CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

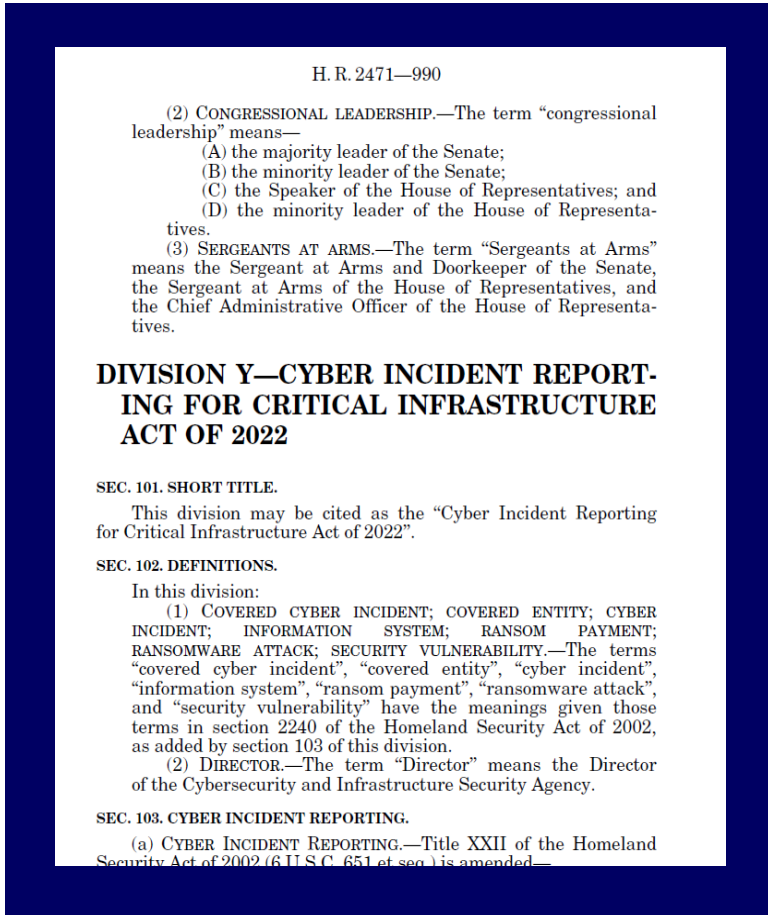
CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

NOTICE OF PROPOSED RULEMAKING INFORMATIONAL OVERVIEW

May 2024

Statutory Authority

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



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.

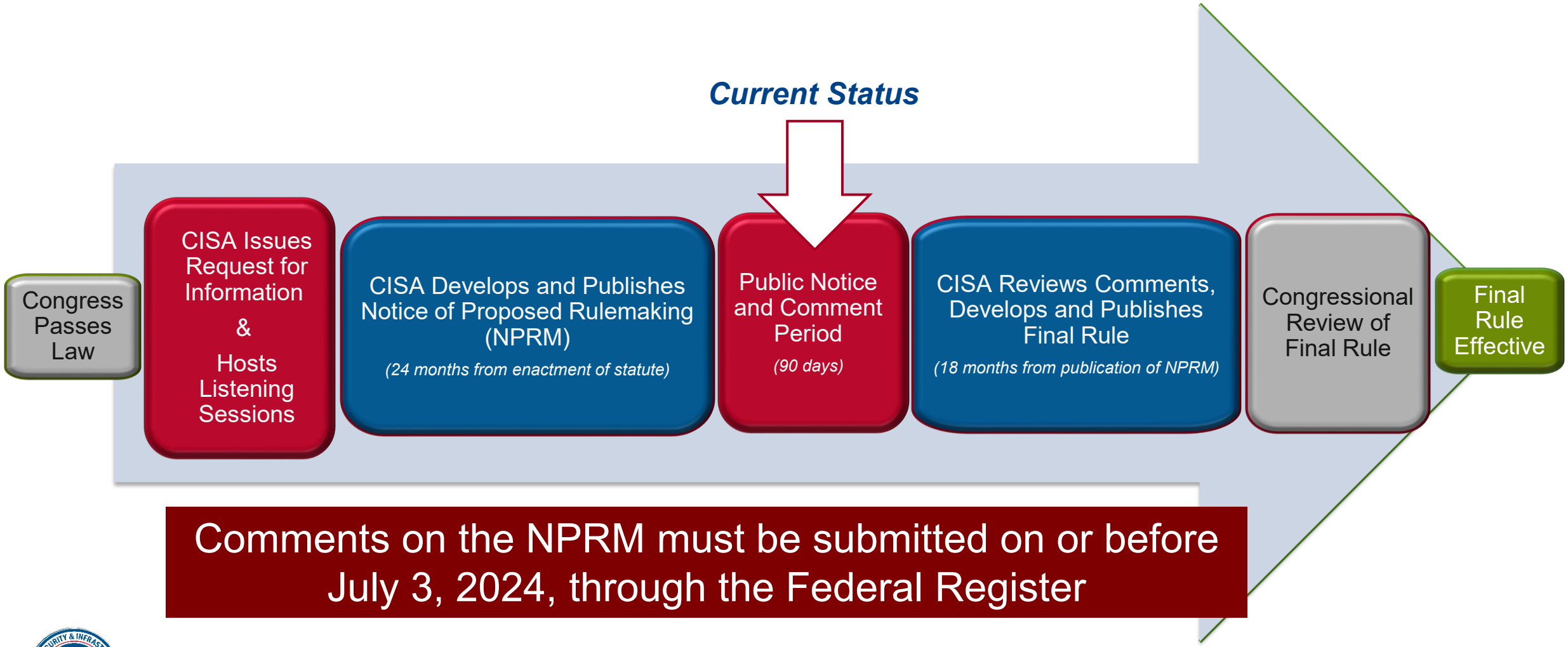
SEC. 103. CYBER INCIDENT REPORTING.

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

Key Proposed Regulatory Requirements

- **Covered Cyber Incident Reporting**
  - A Covered Entity that experiences a Covered Cyber Incident must report it to CISA no later than 72 hours after the Covered Entity reasonably believes the incident has occurred
- **Ransom Payment Reporting**
  - A Covered Entity that makes a Ransom Payment, or has another entity make one on its behalf, as the result of a Ransomware Attack, must report it to CISA no later than 24 hours after the payment has been disbursed
- **Supplemental Reporting**
  - A Covered Entity must promptly submit a supplemental report to CISA in two circumstances:
    - Substantial new or different information about a previously reported Covered Cyber Incident becomes available
    - The entity, or another entity on its behalf, makes a Ransom Payment related to a previously reported Covered Cyber Incident
- **Data and Records Preservation**
  - A Covered Entity that is required to submit a CIRCIA Report must preserve certain data and records

CIRCIA Rulemaking Schedule



Comments on the NPRM must be submitted on or before July 3, 2024, through the Federal Register

NPRM Package Overview

The CIRCIA NPRM Package consists of three documents:

1. **Notice of Proposed Rulemaking**
   - Preamble: An explanation of what CISA is proposing, why, and what other approaches CISA considered
   - Regulatory Text: The language proposed for inclusion in the Code of Federal Regulations

2. **Preliminary Regulatory Impact Analysis (RIA)**
   - Preliminary economic analysis of the proposed regulations, which is required by law and Executive Order, including a cost-benefit analysis

3. **Draft Privacy and Civil Liberties Guidance**
   - CISA's draft of the privacy and civil liberties guidance governing the submission, receipt, retention, use, and dissemination of information contained in CIRCIA Reports and responses to CIRCIA Requests for Information, which CISA was required to develop by CIRCIA

All three documents are available for public review and comment in the CIRCIA docket on www.regulations.gov

Core Content of Proposed Regulations

- **Definition of "Covered Entity" and Applicability Criteria** (i.e., who is required to report Covered Cyber Incidents and Ransom Payments to CISA)
- **Definition of "Covered Cyber Incident"** (i.e., what incidents must be reported to CISA)
- **Reporting Requirements and Exceptions**
- **Report Submission Deadlines**
- **Manner, Form, and Content of CIRCIA Reports**
- **Third-Party Reporting Procedures**
- **Data and Records Preservation Requirements**
- **Enforcement Mechanisms**
- **Information Protections and Restrictions on Use**

Who the Regulation Applies to (1 of 3)

- **Statutory Parameters**
  - CIRCIA defines a Covered Entity as “an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule”
  - CIRCIA also requires that CISA include in the rule a description of the types of entities that constitute covered entities based on:
    - the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;
    - the likelihood that such an entity may be targeted by a malicious cyber actor; and
    - the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure

- **NPRM Proposed Applicability Criteria for Covered Entities**
  - Any entity in a critical infrastructure sector that either:
    - Exceeds the applicable small business size standard established by the Small Business Administration for its industry or
    - Meets one or more of the sector-based criteria (regardless of the specific critical infrastructure sector the entity considers itself to be part of)

Who the Regulation Applies to (2 of 3)

- **High-Level Summary of Sector-Based Criteria**
  - ***Chemical***: *Owns/operates a Chemical Facility Anti-Terrorism Standards covered chemical facility (or, alternatively, an Environmental Protection Agency Risk Management Program facility)*
  - ***Communications***: *Provides wire or radio communications service to the public, businesses, or government*
  - ***Critical Manufacturing***: *Owns/operates a Critical Manufacturing Sector entity*
  - ***Defense Industrial Base***: *Required to report cyber incidents under Defense Federal Acquisition Regulation Supplement 252.204-7012*
  - ***Emergency Services***: *Provides emergency services or functions to a population of 50,000 or more individuals*
  - ***Energy***: *Is required to report to North American Electric Reliability Corporation or to the Department of Energy under OE-417 (Electric Emergency Incident and Disturbance Reporting)*
  - ***Financial Services***: *Owns/operates a legal entity that qualifies as one or more specified financial service entities*
  - ***Government Facilities***: *Is a State, Local, Tribal, or Territorial (SLTT) Government Entity for a jurisdiction with a population of 50,000 or more individuals*
  - ***Government Facilities – Education***: *Is a state or local education agency or educational service agency serving a student population with 1,000 or more students or is an Institute of Higher Education receiving Title IV funding*
  - ***Government Facilities – Elections***: *Manufactures, sells, or provides information and communication technology to support elections processes or reports/displays results on behalf of a SLTT Government Entity*

Given spacing limitations, this slide does not attempt to provide each sector-based criterion verbatim. Please refer to the proposed regulatory text contained in the NPRM for the full language of each sector-based criterion.

Who the Regulation Applies to (3 of 3)

- **Sector-Based Criteria** ***(cont.)***
  - ***Healthcare and Public Health***: *Owns/operates a large or critical access hospital; or manufactures certain essential drugs or Class II or III medical devices*
  - ***Information Technology (IT)***: *Knowingly provides or supports IT hardware/software/systems/services to Federal government; develops or sells/licenses/maintains critical software; is an original equipment manufacturer or vendor of operational technology hardware or software components; or performs functions related to domain name operations*
  - ***Nuclear***: *Owns/operates a commercial nuclear power reactor or fuel cycle facility*
  - ***Transportation***: *Transportation entity required to report cyber incidents to the Transportation Security Administration*
  - ***Transportation – Maritime***: *Entity owns or operates a vessel, facility, or outer continental shelf facility subject to U.S. Coast Guard Maritime Transportation Security Act regulations*
  - ***Water***: *Owns/operates a community water system or publicly owned treatment works for 3,300 or more individuals*

- ***Commercial Facilities, Dams, and Food and Agriculture Sectors*** do not have sector-based criteria
  - They rely on the size-based criterion or other sectors' criteria for coverage

Given spacing limitations, this slide does not attempt to provide each sector-based criterion verbatim. Please refer to the proposed regulatory text contained in the NPRM for the full language of each sector-based criterion.

What Must Be Reported

- **Covered Cyber Incidents**
  - ***Covered Cyber Incident*** means a Substantial Cyber Incident experienced by a Covered Entity
    - ***Substantial Cyber Incident*** means a Cyber Incident that leads to any of the following:
      - A substantial loss of confidentiality, integrity, or availability of the entity's information system or network
      - A serious impact on the safety and resiliency of the entity's operational systems and processes
      - A disruption of the entity's ability to engage in business or industrial operations, or deliver goods or services
      - Unauthorized access to the entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by (i) a compromise of a Cloud Service Provider, Managed Service Provider, or other third-party data hosting provider or (ii) a supply chain compromise
    - Substantial Cyber Incidents ***do not include***:
      - Lawfully authorized activities conducted by a U.S. or SLTT government entity
      - Events perpetrated in good faith in response to a specific request by the system owner or operator
      - Threats of disruption as extortion

- **Ransom Payments**
  - ***Ransom Payment*** means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a Ransomware Attack

Exceptions to Reporting Requirements

1. Substantially Similar Reporting Exception

- A Covered Entity that reports a Covered Cyber Incident, Ransom Payment, or information required in a Supplemental Report to another Federal agency does not have to report it to CISA if:
  - The entity is ***required by law, regulation, or contract*** to report ***substantially similar information*** to another Federal agency in a ***substantially similar timeframe*** as it would under CIRCIA, and
  - CISA and the agency have in place an ***information sharing mechanism*** and an ***information sharing agreement*** (which shall be publicly posted to the maximum extent practicable)
- CISA cannot make a final determination about which reporting programs may be eligible for this exception until the final rule is published

2. Domain Name System (DNS) Exception

- A Covered Entity (or function thereof) that is ***critical infrastructure owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces DNS policies*** is exempt from reporting
- CISA proposes interpreting this to exempt:
  - Internet Corporation for Assigned Names and Numbers (ICANN) and its affiliates
  - American Registry for Internet Numbers (ARIN) and its affiliates
  - Root Server Operator functions of Covered Entities recognized by ICANN as responsible for operating one of the 13 root identities

3. Federal Information Security Modernization Act (FISMA) Reporting Exception

- Federal agencies **required by FISMA** to report incidents to CISA are exempt from reporting those incidents under CIRCIA

Manner, Form, and Procedures for Reporting

- **Manner and Form of CIRCIA Reports**
  - Entities must submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form or any other method approved by the Director
    - Built-in flexibility to allow CISA to eventually offer other reporting mechanisms
  - Single form would be used for all types of CIRCIA reports
    - Form would be dynamic with subsequent questions based on answers to gateway questions

- **Third-Party Reporting**
  - A Covered Entity may use a third party to report on the Covered Entity's behalf
    - No limitations on type of entity who can be a third party
    - Third party must provide an attestation that it has been authorization by the Covered Entity to submit on the Covered Entity's behalf
    - Responsibility for compliance stays with Covered Entity

Content of CIRCIA Reports

- **All CIRCIA Reports**
  - Information on the Covered Entity (e.g., name; entity type; physical address; CI sector(s); other identifiers)
  - Contact information
- **Covered Cyber Incident Reports and Ransom Payment Reports**
  - A description of the incident, including impacts; vulnerabilities exploited; tactics, techniques, and procedures (TTPs) used; indicators of compromise; etc.
    - For Ransom Payment Reports only, ransom demand; payment details (e.g., instructions; amount)
  - Information related to the identity of the perpetrator
  - Mitigation and response activities
- **Supplemental Reports**
  - The basis for/purpose of the supplemental report
  - Any substantial new or different information
  - Notice of a ransom payment made following submission of a Covered Cyber Incident Report (if applicable)
  - Optional information to provide notification that a Covered Cyber Incident has concluded (if applicable)

Data and Records Preservation Requirements

- **Data and Records Preservation Requirements**
  - Covered Entities must preserve certain data and records related to the Covered Cyber Incident or Ransom Payment
  - Applies even if the Covered Entity is not required to directly report to CISA under a Substantially Similar Reporting Exception
- **Preservation period**
  - Starts:
    - For Covered Cyber Incidents – date the entity established a reasonable belief a Covered Cyber Incident occurred
    - For Ransom Payments – date a payment was disbursed
  - Ends:
    - Two years after submission of the last CIRCIA Report
- **Examples of data and records that must be preserved**
  - Indicators of compromise and relevant log entries
  - Relevant forensic artifacts, including memory captures, forensic images, relevant network data, and system information
  - Communications with the threat actor

Enforcement

- **Request for Information (RFI)**
  - CISA may issue an RFI if CISA has reason to believe a Covered Entity experienced a Covered Cyber Incident or made a Ransom Payment but failed to report it as required by the CIRCIA regulations
  - A covered entity must reply in the manner and format, and by the deadline, specified by the Director
- **Subpoena**
  - CISA Director may issue a subpoena if the Covered Entity fails to reply or provide an adequate response to an RFI
  - May be issued no earlier than 72 hours after date of service of RFI
  - CISA may refer non-compliance to DOJ, which can bring a civil action to enforce subpoena; failure to comply is punishable as contempt of court
  - Covered entities may appeal issuance of a subpoena through a written request
- **Referral for Suspension, Debarment, and Contracting Actions**
  - Must refer noncompliance that may warrant suspension and debarment to DHS Suspension and Debarment Official for action
  - May refer noncompliance related to performance under a federal procurement contract to contracting official or the Attorney General
- **Applicability**
  - CISA may not take any of these actions against SLTT Government Entities

Treatment of Information

- **Treatment of Information**
  - CIRCIA Reports, responses to RFIs, and/or information contained therein (but not information and reports submitted in response to subpoenas):
    - Will be treated as commercial, financial, and proprietary information, as marked by the Covered Entity
    - Are exempt from disclosure under the Freedom of Information Act (FOIA) and any state/local laws requiring disclosure of information or records
    - Does not waive applicable privileges or protections provided by law, including trade secret protections
    - Are not subject to agency rules and procedures or judicial doctrine regarding *ex parte* communications

Restrictions on Use

- **Restrictions on Use**
  - Prohibition on federal, state, local, or tribal government use of information obtained solely through a CIRCIA Report or response to RFI to regulate, except:
    - if the regulating entity expressly allows the Covered Entity to meet separate regulatory reporting obligations through submission of reports to CISA
    - consistent with regulatory authority specifically relating to prevention or mitigation of cyber threats to information systems to inform the development or implementation of such regulations
  - “No cause of action” liability protection solely for submission of CIRCIA Report
  - Reports, responses to RFIs, or records created for sole purpose of such submission may not be submitted as evidence, subject to discovery, or used in a trial or hearing
  - Federal government can only disclose, retain, or use information provided to CISA in a CIRCIA Report or response to RFI for specified authorized uses (e.g., a cybersecurity purpose)

Privacy Protections

- **Privacy Protections**
  - CISA will delete personal information not needed for contacting a Covered Entity or directly related to a cyberthreat
  - For POC personal information, CISA will safeguard when retained, and anonymize prior to sharing outside of the Federal government

Key Resources

- **CIRCIA NPRM:** Go to www.federalregister.gov and search for 89 FR 23644
- **CIRCIA Docket**: Go to www.regulations.gov and search for CISA-2022-0010
- **CIRCIA Website**: www.cisa.gov/circia
- **CIRCIA Mailbox**: circia@cisa.dhs.gov

For more information:
CISA.gov/CIRCIA

For questions:
CIRCIA@cisa.dhs.gov