CIRCIA

WHAT YOU NEED TO KNOW

What is the CIRCIA NPRM?

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 Requirement
- Enforcement Mechanisms
- Information Protections and Restrictions on Use

STATUTORY PARAMETERS

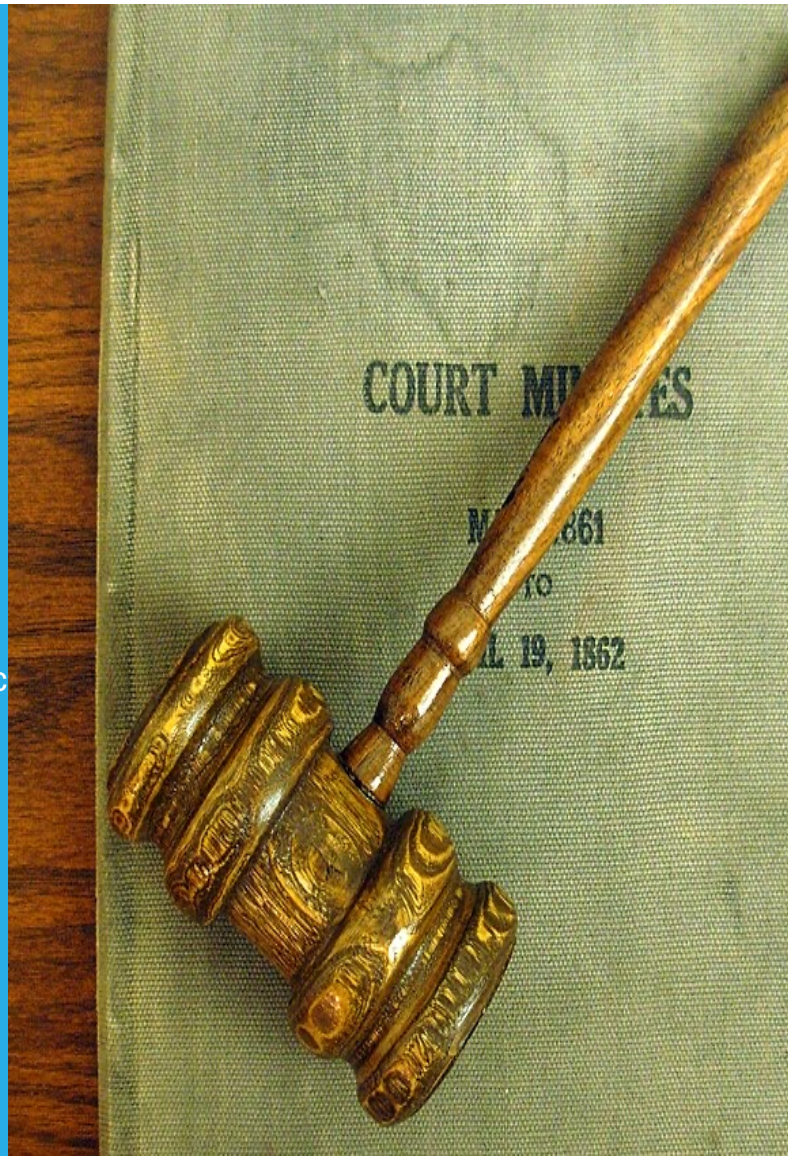
- CIRCIA defines a Covered Entity as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21.

- 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 cause 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 Regulations Apply To

- **Chemical**
- **Communications**
- **Critical Manufacturing**
- **Defense Industrial Base**
- **Emergency Services**
- **Energy**
- **Financial Services**
- Government Facilities
  - Education Subsector
  - Elections Subsector
- Healthcare & Public Health
- Information Technology
- Nuclear
- Transportation
  - Maritime Subsector
- Water
- Commercial Facilities, Dams, and Food & Agriculture

Covered Cyber Incident Reporting

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 Cloud Service Provider, Managed Service Provider, or other third-party data hosting provider or (ii) a supply chain compromise.

Substantial Cyber Incident Exclusions

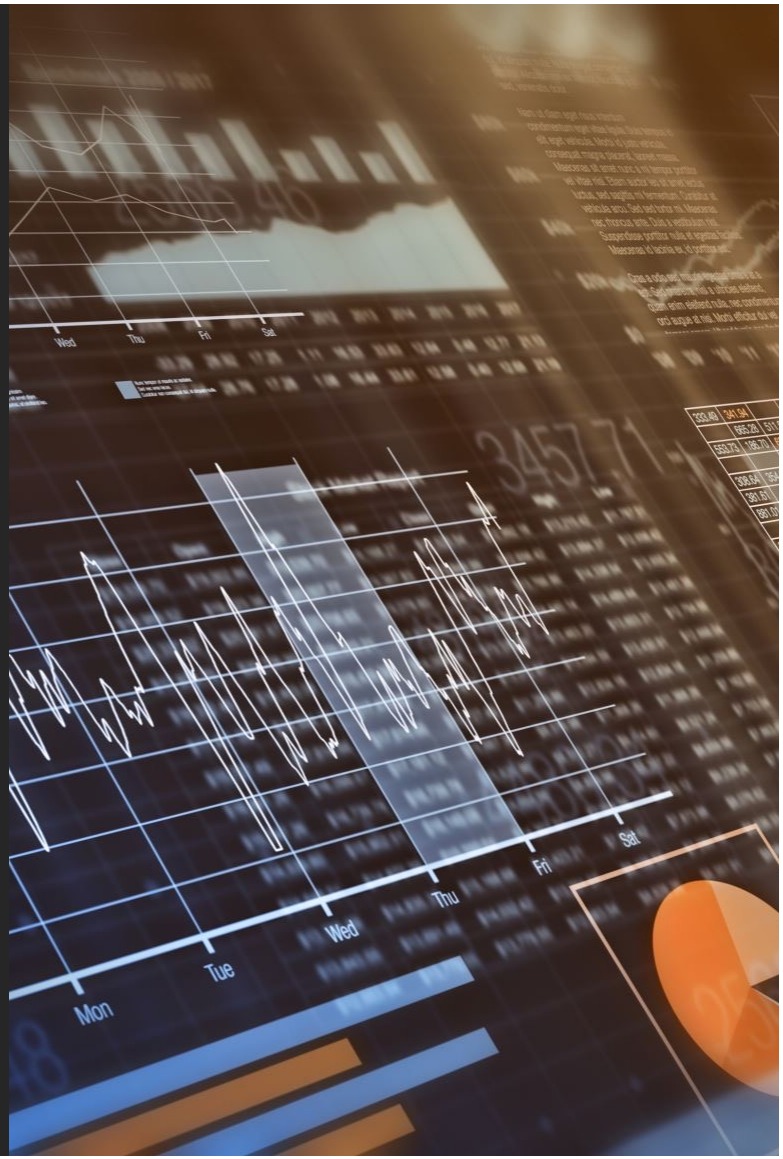
- Lawfully authorized activities conducted by a U.S. or SLTT government entity.
- Events perpetrated in good faith in response to a specific request by the system owner or operator.
- Threats of disruption as extortion

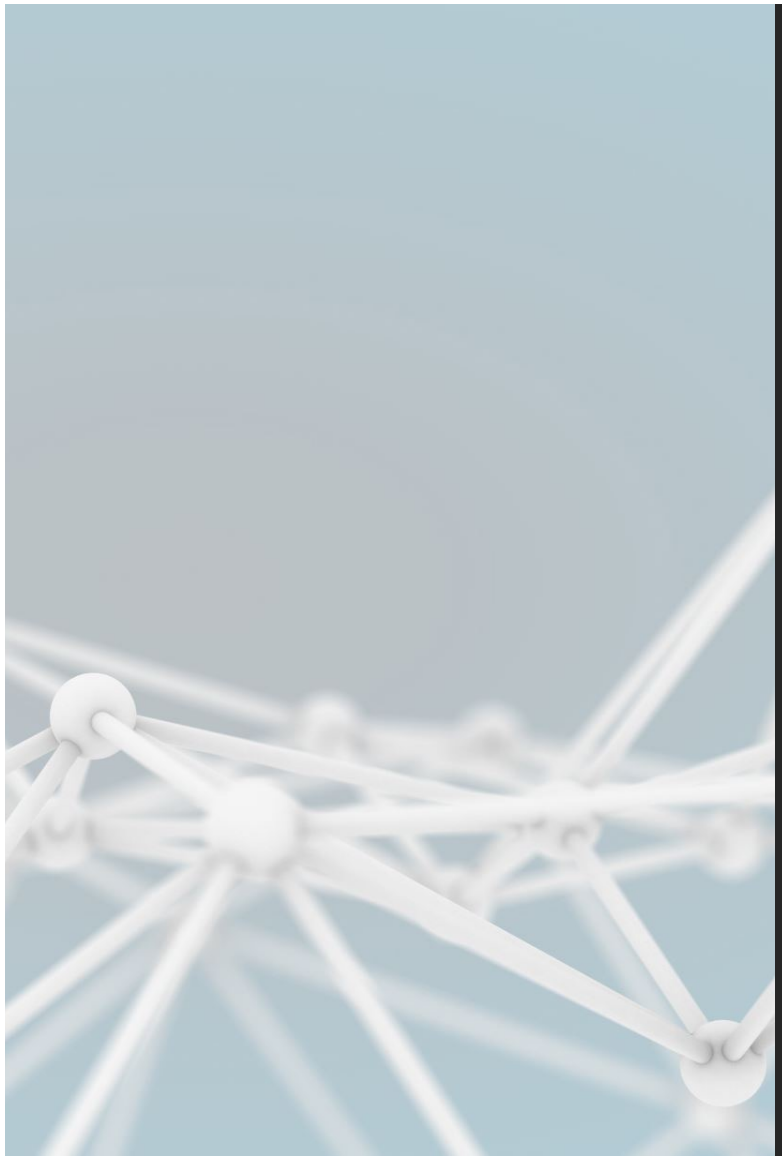
Ransom Payment Reporting

- **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.
- Must be reported within 24 hours of making the payment
- Are two reports required to be filed?

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 assess which reporting programs may be eligible for this exception until the final rule is published.





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

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.

**FISMA is a US federal law to protect government information and operations from cyberthreats. It requires federal agencies to develop, document, and implement information security programs.

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 the type of entity who can be a third party
- Third party must provide an attestation that it has been authorized by the Covered Entity to submit on the Covered Entity's behalf
- Responsibility for compliance stays with Covered Entity

All CIRCIA Reports

- Information on the Covered Entity
  - Name
  - Entity type
  - Physical address
  - CI sector(s)
  - Other identifiers
- Contact Information

Covered Cyber Incident Reports and Ransom Payment Reports

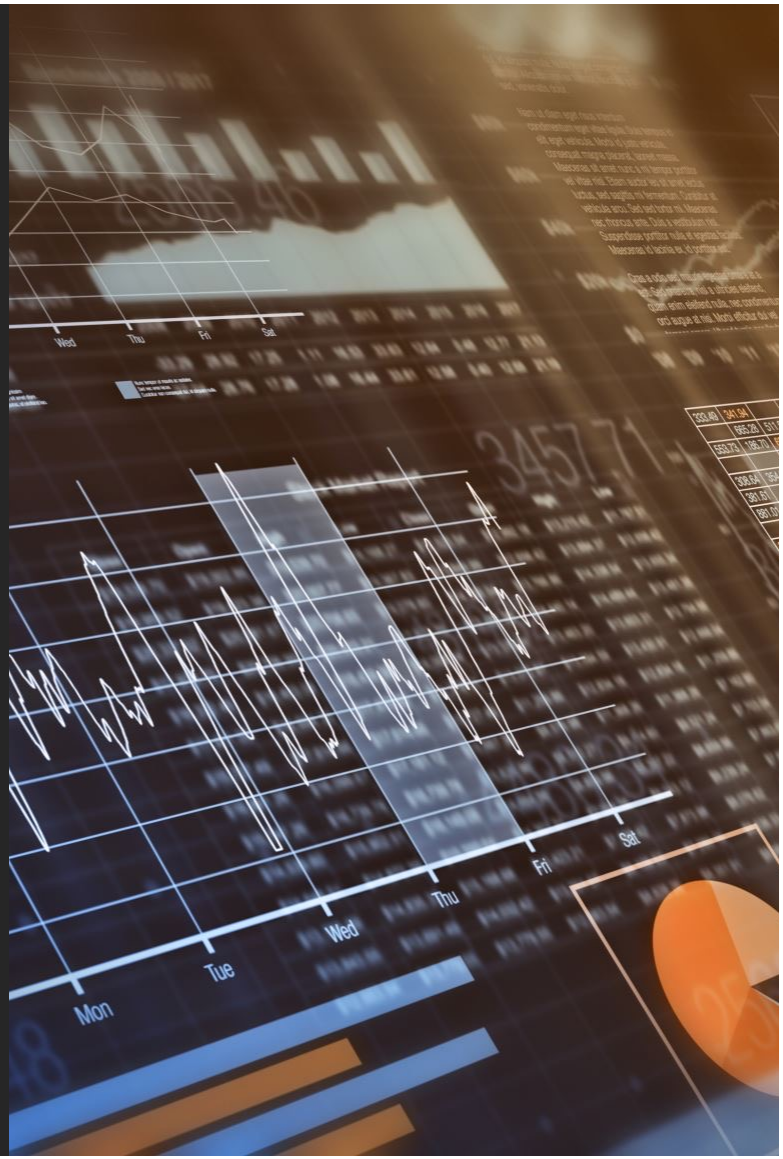
A description of the incident, including impacts, vulnerabilities exploited, TTPs used, IOCs, etc.

Information related to the identity of the perpetrator

Mitigation and response activities

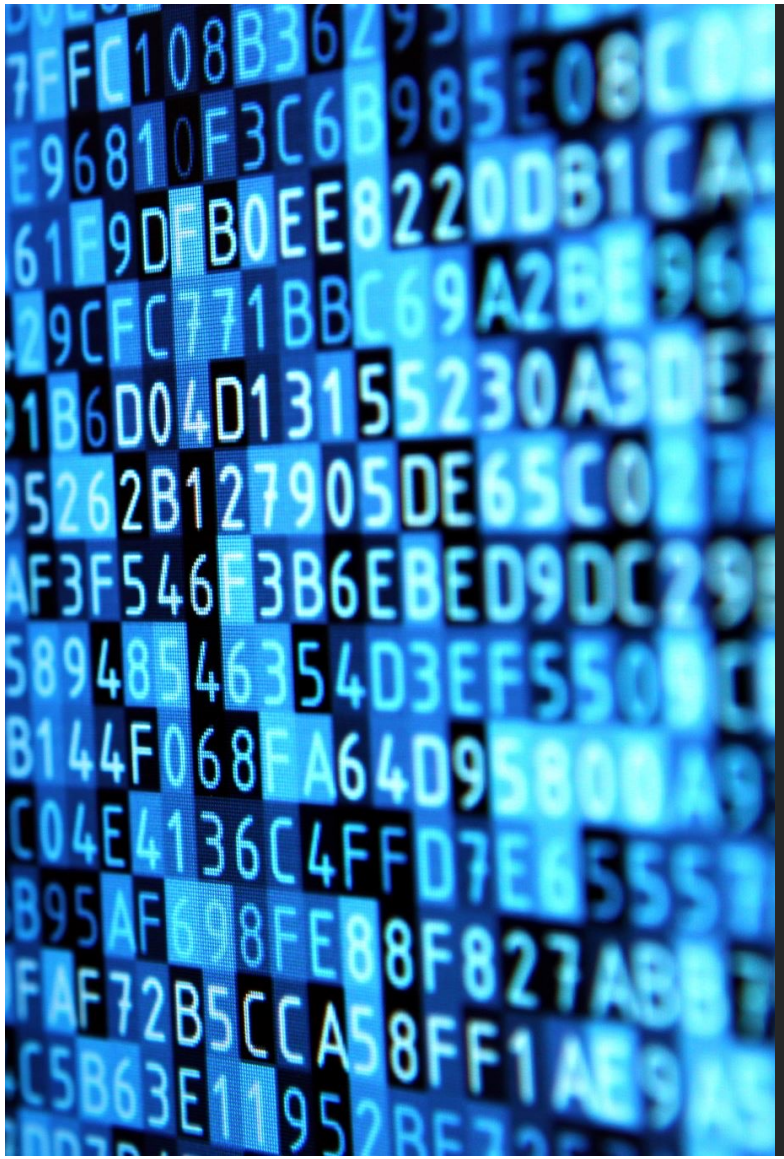
Supplemental Reports

- 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

- 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

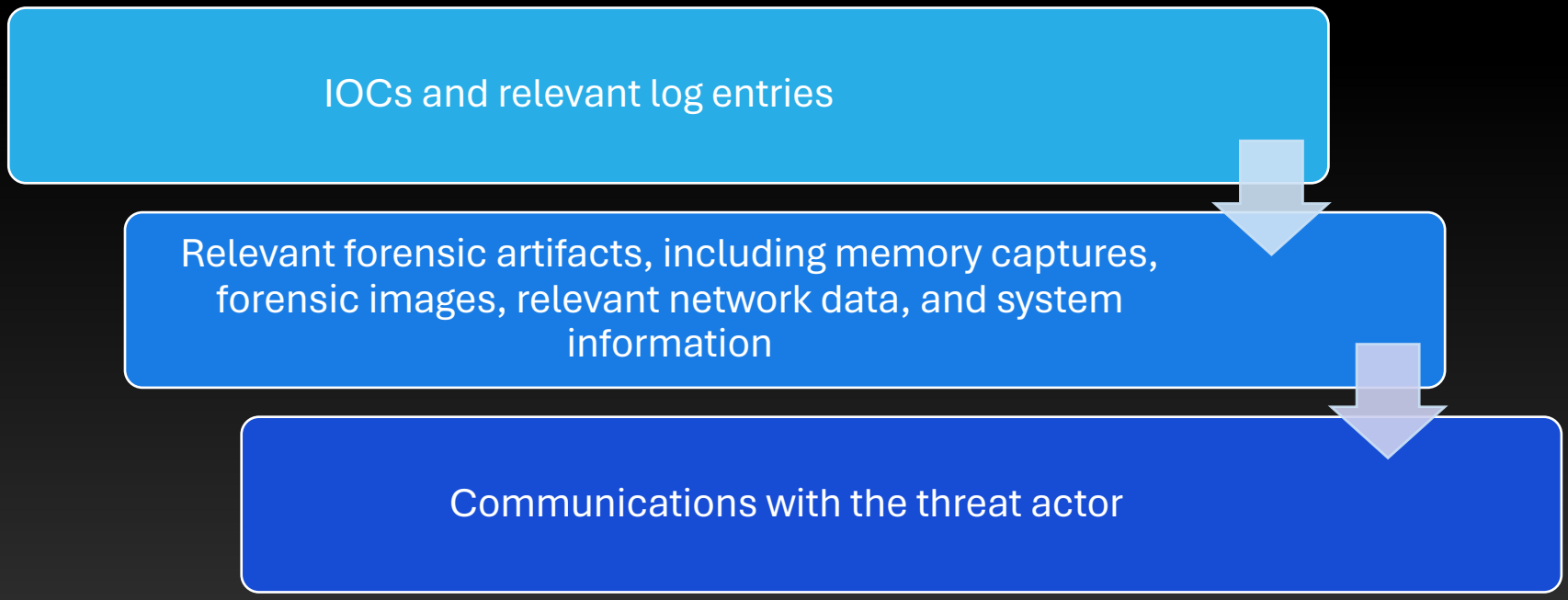
STARTS:

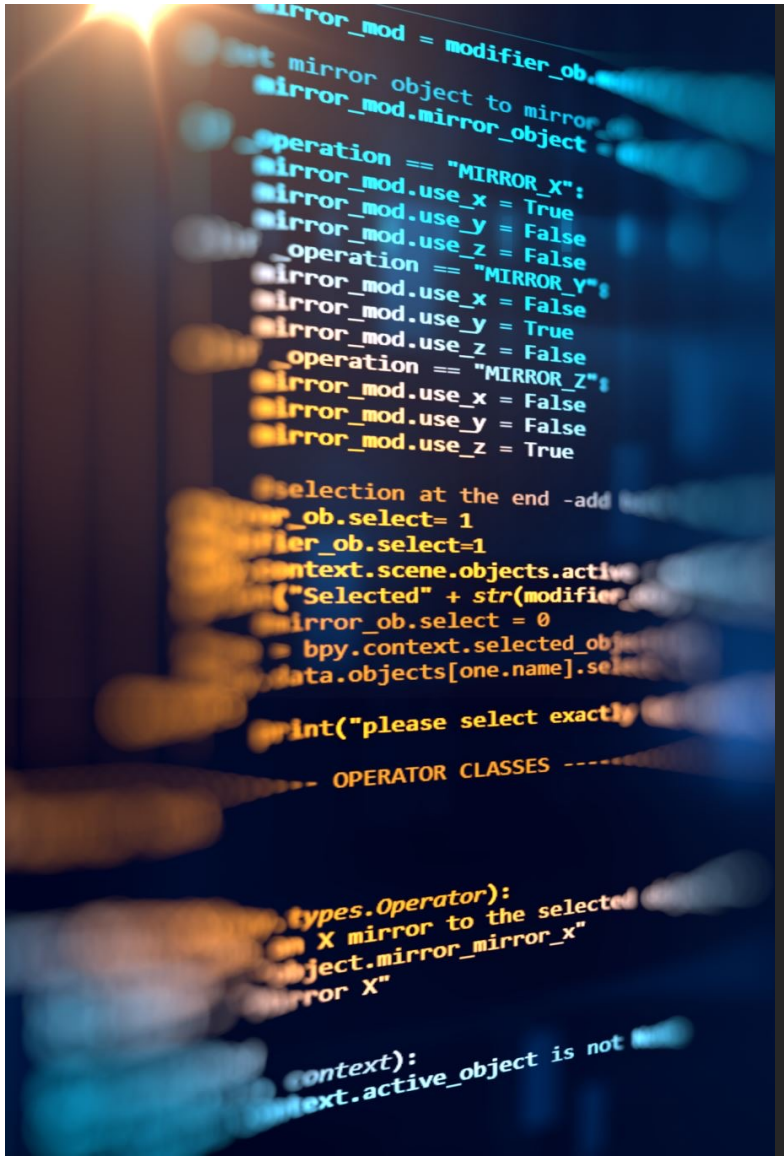
- For Covered Cyber Incidents – date the entity established a reasonable belief a Covered Cyber Incident occurred
- For Ransom Payments – date a payment was disbursed.

ENDS:

- Two years after submission of the last CIRCIA Report

Examples of Data and Records That Must Be Preserved





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

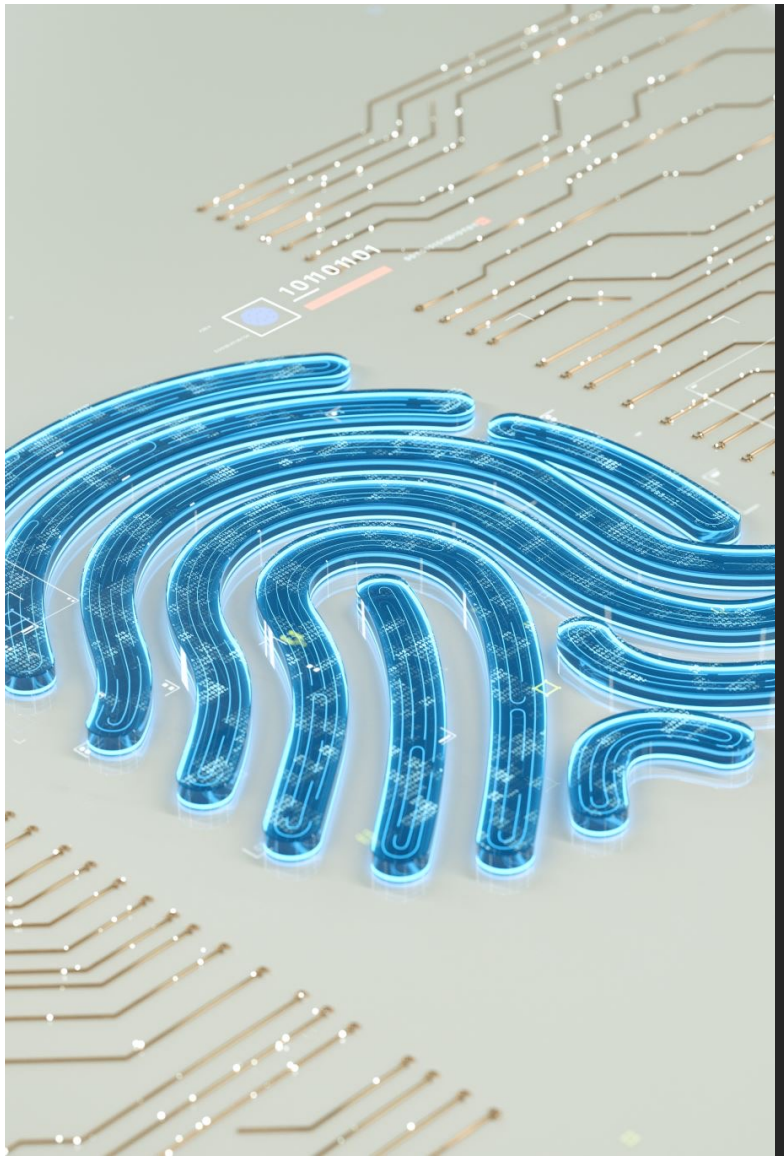
Treatment of Information

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

- 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 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

CISA will delete personal information not needed for contracting 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: www.federalregister.gov and search for 89FR23644

CIRCIA Docket: www.regulations.gov and search for CISA-2022-0010

CIRCIA Website: www.cisa.gov/circia

CIRCIA Mailbox: circia@cisa.dhs.gov


QUESTIONS?

Questions??

Sarah Bigham
Soc@ren-isac.net