

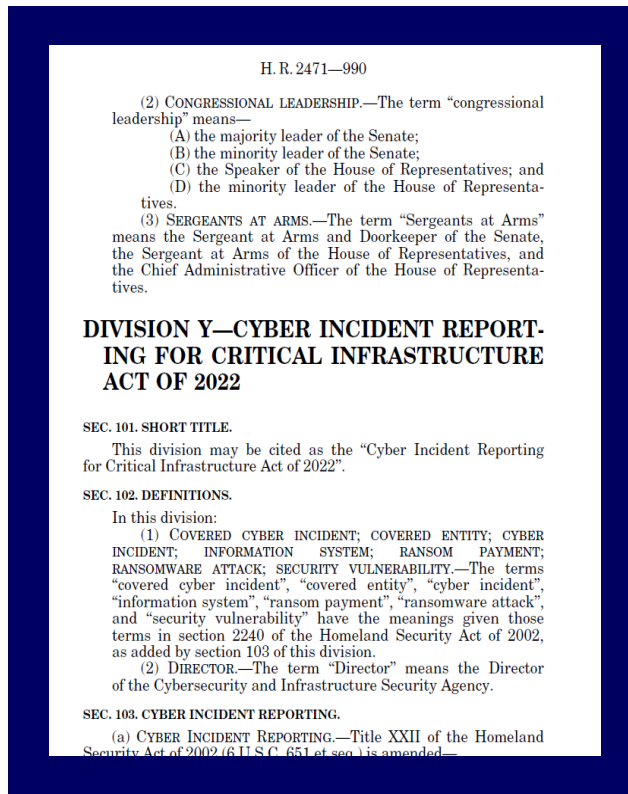
# CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

June 2022



# CIRCIA Overview

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



- 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 items



# CIRCI Key Elements

## Cyber Incident Reporting Initiatives

## Ransomware Initiatives

Regulatory Reporting Requirements

### Cyber Incident Reporting

Covered entities must report to CISA any covered cyber incidents within 72 hours after the entity reasonably should have believed the covered cyber incident occurred

### Ransomware Payment Reporting

Covered entities must report to CISA any ransomware payments within 24 hours of making the payment. CISA must share such reports with Federal agencies, similar to incident information

Info Sharing and Coordination

### 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 CIRCI available to certain federal agencies within 24 hours.

### Ransomware Vulnerability Warning Pilot Program

CISA must establish a pilot to identify systems with vulnerabilities to ransomware attacks and notify the owners of those systems

### Cyber Incident Reporting Council

DHS will establish and Chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize Federal incident reporting requirements

### Joint Ransomware Task Force

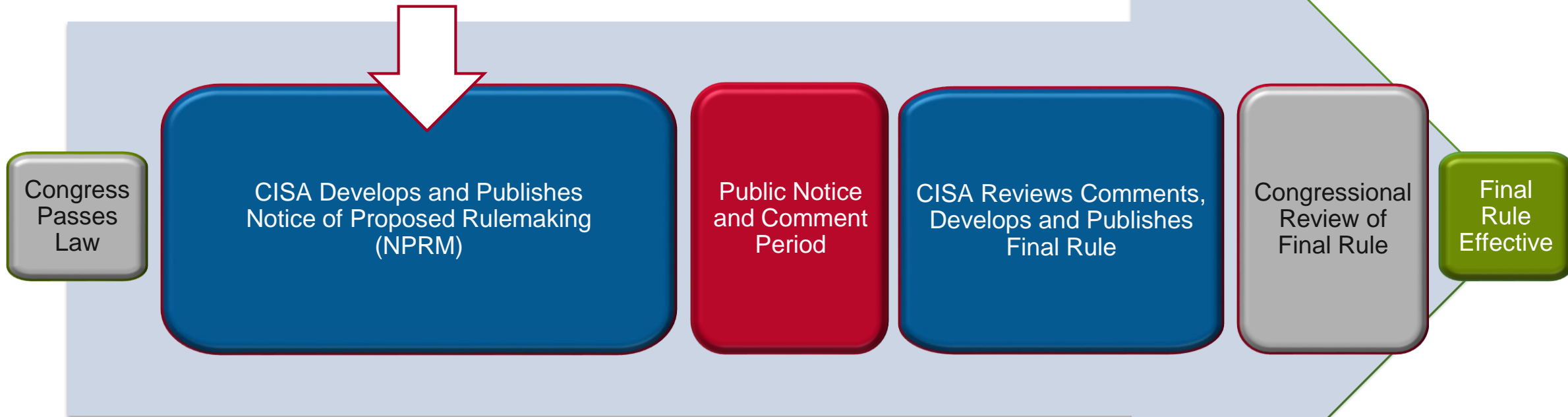
CISA, in consultation with the National Cyber Director, Attorney General, and FBI, shall establish a task force to coordinate an ongoing nationwide campaign against ransomware attacks



# CIRCI A Rulemaking Process

*Before CIRCI A covered cyber incident and ransomware payment reporting requirements go into effect, CISA must develop and issue regulations*

*Current Phase*



- CIRCI A requires that CISA publish a Notice of Proposed Rulemaking (NPRM) within 24 months of enactment of the statute
- CIRCI A also requires CISA to publish Final Rule within 18 months after publication of NPRM



# Voluntary Sharing of Incident Information

CISA encourages organizations to continue voluntarily reporting cyber incidents while CIRCIA reporting requirements are developed.

- Organizations are not required to submit cyber incident or ransomware payment reports to CISA until the yet-to-be-determined effective date of the Final Rule.
- CISA encourages organizations to continue voluntarily sharing cyber event 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 attack. This information is also critical to identifying trends that can help efforts to protect the homeland.
- Organizations can report unusual cyber activity and/or cyber incidents to [report@cisa.gov](mailto:report@cisa.gov) or (888) 282-0870.





For more information:  
[CISA.gov/CIRCIACIA](https://www.cisa.gov/CIRCIACIA)

For questions:  
[CIRCIACIA@cisa.dhs.gov](mailto:CIRCIACIA@cisa.dhs.gov)