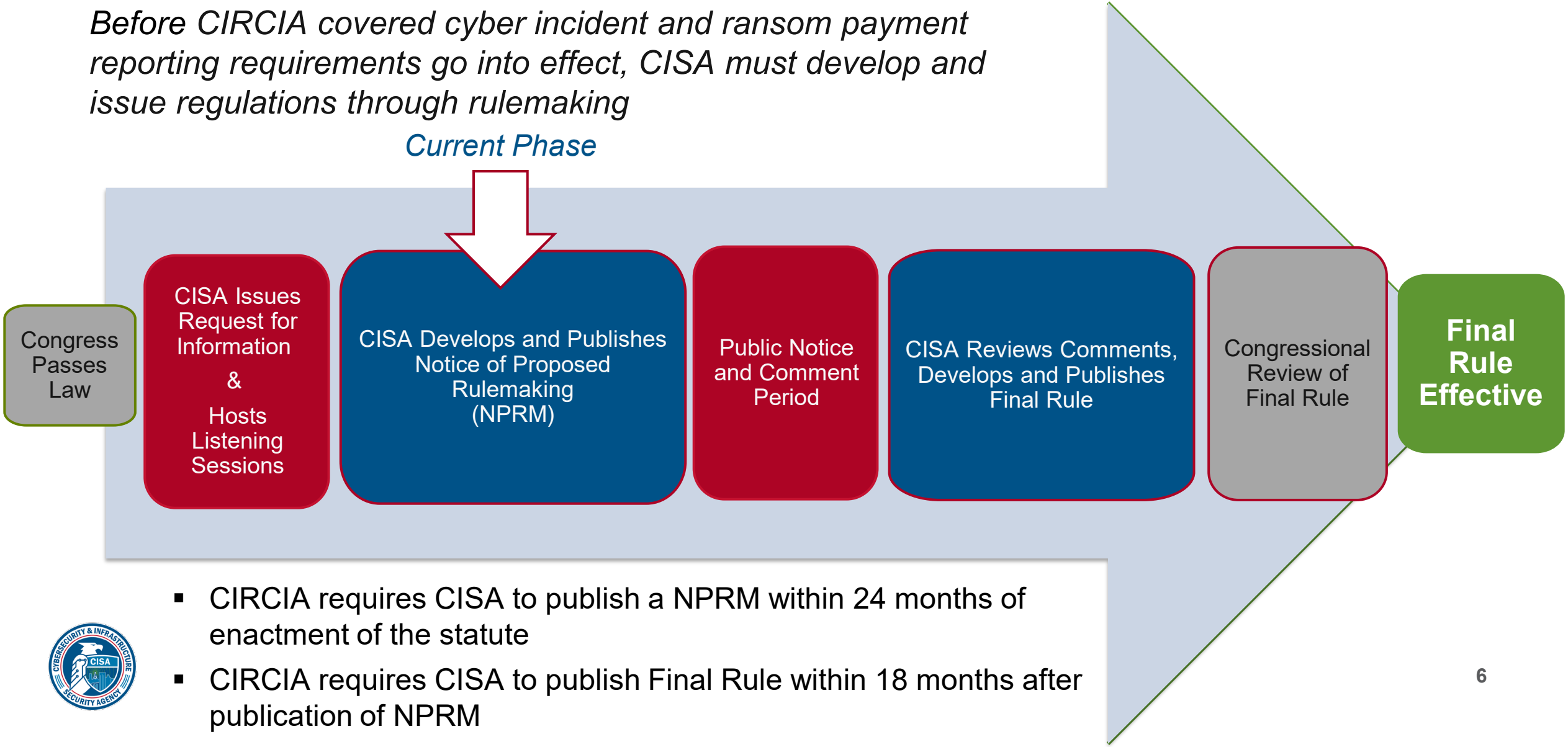
- Codified in 6 U.S.C. 681-681g
- Requires the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate with Federal partners and others on various cyber incident reporting and ransomware-related activities
- Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity-related events

CIRCIA Key Elements



CIRCIA Rulemaking Schedule

Before CIRCIA covered cyber incident and ransom payment reporting requirements go into effect, CISA must develop and issue regulations through rulemaking



- CIRCIA requires CISA to publish a NPRM within 24 months of enactment of the statute
- CIRCIA requires CISA to publish Final Rule within 18 months after publication of NPRM

Required NPRM Content

The following are some of the topics CISA must address in the NPRM

- Definition of “Covered Entity” (i.e., who is required to report covered cyber incidents and ransom payments to CISA)
- Definition of “Covered Cyber Incident” (i.e., what cyber incidents must be reported to CISA)
- Statutory reporting exceptions
- Manner, form, and content of reports
- Deadlines and criteria for supplemental reporting
- Third-party reporting
- Data preservation requirements
- Enforcement mechanisms
- Privacy and civil liberties protections

Stakeholder Engagement

CIRCIA requires CISA to engage certain stakeholders during the rulemaking process.

Federal Consultations

- As required by the statute, CISA has consulted with more than two dozen Federal partners, including the Sector Risk Management Agencies, the Department of Justice, and other Federal agencies with equities in cyber incident reporting
- CISA has also consulted with the Cyber Incident Reporting Council to explore ways to harmonize and minimize potentially duplicative regulatory burdens

State, Local, and Private Sector Engagement

- CIRCIA does not require engagement with non-Federal entities prior to publication of the NPRM; however, CISA is committed to providing stakeholders from across the spectrum with the opportunity to provide ideas and perspectives, within the limitations of the rulemaking process and timeline itself
- To achieve this:
  - On September 12, 2022, CISA released a Request for Information (RFI) providing an opportunity for stakeholders to provide comments in writing
  - CISA also hosted ten in-person and seventeen virtual listening sessions

Outreach and Education Campaign

- Following issuance of the Final Rule, CISA is required to undertake an outreach and education campaign to inform the regulated community of the new reporting requirements, how to submit reports, protections afforded under CIRCIA, and other topics

RFI and Listening Session Results

Key perspectives provided by stakeholders in response to the RFI and during listening sessions

- CISA received approximately 130 written submissions in response to the RFI, had over 150 individuals attend the in-person listening sessions, and hundreds more participated in the virtual listening sessions
  - All written comments and transcripts of the listening sessions have been posted to the docket for the CIRCIA rulemaking at regulations.gov and can be found by searching for CISA-2022-0010
- Some of the themes that emerged from stakeholder comments included:
  - The importance of clarity in key definitions such as “covered entity” and “covered cyber incident”
  - The desire for the Federal government to harmonize CIRCIA with other cyber incident reporting regulatory regimes and avoid entities having to report to multiple Agencies
  - A desire for strong protection of information contained in reports
  - The importance of sharing with the public and private sector entities the results of the assessments, analysis, etc. that CISA performs based on the reports

Voluntary Sharing of Incident Information

CISA encourages organizations to begin or continue voluntarily sharing information about cyber incidents while CIRCIA reporting requirements are developed

- Organizations are not required to submit cyber incident or ransom payment reports to CISA under CIRCIA until the effective date of the Final Rule
- CISA encourages organizations to begin or continue voluntarily sharing cyber incident information with CISA throughout the rulemaking period prior to the effective date of the Final Rule
  - When cyber incidents are reported 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
- Organizations can share information about unusual cyber activity and/or cyber incidents to **report@cisa.gov** or **(888) 282-0870**

For more information:
CISA.gov/CIRCIA

For questions:
CIRCIA@cisa.dhs.gov