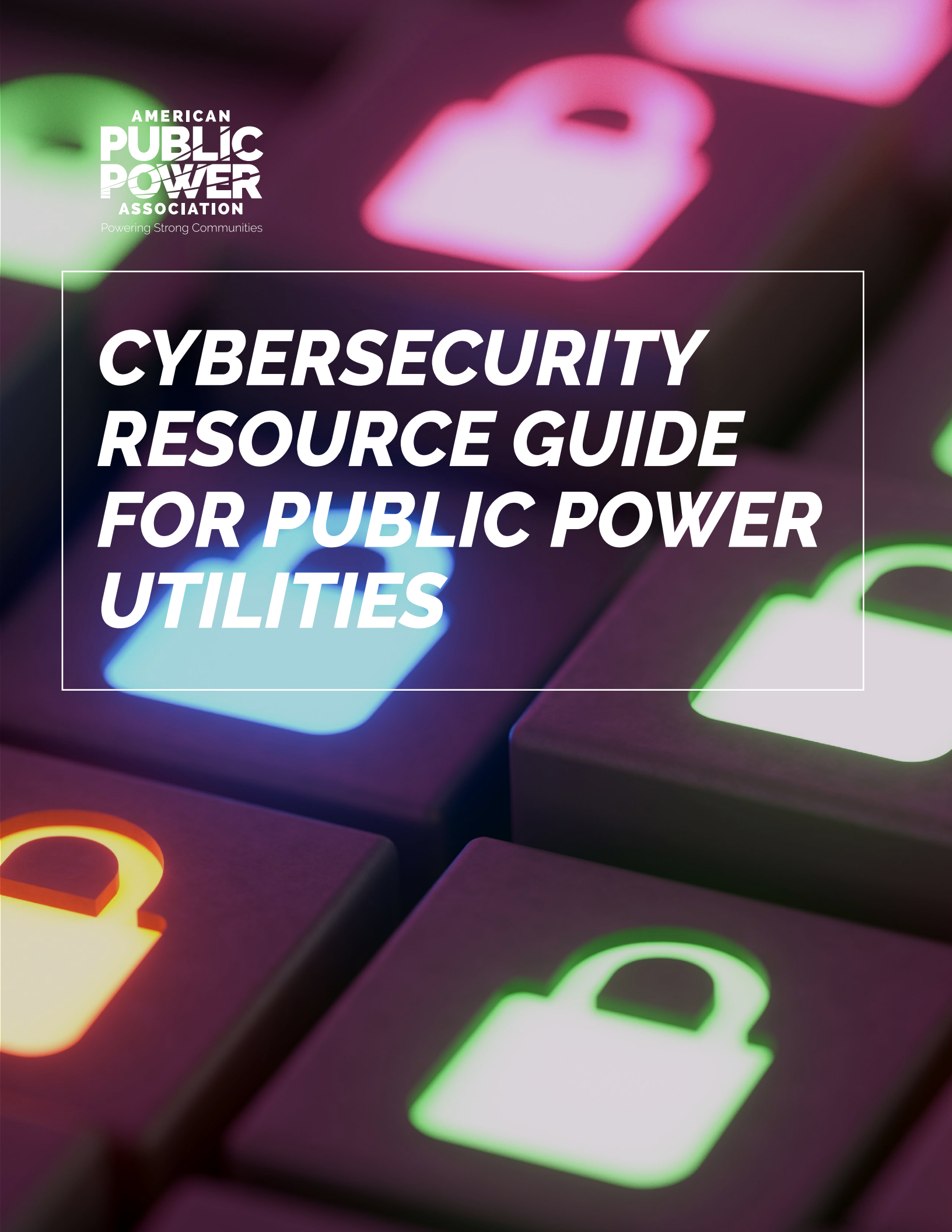



# CYBERSECURITY RESOURCE GUIDE FOR PUBLIC POWER UTILITIES

This material is based upon work supported by the Department of Energy under Award Number DE-CR0000012.



The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million customers that public power utilities serve, and the 96,000 people they employ. We advocate and advise on electricity policy, resilience, cybersecurity, grid operations, technology, trends, and training.

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

# CONTENTS

# INTRODUCTION

Communities served by public power utilities depend upon the reliability and resiliency of the critical energy infrastructure every day. Public power utilities have sensitive utility data stored within their information technology (IT) and operational technology (OT) systems, and they also have sensitive data on employees and customers. Attacks to critical infrastructure systems can jeopardize this data and our nation's security, economy, public safety, and health.

Implementing and sustaining cybersecurity best practices is the first step to protecting against cyberattacks, breaches and other incidents. The American Public Power Association (APPA) acknowledges the importance of protecting the confidentiality, integrity, and availability of critical infrastructure systems and digital assets. This comprehensive, high-level cybersecurity guide, developed by APPA, offers reliable industry guidance and resources aligned with a high level outline of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (Framework). The NIST Framework can help organizations reduce risks and understand industry best practices under five core functions: identify, protect, detect, respond, and recover. Organizations can also use the Framework to set a baseline for their current cybersecurity maturity and revisit the Framework to assist in benchmarking progress.

# HOW TO USE THIS GUIDE

Utilities serving small and medium municipalities, especially those seeking to enhance their cybersecurity programs, can use this guide to help identify resources and methods for assessing and addressing cybersecurity protections using a risk-based approach. The first step is to establish program governance and executive commitment, which includes selecting an appropriate framework upon which to build and manage your Program. This step is generally followed by a risk assessment using the identified framework.

Resources in this Guide are organized and listed in two ways: first, those that are related to each of the five core functions of the NIST Framework; and second, examples of primarily free resources offered by various trusted agencies and organizations. Utilities interested in understanding "how to get started" and "what to do" can go straight to the Five Core Functions and Associated Resources section. For those interested in a more detailed understanding of the NIST Framework and how else these resources can be used should continue reading from here.

# NIST CYBERSECURITY FRAMEWORK OVERVIEW

In February 2013, Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," called for a standardized security framework for critical infrastructure in the United States. In response, NIST published the Cybersecurity Framework (Framework) in February 2014, establishing a comprehensive and voluntary set of rules, guidelines, and standards created in collaboration with representatives from across critical infrastructures and is respected and utilized across the private and government sectors. The NIST Framework is dedicated to improving cybersecurity governance and operations by facilitating a transition from a reactive organizational security posture to a proactive methodical approach. In 2022, NIST began the process for updating the Framework (still unreleased as of this writing).

## Introduction

The Framework is designed to: improve an organization's cybersecurity program based on practices that have been proven effective to enhance an organization's cybersecurity posture; foster stakeholder communication; and facilitate adaption of an enterprise risk management processes. It is a risk-based framework and incorporates customizable activities and best practices that can help organizations understand their risk tolerance levels and align compliance standards to any cybersecurity program. The five core functions (Identify, Protect, Detect, Respond, and Recover) provide a high-level, comprehensive view of an organization's management lifecycle for cybersecurity risk. The core functions also offer references for each subcategory that includes industry standards, guidelines, best practices, and desired baseline outcomes. NIST's Quick Start Guide (Publication 1271) is a helpful resource to start with and can be used to communicate the basic framework to various stakeholders.

## Using the Framework

The Framework does not prescribe a one-size-fits-all approach to risk management; rather, it enables organizations to identify distinctive risk factors and tolerance levels, and then to tailor their approach accordingly. The Framework is pertinent to organizations relying on technology, industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT).

It is imperative that utilities manage the evolving cybersecurity landscape that can open the energy industry to sophisticated threats and vulnerabilities. Risk management is the ongoing practice of identifying, assessing, and responding to risk. To manage risk, organizations must understand the likelihood that an event will occur and the potential resulting impacts. This critical information enables organizations and decision-makers to determine the acceptable level of risk for achieving organizational cybersecurity objectives and risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity goals, objectives, and cybersecurity expenditures. As a result, organizations can leverage the Framework to quantify and communicate adjustments uniquely defined for their

cybersecurity programs and decide how to mitigate, transfer, avoid, and/or accept risks dependent on the potential impact to the delivery of critical services the organization provides.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Applying these risk management processes allows organizations to prioritize decisions regarding cybersecurity and encourages recurring risk assessments and validation of business drivers. The Framework offers organizations the ability to select and direct investments in cybersecurity risk management.

Many organizations have taken advantage of the Framework's flexible and voluntary nature to implement it in a variety of ways. It enables cybersecurity requirements and risks to be communicated to diverse internal and external stakeholders including partners and suppliers. Framework profiles and roadmaps are completely customizable, allowing cost effectiveness for any budget.

The Framework can also be leveraged to identify opportunities to strengthen organizational practices within an existing cybersecurity program or provide the blueprint to establishing a new cybersecurity program. The Framework provides an end-to-end risk management conduit to facilitate communication across the organization and drives strategic decision-making at various organizational levels. The Framework is outcome-driven and scalable to any budget or organization size.

## Framework Categories, Subcategories, Functions and Resources

Per the *NIST Framework for Improving Critical Infrastructure Cybersecurity v 1.1;* the framework Core components are defined as follows:

- **Functions** establish basic cybersecurity activities at their simplest level. The five core functions are: identify, protect, detect, respond, and recover. Organizations can manage cybersecurity risks by using the functions as a guide to organize information, which can facilitate risk management decisions and focus attention and resources on relevant threats that might have an impact. The functions also align with existing methodologies for incident management and can help organizations prioritize investments in cybersecurity.
- **Categories** are subdivisions of a function that combine groups of closely related cybersecurity outcomes. Examples of categories include Asset Management, Identity Management and Access Control, and Detection Processes.
- **Subcategories** further divide each category into specific outcomes of technical and/or management activities. They provide a set of results that, while not extensive, help support achievement of the outcomes in each category. Examples of subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
- **Informative references** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each subcategory. The informative references presented in the framework core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the framework development process.

There are 23 categories and 108 subcategories. Functions and categories each have a unique alphabetic identifier and subcategories are referenced numerically.

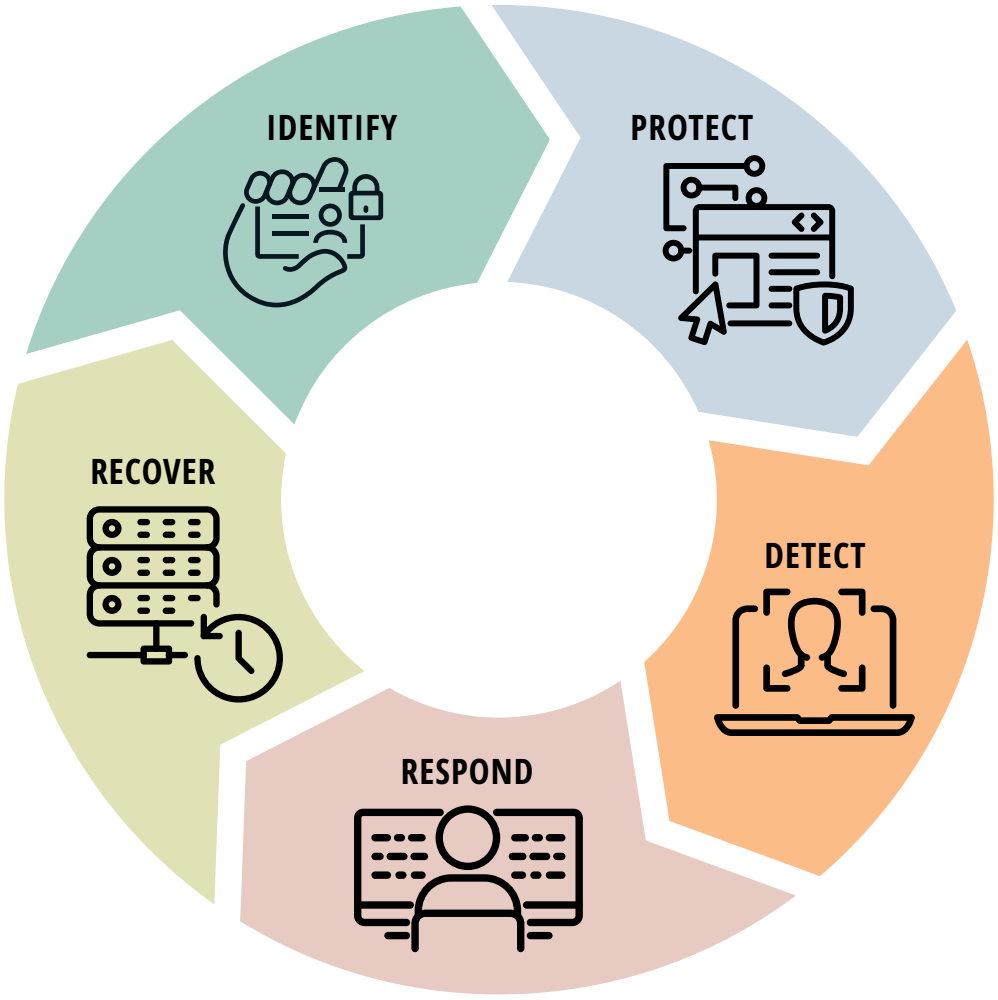
### Profiles and Tiers

Profiles support business/mission requirements and support communication within and between organizations. Using profiles, the Framework identifies business drivers to guide cybersecurity activities as part of the organization's risk management processes. Profiles can help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. They can also help organizations define their environment and identify opportunities to address cybersecurity risk management objectives within that environment to move forward.

Organizations can benchmark their organizational security posture along the Framework based on defined tiers. The four tiers — Partial, Risk Informed, Repeatable, and Adaptive — demonstrate the degree to which an organization's cybersecurity risk management practices and the desired outcome (described in the 108 subcategory statements) have progressed. Tier progression is based upon the increasing degree of risk management, organizational practice complexity, and risk responses. Going through each category and subcategories in the core function can help organizations to determine where they stand on the tier scale. The intentions of the tiers are to meet organizational goals at acceptable levels that are feasible for that particular environment. Tiers do not represent maturity levels but rather how an organization views cybersecurity risk and the processes in place to mitigate risks.

It's crucial that organizations select the most appropriate tier that meets the organization's goals to reduce risk to critical assets and resources. Progression to higher tiers can then be evaluated against a cost-benefit analysis indicating a feasible and cost-effective reduction of cybersecurity risk at the next tier.

# THE FIVE CORE FUNCTIONS AND ASSOCIATED RESOURCES




The five core functions, also known as the Framework Core, represent a cybersecurity lifecycle. Each function is essential to an organizational security posture and successful management of cybersecurity risk. This section of the guide describes the Framework core functions and lists resources (typically free) associated with each function for public power utilities to consider as they look internally at their cybersecurity posture. All resources included in this section are also listed in the compilation of resources by organization.

## Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcomes within this function include *Asset Management; Business Environment; Governance; Risk Assessment;* and *Risk Management Strategy.*

Below are some resources and publications that may be of assistance for addressing NIST CSF's core function "Identify". Please visit NIST for additional Identify resources and publications at www.nist.gov/cyberframework/identify

**CISA Cross-Sector Cybersecurity Performance Goals (CPGs):** As directed by President Biden's National Security Memorandum in 2021, DHS publicly released the cross-sector voluntary CPGs to supplement NIST's CSF with a focus for organizations "seeking assistance in prioritizing investment toward a limited number of high-impact security outcomes, whether due to gaps in expertise, resources, or capabilities or to enable focused improvements across suppliers, vendors, business partners, or customers." Sector specific voluntary CPGs are expected to follow but as of the writing of this guide have not yet started. The accompanying CPGs checklist — which gives you an ability benchmark yourself today vs a year from now — can be a handy resource to start addressing CSFs with a focus on what DHS has identified as some of the easier or higher impact activities. https://www.cisa.gov/cpg

**NIST Special Publication (SP) 800-82r3, Guide to Operational Technology Security (Draft 4/16/22),** provides guidance on how to improve the security of OT systems while addressing their unique performance, reliability, and safety requirements. This third revision of SP 800-82 provides an overview of OT and typical system topologies, identifies typical threats to organizational mission and business functions supported by OT, describes typical vulnerabilities in OT, and provides recommended security safeguards and countermeasures to manage the associated risks.

**CISA Cybersecurity Best Practices for Industrial Control Systems** provides an informative high-level graphic that can be used to communicate with stakeholders. www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

**Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2)** is a different framework that enables entities to conduct a self-assessment of their cybersecurity capabilities and use the results to optimize security investments. It describes a set of industry-vetted cybersecurity practices focused on both IT and OT assets and environments. This tool is available for free from the DOE, and includes a user-friendly C2M2 Self-Evaluation Tool available in HTML and PDF formats. The tool was developed to assist organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience.
www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

## Quick tips to jumpstart your organization's Identify activities

### Make a list of existing inventories of assets.

For example, purchasing records in each business unit, insurance policies, etc., might already include inventories of equipment, hardware, software, and data. A systematic walk-through can be used to develop an inventory of hardware, and there are tools to help identify existing software used in the utility. Conversations with staff in finance, human resources, operations, etc., can be used to create an inventory of sensitive data.


### Identify threats, vulnerabilities, and risks to assets.

There any many sources of cybersecurity threat information. Pick sources that are trusted and start receiving alerts and learning how to interpret the information provided. Combine this information with an understanding of what hardware and software assets are in the utility to help narrow down what threats are most relevant to a specific utility.

### Develop and share organizational cybersecurity policies and procedures.

Trusted relationships with colleagues can increase sharing of lessons learned and resources. Use appropriate formats to ask for examples from other utilities in the public power community.

### Establish organizational cybersecurity roles and responsibilities.

If everyone is responsible for cybersecurity then often no one is responsible. Establish clear cybersecurity responsibilities and expectations for different job roles within the utility. For example, staff with access to sensitive financial information or employee data might have different responsibilities than staff with the authority to impact energy system operations, and that might be different than staff responsible for communications and customer relations.

**CISA Cybersecurity Evaluation Tool (CSET),** offers onsite and self-assessment security control assessments, tools and consulting. Resources provided including mappings of the assessment questions to other control systems cybersecurity standards, and downloadable tools that can be used to do basic security assessments, network architectural review and verification, and network scanning to identify malicious activity and indicators of compromise, and penetration testing. www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

**CISA Cyber Resilience Review (CRR),** evaluates an organization's non-technical operational and cybersecurity practices. The CRR, available to use for free, may be conducted as a self-assessment or as an onsite assessment facilitated by Department of Homeland Security (DHS) cybersecurity professionals. The assessment determines existing organizational maturity and provides a gap analysis for process improvement based on industry best practices. www.cisa.gov/uscert/resources/assessments

**CISA Validated Architecture Design Review (VADR)** is an in-depth assessment of infrastructure based on federal and industry standards, guidelines, and best practices and includes architecture design review, system configuration and log review, and network traffic analysis. www.cisa.gov/cyber-resource-hub

**Public Power Cybersecurity Roadmap** outlines the steps public power utilities can take to improve their cybersecurity readiness, including developing a business plan and communicating the need for cybersecurity resources to management. www.publicpower.org/resource/cybersecurity-roadmap

**Axio360 for Public Power** is a benchmarking tool that enables public power organizations to assess their IT and OT cybersecurity posture against the C2M2 framework against a real-time dashboard with statistics. This also includes access to the Public Power Cybersecurity Scorecard, a short assessment mapped to the C2M2 framework that allows utilities to quickly assess their security posture and identify areas for improvement. Pricing for this tool varies based on customer count and is available through the APPA product store. https://my.publicpower.org/s/store

APPA offers several in-house cybersecurity training programs:

- **Cybersecurity 101: Putting Good Cyber Hygiene into Practice** is an introductory-level course focused on informing and raising awareness of general security concepts and industry best practices regarding safeguarding IT assets.
- **Cybersecurity Training for Management and Boards** provides the foundational knowledge necessary to help management-level employees and decisionmakers at utilities develop a holistic cyber and physical security program.
- **Cybersecurity Risk Management and Third-Party Management Fundamentals** covers how risk management concepts apply to OT cybersecurity and how to implement, demonstrate, and create cybersecurity policies and governance structures to manage risks.

## Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcomes within this function include *Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance;* and *Protective Technology.*

Below are some resources and publications that may be of assistance for addressing NIST CSF's core function "Protect". Please visit NIST for additional Protect resources and publications at www.nist.gov/cyberframework/protect

**Continuous Diagnostics and Mitigation (CDM)** works with partners across the entire Federal Civilian Executive Branch to disseminate and maintain an array of sensors for hardware asset management, software asset management and whitelisting, vulnerability management, compliance setting management, and feed data about an agency's cybersecurity flaws, and present those risks in an automated and continuously updated dashboard. www.cisa.gov/cdm

**CIS Controls Version 8** is a list of actions and best practices, referred to as Safeguards, that organizations can deploy to mitigate the most common cyber threats. Version 8 combines and consolidates the 18 CIS Controls by activities and has been enhanced to keep up with modern systems and software. www.cisecurity.org/controls/v8

**The Malicious Code Analysis Platform** is a web-based service that enables members of the MS-ISAC to submit suspicious files, including executables, dynamic link libraries, documents, quarantine files, and archives for analysis in a controlled and non-public fashion. Users can perform threat analysis based on domain, IP address, URL, hashes, and various indicators of compromise.
www.cisecurity.org/ms-isac/services

**Malicious Domain Blocking and Reporting service,** available to MS-ISAC members, prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
www.cisecurity.org/ms-isac/services/mdbr

**Remote Vulnerability Scanning and Penetrating service,** services are available to identify and assess external vulnerabilities. These tools simulate the tactics and techniques of real-world threats and adversaries and are designed to help organizations eliminate exploitable pathways in their infrastructure.
www.cisa.gov/cyber-hygiene-services

APPA offers several in-house cybersecurity training programs:

- **Cybersecurity 201 for Industrial Control Systems: Architecture, Asset Inventory, Network Security Monitoring & Event Detection** takes a technical focus to outlining a cybersecurity program in the ICS environment.
- **Intermediate Cyber Training for IT/OT Employees** is a mid-level course that reviews both IT and OT fundamental concepts and best practices, including utility-specific examples for enacting cybersecurity measures.

## Quick tips to jumpstart your organization's Protect activities

Maintain and control audit logs and supporting artifacts

Encrypt sensitive data during transit and at rest

Frequently test, update, and automate security software updates

Advocate for cybersecurity professional development, training, and awareness

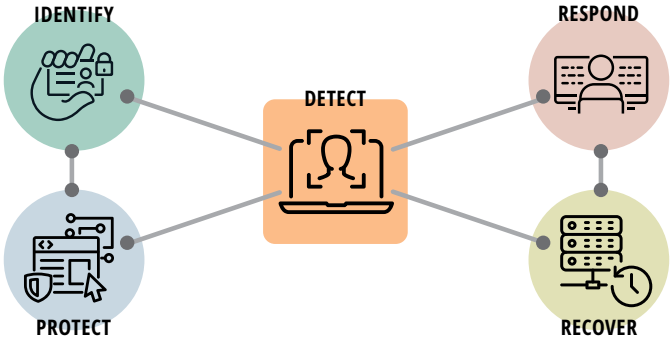
Use security software to protect and scan data for vulnerabilities and events

Regularly backup and store data

Generate formal policies and procedures for disposing of electronic files and devices

## Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events. Examples of outcomes within this function include *Anomalies and Events; Security Continuous Monitoring;* and *Detection Processes.*




Detect is at the intersection of proactively Identifying and Protecting your environments and reactively Responding and Recovering from threats and incidents.

Below are some resources and publications that may be of assistance for addressing NIST CSF's core function "Detect". Please visit NIST for additional Detect resources and publications at www.nist.gov/cyberframework/detect

**Cybersecurity Risk Information Sharing Program (CRISP)** enables and manages the near real-time sharing of IT threat information between participating U.S. electric utilities, DOE resources such as Pacific Northwest National Laboratory, and the E-ISAC. This collaboration among private and public energy sector partners facilitates timely bi-directional sharing of threat information and government informed data enrichment. The data collected through each participating utility's information sharing devices informs and enables improved situational awareness for the operator and strengthened defense of our national security. CRISP is a fee-based service open to U.S. asset owners and operators in the electricity, oil, and natural gas subsectors, as well as ancillary energy sector support organizations. www.eisac.com/s/crisp

**E-ISAC's Small and Medium Utilities Community Weekly Situation Report** may provide useful insights and highlights the most critical security updates and mitigations from the week, which the APPA cybersecurity team also shares with its members.

**IP Range and Domain Space Monitoring,** available to MS-ISAC members, monitors your public IP range and domain space. The MS-ISAC SOC will notify your organization via phone or email regarding evidence of: Web defacements; system compromises; compromised user credentials; IPs connected to a malicious command and control server; indicators of compromise from MS-ISAC network monitoring (Albert); and IPs connected to sinkholes or honey nets.

### Quick tips to jumpstart your organization's Detect activities

Monitor unauthorized access to networks, connections, data, systems, and devices

Monitor and investigate unusual network activities and events

## Respond

Develop and implement appropriate activities to act regarding a detected cybersecurity incident.

The Respond function supports the ability to mitigate the impact of a potential cybersecurity incident. Examples of outcomes within this function include *Response Planning; Communications; Analysis; Mitigation;* and *Improvements.*

Below are some resources and publications that may be of assistance for addressing NIST CSF's core function "Respond." Please visit NIST for additional Respond resources and publications at www.nist.gov/cyberframework/respond

**Public Power Cyber Incident Response Playbook** walks through the steps and best practices utilities can use to respond to a cyber incident. It provides guidance and templates for developing an internal cyber incident response plan based on feedback from the public power community. www.publicpower.org/resource/public-power-cyber-incident-response-playbook

**APPA Emergency Preparedness Tabletop Exercise in a Box** offers guidance and materials to host a tabletop incident response exercise, including checklists, guidance for facilitators, and after-action guidance. The kit includes several scenarios and prompts for cybersecurity incidents. https://my.publicpower.org/s/store#/store/browse/detail/a156g000004Dc5CAAS

### Quick tips to jumpstart your organization's Respond activities

Notify customers, employees and others of loss of data or other data risk

Test and plan for continuity of operations

Regularly update cybersecurity policies and capture lessons learned

Report incidents and attacks to the proper authorities as applicable

Investigate and isolate an attack

Prepare for events that put data at risk

**The Cyber Mutual Assistance Program** is an industry framework developed at the direction of the ESCC to provide emergency cyber assistance within the electric power and natural gas industries. The CMA Program is composed of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency. Participation in the program also establishes a voluntary information sharing agreement between CMA participants to improve the cybersecurity posture of all participants. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of the entities participating in the CMA Program. www.electricitysubsector.org/CMA

**CISA Tabletop Exercise Packages (CTEPs)** are designed "to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios." This is a customizable resource with template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources with scenarios covering a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.

**Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** offers vulnerability and malware analysis, onsite incident response and forensic analysis, intelligence and situational awareness, disclosure of vulnerabilities/mitigations release information, threat analysis and alerts, and virtual, instructor-led, and self-paced workforce development training courses. www.cisa.gov/ics

**GridEx** is a grid security exercise in North America that occurs every other year. GridEx offers E-ISAC members and partner organizations a forum to practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. Exercise participants receive customizable injects and materials that support utility response play at no cost.

## Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

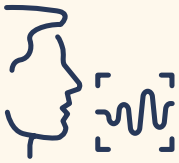
The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcomes within this function include *Recovery Planning; Improvements;* and *Communications.*

Please visit NIST for additional Recover resources and publications at

www.nist.gov/cyberframework/recover

### Quick tips to jumpstart your organization's Recover activities

Keep spare parts and equipment to repair and replace equipment affected by an event



Manage public relations and company reputation

Inform stakeholders of response and recovery activities

# ADDITIONAL PROGRAMMATIC RESOURCES

Various additional resources and programmatic tools are available to help municipal utilities to assess and invest in their cybersecurity posture or prepare to respond to cybersecurity incidents. Please note that all resources identified in this section can also be found in the compilation of resources by organization.

**DOE Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program** was first authorized by Congress in 2022 to provide funding to entities that have limited cybersecurity resources – prioritizing rural, municipal, and small investor-owned utilities that are critical to the reliability of the bulk-power system and/or those that own defense critical electric infrastructure. www.energy.gov/ceser/articles/rural-and-municipal-utility-advanced-cybersecurity-grant-and-technical-assistance

**Reliable Public Power Provider (RP3) program** recognizes utilities that demonstrate high proficiency in reliability, safety, workforce development, and system improvement, including cybersecurity procedures. It provides a pathway for benchmarking sector posture and comparing best practices against other public power utilities. www.publicpower.org/rp3-designated-utilities

**APPA-DOE Cooperative Agreements:** APPA has partnered with the Department of Energy on cooperative agreements, including those focused on improving cybersecurity in the public power community. These cooperative agreements provide APPA with funding to offer certain services and guidance to the public power community, such as the deployment of OT cybersecurity sensors to utilities or to develop training courses and publications. Resources developed through current and previous cooperative agreements can be found at: www.publicpower.org/topic/security-and-resilience-cyber-and-physical

**DOE Operational Technology Defender Fellowship** is a selective fellowship that offers middle- and senior-level OT security managers in the U.S. energy sector a chance to gain knowledge and understanding of cyber strategies and tactics. The fellowship is sponsored by DOE CESER and hosted by Idaho National Laboratory, with support from the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation. https://inl.gov/otdefender

# ADDITIONAL TRAINING AND COLLABORATION RESOURCES

Various additional resources are available, including numerous free trainings that are accessible to many municipal electric utilities as part of local government or as an owner/operator of a critical infrastructure. This section includes a few of the free trainings that can be considered. Please note that all resources identified can also be found in the compilation of resources by organization.

**CISA's Virtual Learning Portal** offers various courses and workshops. Refer to the CISA calendar for a schedule of these training options. Note that all CISA training courses are presented with no tuition to the attendee. www.cisa.gov/cybersecurity-training-exercises

**The Federal Virtual Training Environment (FedVTE)** offers free virtual cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans. https://fedvte.usalearning.gov

**The National Initiative for Cybersecurity Education (NICE),** from NIST, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Its mission is to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development. www.nist.gov/itl/applied-cybersecurity/nice

**The National Initiative for Cybersecurity Careers and Studies** is an online resource for cybersecurity training, education, and career information. NICCS connects government employees, students, educators, and industry with cybersecurity resources and training providers throughout the Nation. NICCS helps end-users to locate cybersecurity education and training resources needed advance their careers in cybersecurity and close the skill gaps across the workforce. https://niccs.cisa.gov/

**GridSecCon** is E-ISAC's annual conference that features world-class training sessions, cutting-edge discussions, and in-depth presentations on emerging cyber and physical threats, policy updates, and lessons learned.

**E-ISAC's Industry Industry Engagement Program** connects organizations with other E-ISAC members and partner organizations for engagement and collaboration.

**E-ISAC's Speaker Program** offers physical and cybersecurity experts for conferences, webinars, or other events.

**The Cybersecurity Defense Community** is a working group of public power utilities, joint action agencies, and state/regional associations that meet regularly to provide input and feedback on APPA's cybersecurity programs, industry/government cybersecurity initiatives (including conferences and events), cyber mutual aid, and publications.

**Cyber Communities & Information Sharing Paths:** APPA hosts listservs for members to share information and to discuss topics with their peers, including groups for Information Technology and Security. These listservs are restricted to employees of member utilities, joint action agencies, and state/regional associations. Interested participants may request to join APPA's listservs through our web form: www.publicpower.org/engage

# RESOURCES BY ORGANIZATION

## American Public Power Association

APPA has created reference resources to help our members in protecting their critical assets and data from cyber exploitation. Reference materials along that vein to date have included:

The **Reliable Public Power Provider, or RP3,** program recognizes utilities that demonstrate high proficiency in reliability, safety, workforce development, and system improvement, including cybersecurity procedures. It provides a pathway for benchmarking sector posture and comparing best practices against other public power utilities. www.publicpower.org/rp3

**Public Power Cybersecurity Roadmap** is designed to help utilities take the next step to improve their cybersecurity readiness, including developing a business plan and communicating the need for cybersecurity resources to management. www.publicpower.org/resource/cybersecurity-roadmap

**Public Power Cyber Incident Response Playbook** walks through the steps and best practices utilities can use to respond to a cyber incident. It provides guidance and templates for developing an internal cyber incident response plan based on feedback from the public power community. www.publicpower.org/resource/public-power-cyber-incident-response-playbook

**Emergency Preparedness Tabletop Exercise** in a Box offers guidance and materials to host a tabletop incident response exercise, including checklists, guidance for facilitators, and after-action guidance. The kit includes several scenarios and prompts for cybersecurity incidents. https://my.publicpower.org/s/store#/store/browse/detail/a156g000004Dc5CAAS

APPA provides additional cybersecurity information and resources at: www.publicpower.org/cybersecurity-resources

**Cybersecurity Training Programs**
**Cybersecurity 101: Putting Good Cyber Hygiene into Practice** is an introductory-level course focused on informing and raising awareness of general security concepts and industry best practices regarding safeguarding IT assets.

**Cybersecurity Training for Management and Boards** provides the foundational knowledge necessary to help utilities develop a holistic cyber and physical security program. It is aimed at management-level employees and decisionmakers to improve cybersecurity awareness at the highest levels of an organization.

**Cybersecurity Risk Management and Third-Party Management Fundamentals** provides training on risk management concepts as they apply to OT cybersecurity and how to apply, demonstrate, and create cybersecurity policies and governance structures to manage risks.

**Cybersecurity 201 for Industrial Control Systems: Architecture, Asset Inventory, Network Security Monitoring & Event Detection** takes a more technical focus to outlining a cybersecurity program in the ICS environment.

**Intermediate Cyber Training for IT/OT Employees** is a mid-level course that covers both IT and OT fundamental concepts and best practices, including utility-specific examples for enacting cybersecurity measures.

Additional information about these and other courses is available from the APPA Academy website: www.publicpower.org/house-training

**Axio360 for Public Power** is a benchmarking tool that enables organizations to assess their IT and OT cybersecurity posture against the C2M2 framework and access a real-time dashboard with assessment statistics. This also includes access to the Public Power Cybersecurity Scorecard, a short assessment mapped to the C2M2 framework that allows utilities to quickly assess their security posture and identify areas for improvement. Pricing for this tool varies based on customer count and is available through the APPA product store.
https://my.publicpower.org/s/store

**Cyber Communities & Information Sharing Paths:** APPA hosts a number of listservs for members to share information and to discuss topics with their peers, including groups for Information Technology and Security. These listservs are restricted to employees of member utilities, joint action agencies, and state/regional associations. Interested participants may request to join APPA's listservs through our web form: www.publicpower.org/engage

**APPA-DOE Cooperative Agreements:** APPA has partnered with the Department of Energy on several cooperative agreements, including agreements focused on improving cybersecurity in the public power community. These cooperative agreements provide APPA with funding to offer certain services to the public power community, such as the deployment of OT cybersecurity sensors to utilities or to develop training courses and publications. Resources and news about APPA's current and previous cooperative agreements can be found at: www.publicpower.org/topic/security-and-resilience-cyber-and-physical

**The Cybersecurity Defense Community** is a working group of public power utilities, joint action agencies, and state/regional associations that meet regularly to provide input and feedback on APPA's cybersecurity programs, industry/government cybersecurity initiatives (including conferences and events), cyber mutual aid, and publications.

## Department of Energy

DOE is the Sector Risk Management Agency (SRMA) for the electric sector, including for cybersecurity. With that role in mind, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is tasked with addressing cybersecurity, including partnering with industry as well as creating tools and resources for it. CESER is also responsible for Emergency Support Function 12 (ESF 12), which manages the federal government's response and recovery functions to the energy sector during an incident requiring coordinated federal response. For more details about CESER, please visit: www.energy.gov/ceser/

**Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (RMUC Program)** was first authorized by Congress in 2022 to provide funding to entities that have limited cybersecurity resources – prioritizing rural, municipal, and small investor-owned utilities that are critical to the reliability of the bulk-power system and/or those that own defense critical electric infrastructure. www.energy.gov/ceser/articles/ceser-announces-launch-rural-and-municipal-utility-advanced-cybersecurity-grant-and

**Cooperative Agreements:** The DOE regularly funds cooperative agreements aimed at improving cybersecurity within the public power community.

**Cybersecurity Capability Maturity Model (C2M2)** enables entities to assess their cybersecurity capabilities and optimize security investments. It applies a set of industry-vetted cybersecurity practices focused on both IT and OT assets and environments. There is a free, user-friendly C2M2 Self-Evaluation Tool available in HTML and PDF formats. The tool was developed to assist organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

**Operational Technology Defender Fellowship:** This selective fellowship offers middle- and senior-level OT security managers in the U.S. energy sector a chance to gain knowledge and understanding of cyber strategies and tactics. The fellowship is sponsored by the DOE and hosted by Idaho National Laboratory, with support from the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation. https://inl.gov/otdefender/

## National Institute of Standards and Technology

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The NIST OT Security Program includes multiple collaborative projects from across the NIST Information Technology Laboratory and Communications Technology Laboratory. www.nist.gov

**NIST Cybersecurity Framework Version 1.1** is a comprehensive resource that was created in collaboration with critical infrastructure owners and is dedicated to improving cybersecurity governance and operations by influencing an environmental transition from a reactive organizational security posture to a proactive methodical approach.

**NIST Publication 1271 Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide,** provides direction and guidance to improve cybersecurity risk management via utilization of the NIST Cybersecurity Framework.

**NIST Special Publication (SP) 800-82r3, Guide to Operational Technology Security (Draft 4/16/22),** provides guidance on how to improve the security of OT systems while addressing their unique performance, reliability, and safety requirements.

## Cybersecurity and Infrastructure Security Agency

CISA directs efforts to identify, control, and reduce risk to our national cyber and physical infrastructures. Industry stakeholders and government agencies work together to provide resources, analyses, and tools to help enhance cyber, communications, and physical security and resilient infrastructure for the American people. Leadership strategically oversees the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners. www.cisa.gov

DHS CISA has a services catalog that outlines by services available by categories of entity types – State, Local, Tribal & Territorial Governments (SLTT); non-profit sector; industry & private sector; federal departments and agencies; and academic institutions – in which public power can fall under multiple categories. www.cisa.gov/sites/default/files/publications/FINAL_PDFEPUB_CISA%20Services%20Catalog%202.0.pdf

Examples of CISA resources include:

**Trainings and Exercises** including in-person and virtual courses in addition to regional training courses and workshops in various locations.

- **The Federal Virtual Training Environment** offers free virtual cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans. https://fedvte.usalearning.gov
- **CISA Tabletop Exercise Packages** are designed "to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios." This is a customizable resource with template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources with scenarios covering a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.
- **CISA's Virtual Learning Portal** offers various courses and workshops. Refer to the CISA calendar for a schedule of these training options. Note that all CISA training courses are presented with no tuition cost to the attendee. www.cisa.gov/cybersecurity-training-exercises

**Cross-Sector Cybersecurity Performance Goals (CPGs):** As directed by President Biden's National Security Memorandum in 2021, DHS publicly released the cross-sector voluntary CPGs to supplement NISTs CSF with a focus for organizations "seeking assistance in prioritizing investment toward a limited number of high-impact security outcomes, whether due to gaps in expertise, resources, or capabilities or to enable focused improvements across suppliers, vendors, business partners, or customers." Sector specific voluntary CPGs are expected to follow but as of the writing of this guide have not yet started. The accompanying CPGs checklist, which gives you an ability benchmark yourself today vs a year from now, can be a handy resource to start addressing CSFs with a focus on what DHS has identified as some of the easier or higher impact activities. www.cisa.gov/cpg

**Cybersecurity Best Practices for Industrial Control Systems** provides an informative high-level graphic that can be used to communicate with stakeholders

cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

**Cyber Resilience Review (CRR)** is a free resource available to evaluate an organization's non-technical operational and cybersecurity practices. The CRR may be conducted as a self-assessment or as an onsite assessment facilitated by DHS cybersecurity professionals. The purpose of the assessment is to determine existing organizational maturity as well as provide a gap analysis for process improvement based on industry best practices. www.cisa.gov/uscert/resources/assessments

**Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** offers vulnerability and malware analysis, onsite incident response and forensic analysis, intelligence and situational awareness, disclosure of vulnerabilities/mitigations release information, threat analysis and alerts, and virtual, instructor-led, and self-paced workforce development training courses. www.cisa.gov/ics

**Continuous Diagnostics and Mitigation (CDM)** works with DHS and other partners across the entire Federal Civilian Executive Branch to disseminate and maintain an array of sensors for hardware asset management, software asset management and whitelisting, vulnerability management, and compliance setting management. CDM sensors feed data about an agency's cybersecurity flaws and present those risks in an automated and continuously updated dashboard. www.cisa.gov/cdm

**Cybersecurity Evaluation Tool (CSET)** offers onsite and self-led security control assessments, tools, and consulting. Resources provided consist of a mapping tool to control systems standards and downloadable tools that help conduct basic security assessments, network architectural review and verification, network scanning to identify malicious activity and indicators of compromise, and penetration testing. http://ics-cert.us-cert.gov/assessments

**Validated Architecture Design Review (VADR)** is an in-depth assessment of infrastructure based on federal and industry standards, guidelines, and best practices and includes architecture design review, system configuration and log review, and network traffic analysis. www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_VADR_508C.pdf

**Remote Vulnerability Scanning and Penetrating Testing** services are available to identify and assess external vulnerabilities. These tools simulate the tactics and techniques of real-world threats and adversaries and are designed to help organizations eliminate exploitable pathways in their infrastructure. www.cisa.gov/cyber-hygiene-services

## Electricity Information Sharing and Analysis Center

The E-ISAC offers its members and partners resources to reduce cyber and physical security threats to the North American electricity industry. Membership in the E-ISAC is free to electricity and gas asset owners and operators (the E-ISAC is funded via the North American Electric Reliability Corporation Assessment model, so no additional fees are required for utilities). The E-ISAC provides actionable products, programs, and services and offers situational awareness and analysis to its membership. The E-ISAC operates a secure portal that serves as a hub for secure bi-directional information sharing among members, partners, and analysts focused on the energy sector. The E-ISAC is firewalled from NERC compliance, and voluntary information cannot be used in regulatory action, ensuring a trusted sharing environment. www.eisac.com

E-ISAC programs include:

**GridEx** is a grid security exercise in North America that occurs every other year. GridEx offers E-ISAC member and partner organizations a forum to practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. Exercise participants receive customizable injects and materials that support utility response play at no cost.

**Cybersecurity Risk Information Sharing Program (CRISP)** enables and manages the near real-time sharing of IT threat information between participating U.S. electric utilities, DOE resources such as Pacific Northwest National Laboratory, and the E-ISAC. This collaboration among private and public energy sector partners facilitates timely bi-directional sharing of threat information and government-informed data enrichment. The data collected through each participating utility's information sharing devices informs and enables improved situational awareness for the operator and strengthened defense of our national security. CRISP is a fee-based service open to U.S. asset owners and operators in the electricity, oil, and natural gas subsectors, as well as ancillary energy sector support organizations. www.eisac.com/s/crisp

**GridSecCon** is an annual conference that features world-class training sessions, cutting-edge discussions, and in-depth presentations on emerging cyber and physical threats, policy updates, and lessons learned. www.eisac.com/s/gridseccon

**Industry Engagement Program** connects E-ISAC member and partner organizations with the organization for engagement and collaboration.

**Speaker Program** offers physical and cyber security experts for conferences, webinars, or other events.

**Small and Medium Utilities Community Weekly Situation Report** highlights the most critical security updates and mitigations from the week, which the APPA cybersecurity team also shares with its members.

## Multi-State Information Sharing and Analysis Center

The MS-ISAC provides real-time network monitoring and management, threat analysis, and early warning notifications through the 24/7/365 Security Operations Center (SOC). Membership in the MS-ISAC is free to state, local, tribal, and territorial government entities. In addition to providing cybersecurity resources — including daily tips, monthly newsletters, and guides, amongst others — below are some examples of additional tools they offer members: www.cisecurity.org/ms_isac

**IP Range and Domain Space** monitoring of your public IP range and domain space. The MS-ISAC SOC will notify your organization via phone or email regarding evidence of: Web defacements; system compromises; compromised user credentials; IPs connected to a malicious command and control server; indicators of compromise from MS-ISAC network monitoring (Albert); and IPs connected to sinkholes or honey nets.

**The Malicious Code Analysis Platform** is a web-based service that enables members to submit suspicious files, including executables, dynamic link libraries, documents, quarantine files, and archives for analysis in a controlled and non-public fashion. Additionally, the platform enables users to perform threat analysis based on domain, IP address, URL, hashes, and various indicators of compromise.
www.cisecurity.org/ms-isac/services

**Malicious Domain Blocking and Reporting** is a service that prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block most ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
www.cisecurity.org/ms-isac/services/mdbr

**Incident response and remediation** through a team of security experts.

**Trainings and webinars** across a broad array of cybersecurity topics.

## Electricity Subsector Coordinating Council

ESSC's Cyber Mutual Assistance (CMA) program is composed of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.

## National Initiative for Cybersecurity Education

NICE, led by NIST, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Its mission is to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development. www.nist.gov/itl/applied-cybersecurity/nice

## National Initiative for Cybersecurity Careers and Studies

NICCS is an online resource for cybersecurity training, education, and career information. NICCS connects government employees, students, educators, and industry with cybersecurity resources and training providers throughout the nation. NICCS helps end-users to locate the cybersecurity education and training resources needed advance their careers in cybersecurity and close the skill gaps across the workforce. https://niccs.cisa.gov/

## Center for Internet Security

CIS is home to MS-ISAC®, the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. state, local, tribal, and territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

**CIS Controls Version 8** is a list of actions and best practices, referred to as Safeguards, that organizations can deploy to mitigate the most common cyber threats. Version 8 combines and consolidates the 18 CIS Controls by activities, rather than by who manages the devices, as was the case in past versions of the controls. www.cisecurity.org/controls/v8

# APPENDIX

## Acronyms

**APPA** American Public Power Association

**C2M2** Cybersecurity Capability Maturity Model

**CDC** Cybersecurity Defense Community

**CDM** Continuous Diagnostics and Mitigation

**CEA** Cybersecurity Enhancement Act of 2014

**CESER** Cybersecurity, Energy Security and Emergency Response (DOE office)

**CIS** Center for Internet Security

**CISA** Cybersecurity and Infrastructure Security Agency

**CMA** Cyber Mutual Assistance

**COBIT** Control Objectives for Information and Related Technology

**CPG** Cross-sector Performance Goal

**CPS** Cyber-Physical Systems

**CRISP** Cybersecurity Risk Information Sharing Program

**CRR** Cyber Risk Review

**CSC** Critical Security Control

**CSET** Cybersecurity Evaluation Tool

**CSF** Cybersecurity Framework

**CTEP** CISA Tabletop Exercise Package

**DHS** Department of Homeland Security

**DOE** Department of Energy

**EO** Executive Order

**E-ISAC** Electricity Information Sharing and Analysis Center

**ESCC** Electricity Subsector Coordinating Council

**ESF** Emergency Support Function

**HTML** Hypertext markup language

**ICS** Industrial Control System

**ICS-CERT** Industrial Control System Cyber Emergency Response Team

**IoT** Internet of Things

**IP** Internet Protocol

**ISAC** Information Sharing and Analysis Center

**ISO** International Organization for Standardization

**IT** Information Technology

**MCAP** Malicious Code Analysis Platform

**MDBR** Malicious Domain Blocking and Reporting

**MS-ISAC** Multi-State Information Sharing and Analysis Center

**NICCS** National Initiative for Cybersecurity Careers and Studies

**NICE** National Initiative for Cybersecurity Education

**NERC** North American Electric Reliability Corporation

**NIST** National Institute of Standards and Technology

**OT** Operational Technology

**RMUC** Rural and Municipal Utility Advanced Cybersecurity grant and technical assistance program

**RP3** Reliable Public Power Provider program

**SLTT** State, local, tribal and territorial

**SOC** Security Operations Center

**SRMA** Sector Risk Management Agency

**SP** Special Publication

**VADR** Validated Architecture Design Review

AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804

www.PublicPower.org
#PublicPower