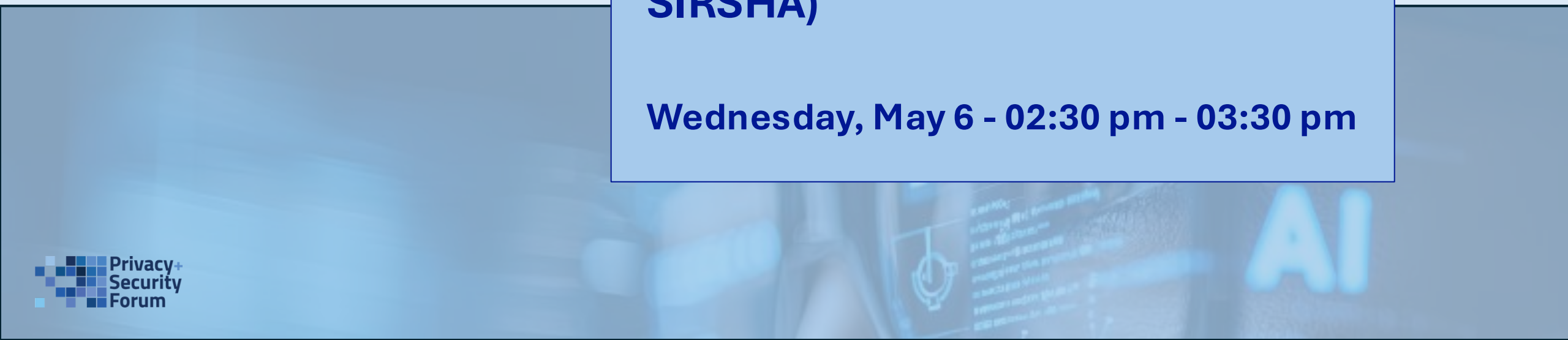
# Privacy + Security Forum

## Session: Contending with CIRCIA (Whether You Say SIR-SEEYA or SIRSHA)

**Wednesday, May 6 - 02:30 pm - 03:30 pm**




Privacy + Security Forum

# Contending With CIRCIA: Regardless of Whether You Say SIR-SEEYA' or SIRSHA


**Randy Sabett**
Special Counsel,
Cooley

**Erin Whitmore**
Managing Director,
Executive Risk &
Strategic Intelligence,
CYPFER


Privacy + Security Forum

# Session: The Cyber Incident Reporting for Critical Infrastructure Act of 2022

## Session Style

- Panel Discussion Style with Speaker Perspectives

## Agenda

- Overview of CIRCIA Timeline and History
- Current State, Provisions, and Requirements
- Future Considerations
- Questions and Open Discussion

Privacy+ Security Forum

# Cyber Incident Reporting for Critical Infrastructure Act of 2022

- Signed into law by President Biden on Signed into law by President Biden on **March 15, 2022**
- Federal legislation that created **mandatory cyber incident reporting** obligations for critical infrastructure entities
- Administered primarily by the **Cybersecurity and Infrastructure Security Agency (CISA)**
- Designed to give the federal government **real-time visibility** into cyber threats targeting the nation's most essential systems
- Part of a broader federal push toward **proactive, rather than reactive**, cybersecurity governance

Privacy+ Security Forum

# The Threat Landscape That Drove CIRCIA

## Motivating events:

| Incident | Year | Impact |
|---|---|---|
| SolarWinds Supply Chain Attack | 2020 | ~18,000 organizations compromised, including federal agencies |
| Colonial Pipeline Ransomware | 2021 | Fuel supply disrupted across the Eastern U.S. |
| JBS Foods Ransomware | 2021 | Global meat supply chain disrupted |
| Kaseya VSA Attack | 2021 | ~1,500 downstream businesses affected |
| Microsoft Exchange Vulnerabilities | 2021 | Tens of thousands of servers compromised |

**Key Takeaway:** Voluntary reporting did not provide federal government timely, actionable incident data — potentially creating blind spots in national cyber defense.

# Legislative History & Road to Enactment

- The Path to CIRCIA: A Multi-Year Legislative Effort
  - **Timeline:**
    - **2018:** Proposal for the Development of a Strategic Cyber Incident and Data Breach Notification Framework (U.S. Chamber of Commerce)
    - **2019–2020:** Early congressional proposals for mandatory cyber reporting introduced; no consensus reached
    - **2021:** Colonial Pipeline and SolarWinds attacks galvanize legislative urgency
    - **June 2021:** Senate Armed Services Committee considers cyber reporting provisions
    - **October 2021:** Bipartisan draft legislation introduced in both chambers
    - **February 2022:** Senate passes CIRCIA as part of the Consolidated Appropriations Act
    - **March 15, 2022:** President Biden signs CIRCIA into law
    - **Bipartisan Support:** Legislation passed with strong bipartisan backing, reflecting broad consensus on need for cyber transparency

# Core Provisions of CIRCIA

- What Does CIRCIA Require?
  - **Three Primary Mandates:**
    - **Covered Cyber Incident Reporting**
      - Report significant cyber incidents within **72 hours** of reasonable belief that an incident has occurred
    - **Ransomware Payment Reporting**
      - Report ransomware payments within **24 hours** of making the payment
    - **Supplemental Reporting**
      - Submit updated reports if new or different information becomes available or upon request from CISA

# Core Provisions of CIRCIA (Cont'd)

- What Does CIRCIA Require?
  - **Additional Provisions:**
    - Establishes a **Cyber Incident Reporting Council** to harmonize federal reporting requirements
    - Directs CISA to share incident data with relevant government agencies and the private sector
    - Information submitted is protected from certain uses, including as evidence in regulatory enforcement actions

# Who Must Comply? Covered Entities

- Scope: Critical Infrastructure Sectors Covered
  - **Governed by Presidential Policy Directive 21 (PPD-21) — 16 Sectors:**
    - Chemical | Commercial Facilities | Communications
    - Critical Manufacturing | Dams | Defense Industrial Base
    - Emergency Services | Energy | Financial Services
    - Food & Agriculture | Government Facilities | Healthcare & Public Health
    - Information Technology | Nuclear | Transportation Systems | Water & Wastewater
  - **Key Scoping Factors (to be defined by final rule):**
    - Size of the entity
    - Sector of operation
    - Nature and criticality of operations
    - Prior incidents or vulnerabilities

**Note:** CISA's NPRM proposed an expansive scope — exact entity coverage is being finalized through rulemaking.

# What Triggers Reporting? Covered Cyber Incidents

- **Defining a "Covered Cyber Incident"**
  - **Triggering Criteria (per CIRCIA & proposed rule):**
    - **Substantial loss** of confidentiality, integrity, or availability of an information system or network
    - **Serious impact** on safety and resiliency of operational systems and processes
    - **Disruption** of business or industrial operations
    - **Unauthorized access** via a third-party supplier or managed service provider
  - **Key Definitions in Flux:**
    - "Substantial" and "significant" thresholds are subject to final rulemaking
    - CISA's NPRM proposed broad definitions, drawing significant industry comment
    - Ransomware payment reporting is triggered regardless of whether the underlying incident is "covered"
  - **Exclusions Proposed:**
    - Incidents solely affecting personal devices
    - Certain lawfully authorized activities by government

# CISA's Role & Responsibilities

- **CISA as the Lead Agency**
  - **CISA's Core Obligations Under CIRCIA:**
    - Develop and issue **implementing regulations** via notice-and-comment rulemaking
    - Receive, triage, and analyze **incident reports**
    - **Share information** with sector risk management agencies, law enforcement, and intelligence community
    - Establish a **24x7 reporting mechanism** and online portal
    - Publish **anonymized, aggregated threat data** for public benefit
    - Create the **Ransomware Vulnerability Warning Pilot (RVWP)** program
    - Coordinate with the **Cyber Incident Reporting Council** to rationalize overlapping federal reporting requirements (e.g., SEC, NERC, TSA)

# The Rulemaking Process

- From Statute to Regulation: The CIRCIA Rulemaking Timeline
  - **Statutory Rulemaking Deadlines:**

| Milestone | Statutory Deadline | Actual Date |
|---|---|---|
| Request for Information (RFI) | Within 60 days of enactment | September 2022 |
| Preliminary Proposed Rulemaking | 24 months after enactment | March 2024 |
| Notice of Proposed Rulemaking (NPRM) | Published | April 4, 2024 |
| Public Comment Period | 60 days | Closed July 3, 2024 |
| Final Rule | Target: ~18 months post-NPRM | Pending |

  - **Volume & Complexity:**
    - CISA received **thousands of public comments** on the NPRM
    - Industry stakeholders raised concerns about scope, definitions, and compliance burdens
    - Multiple congressional hearings held to scrutinize the proposed rule

# The NPRM: Key Proposals & Controversies

- April 2024 NPRM — Key Proposals & Industry Response
  - **Notable NPRM Proposals:**
    - **~316,000 entities** potentially covered — a scope widely criticized as overbroad
    - Broad definition of "covered cyber incident" using a "reasonable belief" standard
    - Mandatory reporting even for **potential** or **suspected** incidents
    - Required preservation of data and systems following an incident
    - Proposed **civil enforcement** and subpoena authority for CISA
  - **Major Industry Objections:**
    - Scope too expansive, covering small businesses with minimal cyber risk
    - 72-hour window deemed unworkable during active incident response
    - Potential **duplication** with SEC, NERC CIP, HIPAA, and state breach notification laws
    - Concerns over **liability exposure** and government use of reported data
    - Definitional vagueness creating compliance uncertainty

# Current Status as of 2025–2026

- Where Does CIRCIA Stand Today?
  - **Post-Comment Period Developments:**
    - CISA analyzing voluminous public comments received through July 2024
    - Final rule expected to be **substantially revised** from the NPRM based on stakeholder feedback
    - **Trump Administration (January 2025):** Regulatory freeze and executive orders directing review of pending rules — CIRCIA final rule status subject to ongoing evaluation
    - CISA leadership changes under administration have introduced **timeline uncertainty**
    - Congress continues to oversee the rulemaking and has expressed interest in **streamlining** the rule's scope
    - Cyber Incident Reporting Council continues work on **harmonization** of overlapping federal reporting frameworks

# Current Status as of 2025–2026

(cont'd)

- Where Does CIRCIA Stand Today?
  - **Practical Reality:**
    - No final rule in effect as of Q2 2026
    - Mandatory reporting obligations **not yet enforceable** for most entities
    - Organizations advised to prepare compliance programs proactively

Privacy+ Security Forum

# Don’t Forget About CISA 2015….

- **CISA 2015 voluntary reporting**
  - Consolidated Appropriations Act reauthorized CISA until September 2026
  - Continues approach of limiting liability for use of defensive measures and disclosure of cyber threat indicators (CTIs)

Privacy+ Security Forum

# Compliance Considerations & Looking Ahead

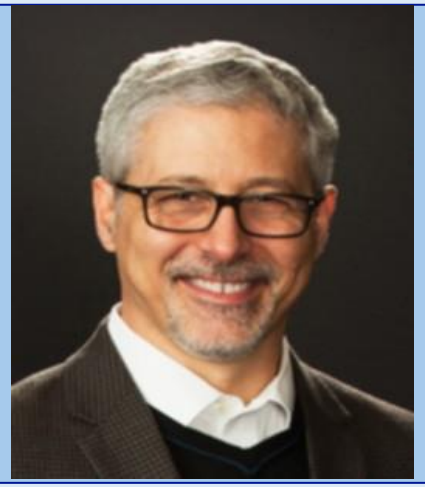
- Preparing Now: Key Takeaways for Covered Entities
  - **Steps Organizations Should Take Today:**
    - **Assess Scope:** Determine whether your organization likely qualifies as a covered entity under one or more critical infrastructure sectors
    - **Map Existing Reporting Obligations:** Identify overlap with SEC rules, NERC CIP, HIPAA, state breach laws, and sector-specific requirements
    - **Build Incident Response Infrastructure:** Ensure 72-hour reporting is operationally feasible — designate reporting personnel and document procedures
    - **Engage with Counsel:** Monitor rulemaking developments and evaluate comment opportunities if a supplemental NPRM is issued
    - **Inventory Third-Party Risk:** Address supply chain and managed service provider exposure, which CIRCIA reporting covers
    - **Train Personnel:** Ensure legal, IT, and security teams understand CIRCIA's forthcoming obligations

# Compliance Considerations & Looking Ahead
(cont'd)

- **What to Watch:**
  - Publication of the Final Rule (timing uncertain)
  - CISA portal launch and reporting mechanism details
  - Administration policy direction on regulatory scope
  - Legislative amendments to CIRCIA

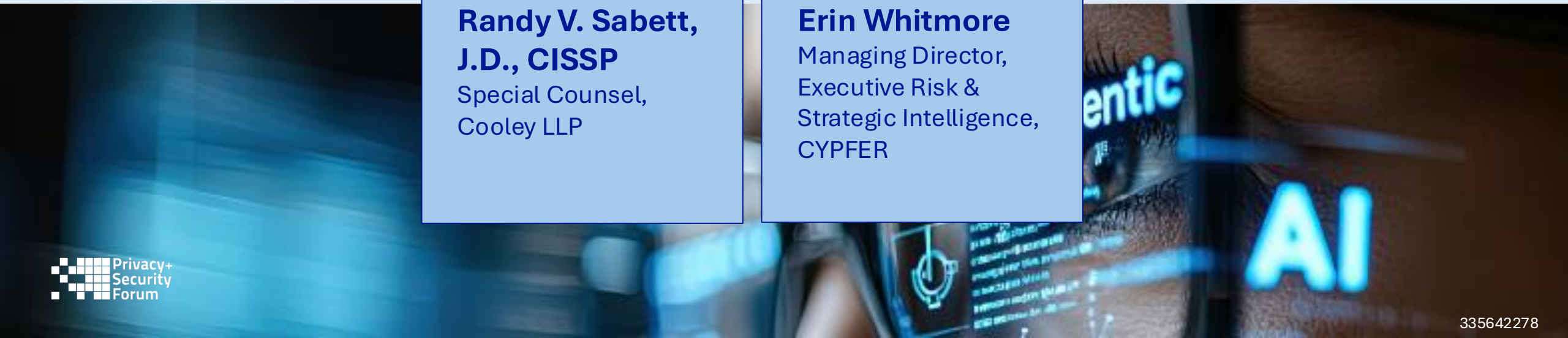
# Questions and open floor

# Stay in touch: Continue the conversation with us




**Randy V. Sabett, J.D., CISSP**
Special Counsel,
Cooley LLP

**Erin Whitmore**
Managing Director,
Executive Risk &
Strategic Intelligence,
CYPFER


Privacy+ Security Forum