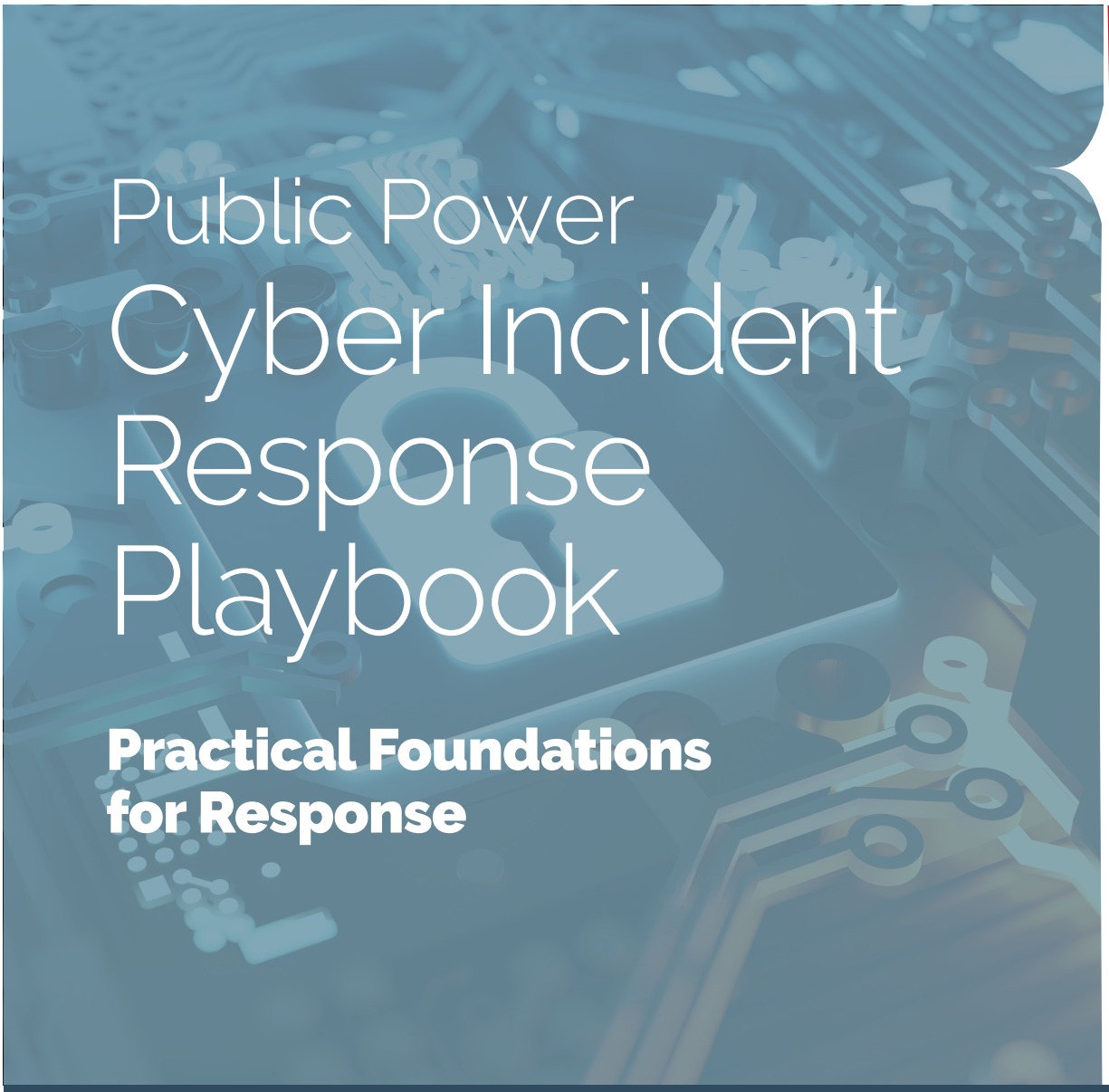
AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities



Public Power Cyber Incident Response Playbook

Practical Foundations for Response

SEPTEMBER 2026

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number(s) DE-CR0000026.

Practical Foundations for Response Document Development

American Public Power Association developed the Cyber Incident Response Playbook: Practical Foundations for Response document with support from its members. We would like to acknowledge the following individuals who provided their time, resources, and knowledge to its development:

Public Power Utilities

Ian Fitzgerald, Chelan County Public Utility District, WA

Don Krause, *Kaukauna Utilities, WI*

Jacob McClanahan, *City Utilities of Springfield, MO*

Ron McLeroy, *Huntsville Utilities, AL*

Tim Pospisil, *Nebraska Public Power District, NE*

Jackie Pszenny, *Ipswich Electric Light Department, MA*

Eshia Smith, *Lakeland Electric, FL*

Matthew Suire, *Lafayette Utilities System, LA*

Association Staff

Chris Ching, *American Public Power Association*

Rob Denaburg, *American Public Power Association*

Table of Contents

1 How to Use the Guide

This guide provides small and medium public power utilities a practical framework to develop and implement a cyber incident response plan, as well as coordinate response and communication during a cybersecurity incident. The guide is derived from APPA's Cybersecurity Incident Response Playbook, which provides significant additional detail and step-by-step guidance on these topics.

For utilities looking for a fundamental and scalable approach to cyber incident response, this guide highlights key elements from the playbook while focusing on practical recommendations for smaller entities. A tiered approach to improving incident response capabilities, with goals for each level of maturity, is outlined in the appendix.

2 Essential Planning Efforts

There are five key planning actions required before an incident to establish a credible and effective incident response process.

2.1: Designate a Cyber Incident Response Manager

Assign an incident response lead with the authority to declare an incident, start containment actions, and coordinate incident response efforts. It is also helpful to designate an alternate or backup in case the assigned lead is unavailable when an incident occurs.

NOT SURE WHERE TO START?

Ask yourself: *"Who is the person you would call today if none of the computers were working?"* Start with that person as your incident response manager, subject to change if your organization identifies someone else for the role. Then, for the backup: *"Who is the next person you would call if they didn't answer?"*

2.2: Define Incident Response Team Roles

Even if you have a small staff, there are incident response roles in addition to the Cyber Incident Response Manager that are essential for incident management. In some organizations, one person may serve in more than one role. There may also be individuals outside your organization, including contractors, that are able to assume one or more of these roles to support your incident response. The functions associated with these roles are more important than specific titles or names.

- Information technology (IT) technical lead (responsible for enterprise systems)
- Operational technology/supervisory control and data acquisition (OT/SCADA) lead (responsible for operational systems)
- Communications point of contact (coordinates external messaging)
- Executive decision-maker (authorizes major actions and spending)
- Legal/counsel (provides guidance to minimize legal risk)

It is also important to understand how the cyber incident response team will integrate with a broader response structure in events that necessitate a larger organizational response.

2.3: Build a Contact List

Identify and document key partners that you might need to contact during a cyber incident. It is important to maintain at least one offline copy, update the offline copy any time you make changes to the list, and ensure that members of the incident response team have easy access to it. Review the list periodically to ensure it remains accurate. The contact list should include, at a minimum:

- Incident response team members and designated backups
- Relevant internal stakeholders
- Key vendors and maintenance providers
- Internet service provider (ISP)
- Managed security service provider (MSSP) [as applicable]
- On-call incident response or forensics support [as applicable]
- Information sharing partners (e.g., Electricity Information Sharing and Analysis Center [E-ISAC])
- Industry contacts (e.g., APPA, joint action agency/state association, Cyber Mutual Assistance)
- Cyber insurance provider, including breach response contact [if applicable]
- Law enforcement and other government contacts

2.4: Know Your Environment

Asset inventories and network maps are very helpful for understanding impacts to your systems and response requirements. It is helpful to know (and be able to easily reference):

- Which of your IT and OT systems are high priority
- What your network map (including IT/OT segmentation and remote access paths) looks like
- Where logs are stored and how to access them
- Who can disable accounts, rotate credentials, and isolate segments
- Where backups are stored and the procedures to restore from backup

NOT SURE WHERE TO START?

Ask yourself:

- How many firewalls do you have and who can make changes?
- How many servers and domain controllers do you have, and who can make changes?
- How many engineering workstations for programming OT devices do you have?
- How many network administrator accounts are there?

2.5: When to Call for Help

To reduce uncertainty and ease the burden of decision-making in high-stress environments, consider predefining discrete events or circumstances that trigger efforts to engage outside help. For example:

- You cannot determine incident scope within a few hours
- The attack includes possible or confirmed impacts to OT/SCADA
- You expect prolonged disruption of critical services
- The incident is attracting public or media attention
- Your team does not have the tools to investigate safely

Note: *If you have cyber insurance, you may need to contact your provider early in the process and follow any necessary steps to ensure coverage. Consider creating a process for engaging insurance provider(s).*

QUICK REFERENCE GUIDE

To improve decision-making and reduce uncertainty in an incident, consider creating a guide that establishes key steps to take in the first 15 minutes, first hour, etc.

3 Incident Severity and Escalation

Use a scale to align response effort to incident severity. This one uses low/medium/high for simplicity, but others available in the playbook offer more granularity.

Incident Level	Indicators	Actions
Low	Suspicious activity or a confirmed compromise with limited potential impact	Handle with IT team and cyber incident response manager
Medium	IT-only impacts, including potential malware, credential compromise, data exposure, or business system disruption	In addition to cyber incident response manager and IT team, involve legal and communications point of contact (POC); consider external reporting and support
High	Compromise of control systems or impacts to power delivery	Activate full team immediately and engage external partners

4 Response Lifecycle

Figure 1 depicts a typical incident response lifecycle.

Figure 1: Incident Response Lifecycle

The **Essential Planning Efforts** outlined in Section [2] provide practical steps to help with the prepare phase. This section provides specific recommended actions for each of the subsequent phases.

4.1: Detect (and Triage)

Immediately after your utility suspects an incident may be occurring, consider:

- Starting an incident log (what time, who observed, what was observed, actions taken)
- Notifying the Cyber Incident Response Manager and IT Lead (and OT/SCADA Lead if OT is in scope)
- Increase monitoring: centralize logs, enable endpoint detection and response isolation features (if available)
- Preserving basic evidence (export logs, take screenshots, save suspicious emails/attachments)
- For utilities with simple IT/OT network connections, sever the link to prevent cross-contamination

Triage questions:

- What system(s) are affected?
- Is the behavior ongoing? Is it spreading?
- What is the business and operational impact right now?
- Any signs of data access/exfiltration?
- Could compromise of IT impact OT through shared credentials, jump hosts, or remote access?

DOCUMENT AND PRESERVE EVIDENCE

Throughout this cycle, it is helpful to capture (and securely store) details about the incident that can support response and stakeholder engagement efforts. This might include:

- A timeline of events and actions
- Impacted systems and relevant details (e.g., IPs, host names, accounts)
- Indicators of compromise (hashes, domains, emails, processes)
- Where logs were collected from and who handled them
- Stakeholders contacted and guidance/ instructions received

To allow for evidence collection and forensics, **it is important not to shut down impacted devices** unless failing to do so presents a health and safety risk.

4.2: Contain

The focus of this stage is stopping the damage and considering recovery options. Possible containment actions, in order of least to most disruptive:

- Isolate affected endpoints/servers from the network (quarantine Virtual Local Area Network (VLAN), disconnect cables, disable Wi Fi)
- Disable suspected compromised accounts, force password resets, revoke tokens/sessions
- Block known malicious internet protocol (IP) addresses/ domains at firewall and via ISP (if known)
- If OT risk is possible: tighten IT/OT boundaries (restrict remote access, enforce jump-host only, disable non-essential interconnections)
- Notify staff of heightened security needs; temporarily discontinue non-critical remote access; and shut down any nonessential, unimpacted devices

4.3: Eradicate

Once you understand enough about the incident and attacker to respond safely, take steps to remove the attacker's foothold and persistence measures and attempt to close potential avenues for reinfection. You can do this by:

- Patching exploited vulnerabilities
- Removing unauthorized tools and scheduled tasks
- Removing malware and artifacts
- Reimaging systems where trust is low
- Rotating credentials (especially admin/service accounts) and reviewing privileged access
- Hunting for potential spread (e.g., adjacent systems, shared file servers, domain controllers, OT jump hosts)
- Validating that the attacker did not create new user or service accounts
- Applying fixes to OT devices (e.g., intelligent electronic devices [IEDs]/remote terminal units [RTUs]/ programmable logic controllers [PLCs]) after validating vendor guidance

4.4: Recover

After removing the attacker(s) from your systems, the focus is on returning to known-good operations by restoring and validating systems in a deliberate order. Actions in this phase typically include:

- Confirming the environment is clean enough to restore (e.g., no active command-and-control)
- Restoring from known-good backups after malware scans and integrity checks
- Rebuilding systems from gold images or hardened configurations where trust is uncertain
- Validating functionality and security before reconnecting to production
- Validating control room visibility, alarm integrity, and safe operating modes for OT/SCADA
- Coordinating with operations for staged re-energization or return-to-service [if applicable]

4.5: Learn

After operations return to normal and staff have had a chance to recover from any mental or physical strain associated with the incident, conduct a short review to identify opportunities to be more resilient to future attacks. This may include:

- Identifying what happened and why (e.g., root cause, initial access)?
- Identifying what worked and what was challenging (e.g., contacts, authority, tooling, backups)?
- Identifying what to improve for the future (e.g., controls, plans, training)?
- Updating the plan and contact list(s), as necessary
- Holding a tabletop exercise to validate updated plans, policies, and procedures

5 Communications and Legal

5.1: Communications

There are multiple aspects of communications that are important to consider ahead of and during an incident.

Communicating Internally and with External Partners

- Maintain contact information (including an offline copy) for internal and external incident response partners and update it regularly
- Identify alternate methods of communication if primary methods are unavailable
- Streamline communications to external partners to avoid duplication or mixed messaging
- After incident resolution, hold a debrief to get perspectives on the response process from staff and other stakeholders. This helps foster ownership and responsibility for improved response outcomes in the future.

Communicating to the Public

- Designate a POC and backup to communicate publicly during an incident
- Route all communications with the public through that spokesperson
- Avoid speculation and only share confirmed information
- Use plain language, avoid deep technical details
- Create a crisis communications plan with pre-approved templates for cyberattack messaging
- Provide the public with a single place to find updates (e.g., website, social media) and set an update cadence

5.2: Legal

Involving legal counsel early can help avoid potential legal issues in the aftermath of an incident. While your legal counsel is unlikely to be a cyber subject matter expert, they play an important role in guiding aspects of the response (e.g., evidence handling, notifications, regulatory requirements, information sharing). Legal counsel can help:

- Confirm reporting obligations and timelines
- Review external statements and customer/employee notifications
- Coordinate with law enforcement and regulators, as necessary
- Preserve privilege, where applicable

6 Engaging Help

Many public power utilities do not have sufficient staff to handle major incidents alone. Engaging help early can help you manage severe incidents that overwhelm internal resources. As part of your incident response, consider engaging the following stakeholders:

- Vendors and service providers can help collect evidence and validate vulnerabilities and mitigations
- Incident response support (including forensics) can help with triage, incident scoping, containment, and eradication
- Cyber insurance providers may also provide (and may require the use of) incident response support resources
- Information sharing organizations (e.g., E-ISAC) can correlate threat information and help share mitigations or solutions
- Peer utilities can provide support, including via the Cyber Mutual Assistance program
- Some state and local governments may offer assistance, and APPA can help coordinate assistance from federal government partners if warranted
- Law enforcement can support the response if you suspect criminal activity, extortion, or other major impacts

Appendix A
Glossary

Acronym/Term	Definition
APPA	American Public Power Association
DOE	Department of Energy
Domains	Network or internet naming areas used to identify systems, services, or administrative boundaries
E-ISAC	Electricity Information Sharing and Analysis Center
Endpoints	User or system devices connected to a network, such as laptops, desktops, servers, mobile devices, or workstations
Exfiltration	Unauthorized movement or transfer of data out of an organization's systems or network
IEDs	Intelligent electronic devices
IP	Internet protocol
ISP	Internet service provider
IT	Information technology
Jump host	An intermediate, controlled system used to access restricted network segments or critical systems
Logs	Records of system, network, application, or security events that support monitoring, investigation, and incident response
MFA	Multi-factor authentication
MSSP	Managed security service provider
NDA	Non-disclosure agreement
OT	Operational technology
PLCs	Programmable logic controllers
POC	Point of contact
RTUs	Remote terminal units
SCADA	Supervisory control and data acquisition
Tokens/sessions	Authentication artifacts or active login sessions that allow continued access to systems or applications
VLAN	Virtual local area network

Appendix B

Incident Handling Form Templates

Incident handling forms can support incident response processes and are intended for internal use. The utility's legal team should oversee incident investigation, and all incident documentation should be done at the direction of legal counsel. The incident handling forms in this appendix were modeled after templates from the SANS Institute.

CYBER INCIDENT RESPONSE HANDLING FORMS **PAGE __ OF__**

CYBER INCIDENT CONTACT LIST

DATE UPDATED: _____

CYBER INCIDENT RESPONSE TEAM

Cyber Incident Response Manager

Name

Title

Phone

Mobile

Email

Address

Chief Counsel

Name

Title

Phone

Mobile

Email

Address

IT Technical Lead

Name

Title

Phone

Mobile

Email

Address

OT Technical Lead

Name

Title

Phone

Mobile

Email

Address

Public Affairs Lead	**Legal Affairs Personnel**
Name	Name
Title	Title
Phone	Phone
Mobile	Mobile
Email	Email
Address	Address

SAMPLE CRITICAL ASSET INVENTORY LIST DATE UPDATED:_____

This sample critical asset inventory list was developed using the North American Electric Reliability Corporation (NERC) report, *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets,* as a guide.

CRITICAL FUNCTION: POWER GENERATION

CRITICAL ASSET	CYBER ASSET	NETWORK ADDRESS	SYSTEMS USING CYBER ELEMENTS	RECOVERABILITY PRIORITY
Power Generator	[Entity-specific identifier]	123.123.1.2	Turbine Control System	[HIGH] [MEDIUM] [LOW]
Power Generator	[Entity-specific identifier]	123.123.1.2	Integrated Plant Control	
Power Generator	[Entity-specific identifier]	123.123.1.2	Continuous Emissions Monitoring System (CEMS)	

CRITICAL FUNCTION: GRID OPERATIONS

CRITICAL ASSET	CYBER ASSET	NETWORK ADDRESS	SYSTEMS USING CYBER ELEMENTS	RECOVERABILITY PRIORITY
Control Center	[Entity-specific identifier]	123.123.1.2	SCADA Supervisory Control	[HIGH] [MEDIUM] [LOW]
Control Center	[Entity-specific identifier]	123.123.1.2	State Estimator	
Control Center	[Entity-specific identifier]	123.123.1.2	Print Server	

CRITCAL FUNCTION: TRANSMISSION SUBSTATIONS OPERATIONS

CRITICAL ASSET	CYBER ASSET	NETWORK ADDRESS	SYSTEMS USING CYBER ELEMENTS	RECOVERABILITY PRIORITY
Transmission Substation	[Entity-specific identifier]	123.123.1.2	Protective Relaying	[HIGH] [MEDIUM] [LOW]
Transmission Substation	[Entity-specific identifier]	123.123.1.2	Phasor Measurement Unit (PMU)	
Transmission Substation	[Entity-specific identifier]	123.123.1.2	Special Protection Systems (SPS)	

INCIDENT IDENTIFICATION

DATE UPDATED:_____

Incident Detector Information

Name

Date and Time Detected

Title

Phone Mobile

Initial Response Action

Email

Organization

Additional Information

Incident Summary

Type of Incident Detected:

☐ Denial of service (DoS) ☐ Malware ☐ SQL injection

☐ Cyber-physical ☐ Phishing ☐ Man-in-the-middle attack ☐ Zero-day exploit

Incident Information:

Attack vector:

Asset:

Function:

Site (if applicable):

Point of Contact:

Phone:

Mobile:

Email:

Address:

Additional Information:

How was the Incident Detected?:

INCIDENT CONTAINMENT

DATE UPDATED:_____

Isolate impacted systems:

Cyber Incident Response Team Manager approved removal from network? ☐ YES ☐ NO

If YES, date and time systems were removed

If NO, state the reason

Backup impacted systems:

System backup successful for all systems? ☐ YES ☐ NO

Name of person(s) who performed backup

Backup start date and time:

Backup completion date and time:

Backup tapes sealed? ☐ YES ☐ NO Seal Date:

Backup tapes contact

Backup location

Name Date

Signature

INCIDENT ERADICATION

DATE UPDATED:_____

Name of persons and organizations performing forensics on systems:

Name Organization

Phone Email

Name Organization

Phone Email

Name Organization

Phone Email

Was the vulnerability and attack vector identified? ☐ YES ☐ NO

Describe:

What was the validation procedure used to ensure the incident was fully eradicated?

Describe:

Appendix C:

DOE Electric Emergency Incident and Disturbance Report (DOE-417)

DOE, under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. The Electric Emergency Incident and Disturbance Report (Form DOE-417) collects information on electric incidents and emergencies. Schedule 1 and lines N-S in Schedule 2 of the form must be submitted to DOE only when at least one of the thirteen criteria on page one of the form is met. Form DOE-417 must be filed either within one hour or six hours of the incident, depending on the type of incident. For cyber incidents, Schedule 2 line T, Cyber Attributes, must also be filled out.

Cyber-specific events that necessitate filing are bolded below:

Report within one hour	Report within six hours
Physical attack that causes major interruptions	Physical attack that could potentially impact electric power system adequacy or reliability
Reportable Cyber Security Incident (as defined by NERC)	Cyber event that could potentially impact power adequacy or reliability
Cyber event that is not a Reportable Cyber Security Incident that causes operation interruptions	Loss of service to more than 50,000 customers for 1 hour or more
Operational failure or shutdown of the transmission and/or distribution electrical system	Fuel supply emergencies that could impact power system adequacy or reliability
Electrical system separation (islanding)	
Uncontrolled loss of 300 MW or more for more than 15 minutes	
Firm load shedding of 100 MW or more	
System-wide voltage reductions of 3% of more	
Public appeal to reduce use of electricity to maintain power continuity	

Electric utilities that operate as reliability coordinators or balancing authorities as well as other utilities — in cases where a balancing authority or reliability coordinator is not involved — must adhere to this reporting requirement. Failure to do so may result in criminal fines, civil penalties, and other sanctions as permitted by law.

DOE Report Filing

DOE's Pacific Northwest National Laboratory has the DOE-417 reporting form on its website. Submit the DOE-417 Event Reporting Form via one of the following:

Online: https://doe417.pnnl.gov/
Fax: (202) 586-8485
Telephone: (202) 586-8100

2451 Crystal Drive
Suite 1000
Arlington, Virginia 22202-4804

www.PublicPower.org

202-467-2900