Can Your Utility Survive a Cyber Attack?

Deep Dive into the Public Power Cyber Incident Response Playbook

Lindsay Kishter, Nexight Group

AMERICAN PUBLIC POWER ASSOCIATION

Agenda

- **Public Power Cyber Incident Playbook Overview**
- **Importance of a Cyber Incident Response Plan**
- **Getting Started:** 10 Steps to Develop a Cyber Incident Response Plan
- **Engaging Help:** Activating the CIRT and Engaging Industry and Government Resources

THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Public Power Cyber Incident Response Playbook Overview

AMERICAN PUBLIC POWER ASSOCIATION

Purpose of the Playbook

Forthcoming *Public Power Cyber Incident Response Playbook* serves several roles:

- Provides **guidance to help a utility develop its cyber incident response plan**— including roles, key processes and procedures, and communication guidance
- Maps out **how members can engage industry/government resources** to share incident information, get support, and coordinate messaging with the public
- Outlines the **process for requesting cyber mutual assistance** for a cyber event that significantly disrupts utility business or operational systems or overwhelms in-house cyber resources and expertise

How the Playbook was Developed

- **Conducted interviews** to understand cyber incident response processes, needs, and playbook priorities
  - Public power utilities using the Cybersecurity Scorecard
  - APPA staff
  - MS-ISAC
  - Cyber Mutual Aid Program leads
- **Facilitated discussions with the Cybersecurity Roadmap Advisory Council (CRAC)** to collect information on building a cyber incident response team, key elements of a cyber incident response plan, and incident thresholds
- **Drew best practices from open-source incident planning guidance** (NIST, SANS, etc.) and existing industry plans/playbooks

What We Heard

- Many small and mid-sized public power utilities have **no formal cyber incident response plan** and need guidance on what steps to prioritize
- Without experiencing a significant cyber incident, **some utilities lack a clear strategy to engage outside resources** if an incident overwhelms the abilities of their cybersecurity staff, vendors, and service providers
- **Small cybersecurity teams can have a flexible, agile response**—provided roles, responsibilities, and contacts are identified ahead of time
- **Management buy-in and sign off is crucial** to give employees the authority to act quickly

Importance of a Cyber IRP

Application Offline

Due to the ransomware attack on the City's computer system, the City's online payment portal is currently not operational.

While this matter is being addressed, customers may bring payments along with bills/statements to the Municipal Building located at 200 Holliday Street. Payments can also be sent by postal mail. Please use only checks or money orders.

Any late fees and penalties related to this payment system will be waived beginning with the date of May 7 and such fees will remain waived until the online payment system is operational.

Thank you for your patience as we work to restore normal operations.

GETTING STARTED: 10 Steps to Develop a Cyber Incident Response Plan

1. Identify Your Cyber Incident Response Team (CIRT)

The CIRT includes the individuals responsible for:

- Assessing, containing, and responding to incidents
- Assessing the business and legal impacts
- Communicating to internal and external stakeholders and reporting incidents to appropriate entities
- Engaging with industry and government response partners to coordinate information and resource sharing when needed

CIRT often includes utility staff + municipal and third-party resources:

- **Municipal IT cybersecurity departments**, legal teams, and public affairs or communications staff
- **Contracted cybersecurity services** for incident detection and response, such as system monitoring and intrusion detection
- **On-call cyber incident response service providers** to assist in key response actions, such as forensic analysis and incident mitigation

Tiered Cyber Incident Response Team (CIRT) Approach

Cyber Incident First Response Team

- Cyber Incident Response Manager
- IT Technical Response Team or Lead (if different from above)
- IT/OT Liaison or Power Operations Lead

Roles:

- Conducts initial investigation of alerts
- Declares a cyber incident
- Mobilizes the full response team resources appropriate to the incident
- May constitute the full IRT for some incidents
- Often oversees plan development and updates after an incident

CIRT Steering Committee

- Senior executive or manager(s), e.g., chief information security officer
- General Counsel or designee

Roles:

- Assess and confirm the First Response Team's declaration of a cyber incident
- Help determine the composition of employees and contractors who make up the Full CIRT
- Oversee incident investigation, response, and reporting
- Elevate the incident and notify the C-suite and Board of Directors in a significant incident

Full Cyber Incident Response Team

- IT Technical Response Team (often a mix of staff and service providers)
- Legal Counsel
- Public Affairs/Communications
- NERC CIP Manager (if applicable)
- Additional scale-up support:
  - Human resources
  - Logistics lead
  - Finance/procurement representative
  - Designated liaison/reporting roles

Roles:

- One IRT member often plays several roles
- Roles may be filled by utility or municipal employees and third-party service providers
- Resources are mobilized based on the needs of the incident
- Activation may expand as the incident evolves
- City/state/federal agencies and other external response organizations may also assist the CIRT with the response

Staffing the Cyber Incident Response Team

Balance the following factors to staff the team:

- **24/7 Availability**: Designate and train backup roles for critical staff. Consider how to supplement lead staff for round-the-clock response.
- **Staff Expertise**: Incident handling and mitigation often requires specialized knowledge and experience.

Leverage your natural disaster incident response plan for roles required in any type of incident (e.g., human resources, logistics, liaisons)

Ensure CIRT members have the necessary authority to act quickly and decisively.

- Who has the authority to disconnect key business and operational networks to isolate an incident?
- Who can request additional support from service providers? What procurement processes are required?
- Who will notify key officials and ensure compliance with reporting requirements?
- Who will report a suspected criminal attack to law enforcement?

2. Develop a 24/7 Contact List for Response Personnel and Partners

- **Document phone numbers, emails, and addresses** of the lead individual for each role, including off-hours contact information.
- **Identify a potential alternate** for each role.
- **Include cybersecurity service providers, ISP, and equipment/device vendor contacts.** Identify:
  - What type of support each contact can provide during an incident
  - Process for engaging their support
  - Who on the CIRT is authorized to engage third-party support services
- **Maintain the list online *and* in a central, offline location**—such as a physical binder or offline computer. Update it yearly.

3. Compile Key Documentation of Business-Critical Networks and Systems

- **Network Scheme** displaying the network architecture with internal network segmentation—Helps to quickly orient cyber response teams.
- **Equipment and configuration inventory** of core assets in utility environment—Enables personnel to quickly determine the potential extent of compromise and the processes or functions that could be affected.
- **Access credentials/account permission list** to discern who has the authorization to access, use, and manage the utility network—Enables personnel to investigate and remove unauthorized access and provide temporary access to incident responders

4. Identify Response Organizations and Establish Mutual Assistance Agreements

- **Maintain an updated list of key contacts or liaisons** for external industry and government response organizations, such as:
  - Cybersecurity liaisons at law enforcement agencies (e.g., FBI, state/local agencies)
  - Incident reporting and information-sharing organizations (e.g., E-ISAC, MS-ISAC, DHS NCCIC)
  - Cyber contacts at APPA and/or Joint Action Agency who can coordinate and connect resources
  - Cyber mutual assistance contacts
  - Federal response agencies (e.g., DOE, DHS, FBI)
- **Sign NDAs and review information-sharing agreements with the legal team in advance** to shave precious time off of incident response.
- **Outline your incident reporting requirements and timelines.** Determine your legal and contractual obligations to report incidents to state/local officials, insurance providers, and other third parties.

5. Develop Technical Response Procedures for Cyber Incident Handling

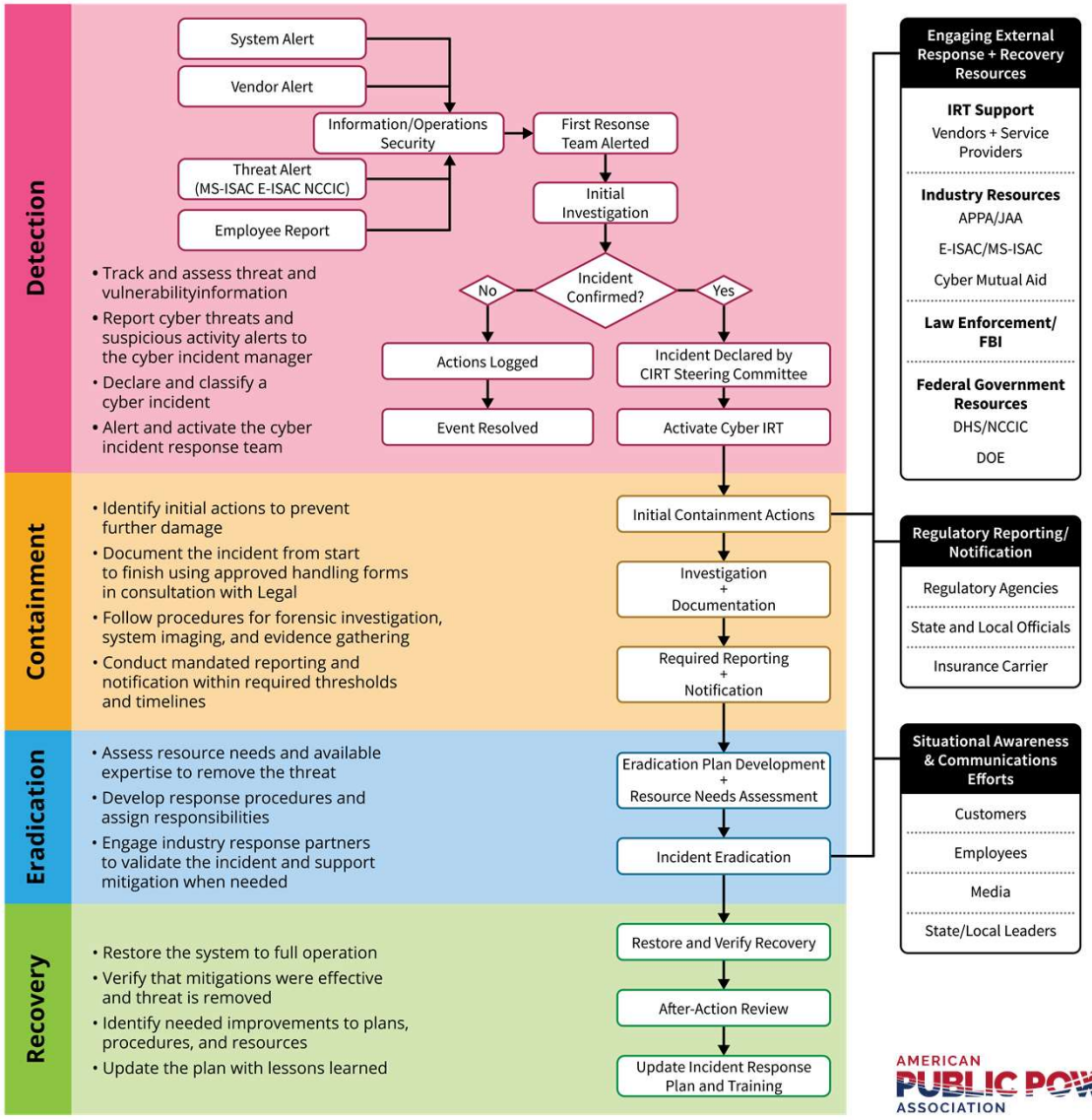
Designate which CIRT members act and when for all phases of incident response:

- **Detection, Investigation, and Analysis** – Procedures for alerting and detection, escalation, declaration of a cyber incident, incident classification and prioritization, incident investigation, and activating an appropriate cyber incident response team
- **Containment** – Conducting initial containment actions, documenting the incident, procedures for evidence gathering and handling, and conducting required incident reporting
- **Eradication** – Developing response solutions, assessing resource needs, engaging external resources and response organizations, and following a response plan to eradicate the threat
- **Recovery** – Cleaning and restoring the system to full operation and verifying that mitigation actions were effective; also includes reviewing response actions, documenting lessons learned, and updating the incident response plan

Cyber Incident Handling Process

Outline specific incident handling procedures for a variety of incidents, including:

- Reporting alerts to identify a cyber incident
- Incident handling forms and documentation
- System imaging and other approved evidence gathering and preservation procedures for forensic investigation



6. Classify the Severity of Cyber Incidents

- **Designating cyber incident severity levels can help the CIRT quickly:**
  - Mobilize the right resources based on the type of incident
  - Convey the potential impacts of an incident when notifying internal and external stakeholders
  - Prioritize response actions
- **Each utility should define severity levels that best reflect their design and operations.** Sample severity levels:
  - Use Level 1–3 to define impacts to business systems
  - Reserve Level 4–5 for cyber incidents that impact operational systems and may affect power delivery

Cyber Incident Severity Levels

Aligns with the National Cybersecurity Center severity levels, also used in the ESCC Playbook

Sample Cyber Incident Severity Levels

		General Definition
Operational System (OT) and Business Impact	Level 5	Cyber or cyber-physical event that directly impacts power delivery at one or multiple utilities
	Level 4	Compromise of network or system that controls power generation and delivery and could lead to an outage at one or multiple utilities
Business System (IT) Impacts	Level 3	Compromise or denied availability to a business-critical enterprise system or service (e.g., corrupt or destroy data)
	Level 2	Compromise of security to non-critical enterprise business systems
	Level 1	Suspected security threat or isolated incident with minimal impact (e.g., unidentified server on network, successful phishing attempt with no loss of data)
	Level 0	Notification of suspicious behavior

Sample Cyber Incident Severity Levels

Business System (IT) Impacts	General Definition	Functional Impact	Information Impact	Recoverability Effort	Alignment to National Cyber Incident Schema
Level 3	**Compromise or denied availability to a business-critical enterprise system or service (e.g., corrupt or destroy data)**	Utility can no longer provide a critical business service to a subset of system users	Sensitive, PII, or proprietary information was accessed, changed, exfiltrated, deleted, or made unavailable	Unpredictable; additional resources and outside help may be needed	Likely to result in a demonstrable impact to the public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
Level 2	**Compromise of security to non-critical enterprise business systems**	Minimal effect; the utility can still provide all critical business services to all users but has lost efficiency or lost some non-critical services	Non-PII or proprietary data was accessed or exfiltrated	Predictable with existing or additional resources	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
Level 1	**Suspected security threat or isolated incident with minimal impact (e.g., unidentified server on network, successful phishing attempt with no loss of data)**	Minimal effect; the utility can still provide all critical services to all users but has lost efficiency	Sensitive information at-risk but not exfiltrated	Predictable with existing or additional resources	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0	**Notification of suspicious behavior**	No effect to the organization's ability to provide all services to all users	No information was exfiltrated, changed, or deleted		Unsubstantiated or inconsequential event

Sample Cyber Incident Severity Levels

		General Definition	Functional Impact	Information Impact	Recoverability Effort	Alignment to National Cyber Incident Schema
Operational System (OT) and Business Impact	Level 5	**Cyber or cyber-physical event that directly impacts power delivery at one or multiple utilities**	Utility can no longer provide a critical operational service to all or a subset of users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Poses an imminent threat to the provision of wide-scale critical infrastructure services
	Level 4	**Compromise of network or system that controls power generation and delivery and could lead to an outage at one or multiple utilities**	Utility can no longer provide a critical business service to all system users or can no longer provide a critical operational service to some users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Likely to result in a significant impact to the public health or safety, national security, economic security, foreign relations, or civil liberties

7. Develop Strategic Communication Procedures

- **Designate a POC within the CIRT** to manage and coordinate internal and external communications.
- **Legal counsel should direct the incident investigation and review and approve all external communications related to a cyber incident** to protect the privileged nature of communications,
- Identify the key internal and external stakeholders, what information to communicate and when, and **what type of cyber incidents warrant communication** with employees, customers, and the media.
- **Develop key messages and notification templates in advance**. Consider an incident that:
  - Significantly impacts energy delivery or operations.
  - Affects access to customer-facing systems, such as billing and payment systems, online customer accounts/dashboards, or the company website.
  - Has been widely reported in the media, especially if the utility has already been speculated as a target.
  - Affects employees' ability to access key business systems, such as email, databases, or software.
  - Requires employees to take some action to help mitigate the incident.
- **Work with APPA public affairs team and the ESCC** to coordinate industry messaging during an incident.

8. Develop Cyber Incident Legal Response Procedures

- **The utility's legal team**—both internal and through outside counsel—**must be central to your cyber incident response plan.**
- The legal team should take steps to help preserve a utility's legal posture by **directing and approving relevant documentation and preservation efforts:**
  - Maintaining a chain of custody for documents and other physical evidence, preserving relevant system logs, and creating backups of affected files
  - Issuing legal hold notices applicable to relevant records
  - Preserving privilege by retaining outside experts and directing investigation and documentation
  - Preparing non-disclosure and information-sharing agreements with third parties
  - Limiting unauthorized disclosure or use of sensitive information
- The legal team should evaluate notification and reporting obligations and conduct necessary notifications

9. Obtain CEO or Senior Executive Buy-In and Sign Off on the Incident Response Plan

- Review contents of the incident response plan with senior executives/general manager and **obtain their buy-in and approval with signature forms.**
- Senior management should particularly review and approve:
  - **Roles and responsibilities** of the cyber incident response team
  - **Authorities** of key team members during incident response
  - Any decision-making or resource procurement **procedures that deviate from normal operations**

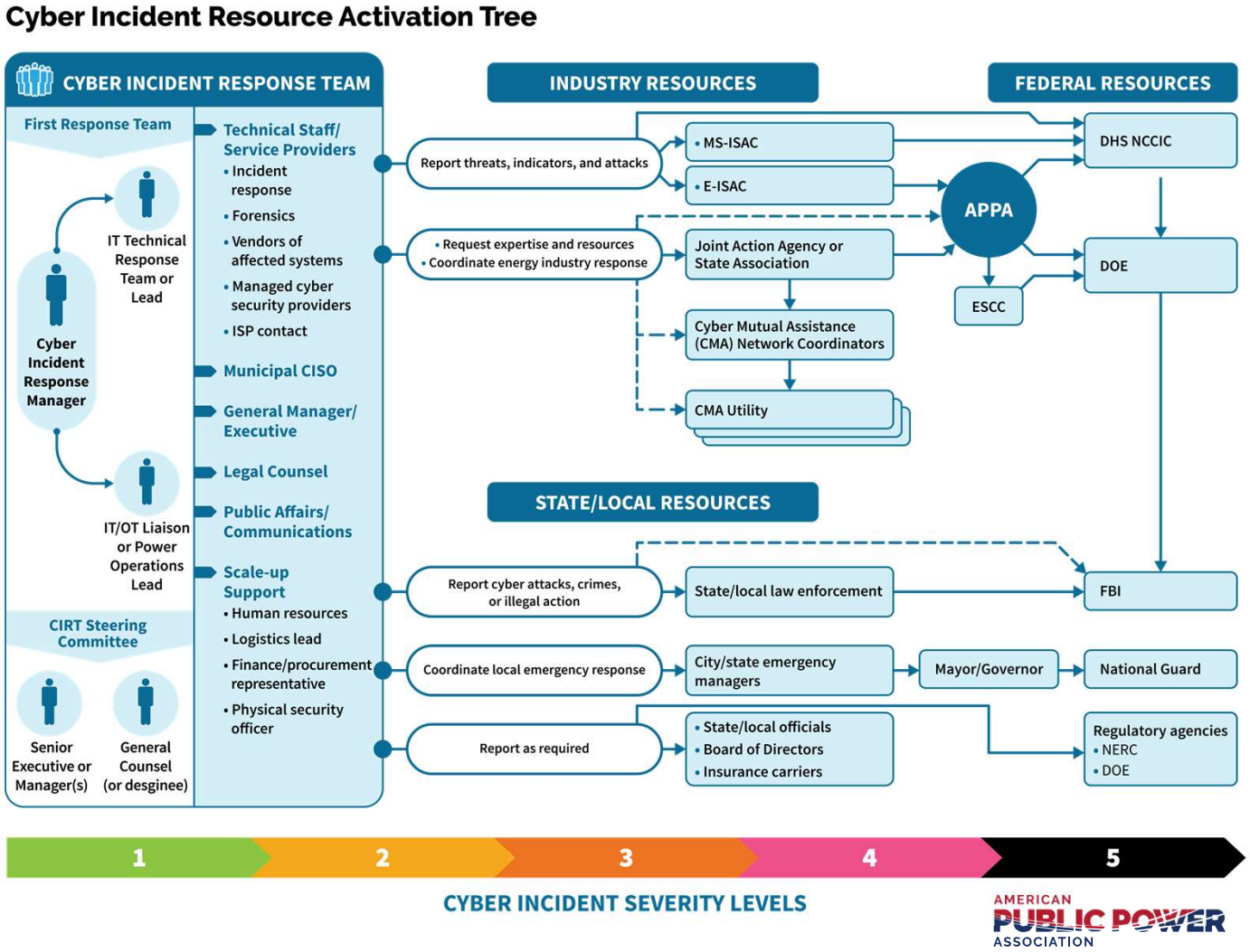
10. Exercise the Plan, Train Staff, and Update Regularly

- **Test a variety of different scenarios and impacts** to identify gaps in procedures or staff capabilities.
  - Conduct abbreviated exercises during plan development to help generate discussions on roles, authorities, and response procedures.
  - In between exercises, conduct drills with small teams of employees to reinforce their roles and identify training needs.
- **Practice incident documentation during exercises**, including using incident handling forms, preserving forensic images, and accessing and investigating logs.
- **Review and update the incident response plan on an annual basis**—especially contact lists—and as part of any post-incident review.

ENGAGING HELP: Activating the CIRT and Engaging Industry and Government Resources

Engaging Help

Few utilities, regardless of size, can manage a significant cyber incident with in-house resources alone



Overview of External Response Organizations

- Report the incident to the **E-ISAC/MS-ISAC**
  - Confirm or correlate an incident and offer mitigations (if known)
  - Offer incident response and forensic support to SLTT members (MS-ISAC)
  - Liaison to federal watch centers (NCCIC, etc.)
- Alert **Joint Action Agency/State Association** and/or **APPA**
  - Provide guidance on industry and media coordination
  - Support **ESCC** Playbook activation and coordination across industry (if multiple entities affected)
  - Serve as liaison **to DOE/DHS/NCCIC** to request/inform federal response teams if a national incident is suspected
- Request resources from **Cyber Mutual Assistance Coordinators** (directly or through Joint Action Agency)
  - Leverage cyber expertise, equipment, and virtual/onsite response support from utility peers
- Contact **state/local law enforcement** or **FBI Cyber Task Force Field Office** if attack suspected
  - Launch criminal investigation
  - Offer/request onsite forensic support as needed
- Coordinate local emergency response with **emergency managers**, the **Mayor/Governor**, and **National Guard** as needed
- Report to **regulators/DOE** if applicable and fulfill **state/city reporting** requirements within required timeframes

Cyber Mutual Assistance (CMA) Program

- **Voluntary, no-cost program** that helps utilities **engage cyber resources and expertise from energy utilities across the nation**
- All organizations that provide or materially support electric or natural gas service are eligible
- **No obligation to commit resources**—enables smaller utilities to draw upon the expertise of larger utilities
- **Requests for assistance can be sent to a Coordinator Committee OR directly to specific participating entities.**
  - Proxies such as JAAs can also be designated to represent smaller utilities in meetings and response activities.
- Expenses incurred in providing emergency cyber assistance are **reimbursed at cost**.

- **To participate in the CMA Program**, each participating entity must:
  - **Sign a Mutual Non-Disclosure and Use of Information Agreement (NDA)**, which will protect the confidentiality of all information shared between entities participating in the CMA program.
  - **Designate a Cyber Mutual Assistance Coordinator (CMA Coordinator)** who will serve as the primary contact for the program. The Coordinator must be a senior-level employee with the authority to act on behalf of the participating entity it represents.
- Requests for assistance may be made:
  - In connection with a cyber emergency; or
  - In advance of a threatened or anticipated cyber emergency

Benefits of Early Incident Notification

- **Correlating incidents across industry to identify coordinated attacks or attack trends**. Reporting suspected or confirmed incidents to the E-ISAC and MS-ISAC early allows these partners to analyze the report against other threats, allowing for early detection of coordinated attacks.
- **Mitigation measures and expertise**. Organizations may be able to recommend mitigations, or analyze malware or threat signatures to identify ways to mitigate the incident.
- **Incident investigation support**. Several external response groups can support the utility's forensic analysis and investigation of an incident, either remotely or onsite.
- **Readying response and coordination resources**. Notifying external response groups early can help kickstart cross-industry coordination, prepare response teams for potentially severe incidents, and support messaging coordination among response partners

Questions?

Lindsay Kishter, Director, Nexight Group
LKishter@nexightgroup.com