AMERICAN PUBLIC POWER ASSOCIATION

Powering Strong Communities

Cybersecurity Information

ENGAGEMENT PLAN

NOVEMBER 2017

This document was developed by Witt O'Brien's with technical and other support from Nathan Mitchell, Sam Rozenberg, and Alex Hofmann of the American Public Power Association.

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000811.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

AMERICAN PUBLIC POWER™ ASSOCIATION
Powering Strong Communities

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 people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

Table of Contents

Executive Summary

Every day brings new reports of cybersecurity attacks on computer networks. As part of a U.S. Department of Energy cooperative agreement, the American Public Power Association initiated a series of projects intended to enhance members' efforts to mitigate against and prepare for cyberattacks. The purpose of this project and the resultant report (and webinar) is to enhance public power providers' and external stakeholders' understanding of the unique needs of public power utilities regarding cybersecurity and to help member utilities develop and implement strategies and tactics to communicate regarding cyber-related threats and consequences to non-expert audiences.

Cyber Risk Environment

- Cybersecurity at public power utilities is often scattered across senior management, information technology (IT), operations, security, human resources (HR), and other functional areas. In some cases, primary responsibility might not even reside within the utility itself.
- Cyber risk and threat information from internal and external sources tends to arrive in a splintered and ad hoc manner.
- There is a broad disconnect between what utility managers believe elected local government board members and executives want to know and when they want to know it, and the *actual expectations* of those individuals.
- Cybersecurity is a growing concern, and public power utilities might not have the resources to address it.

Developing a Cybersecurity Program

- A single individual should own cybersecurity: A "Cybersecurity Program Lead" should manage the process for cyberintelligence information flow within the organization. This is a critical first step in establishing sound protocols and information exchange around cyber.
- Utilities should assess their cyber risk through self-evaluation of risks, vulnerabilities, resiliency, and capabilities related to cyber. Tools such as the public power Cybersecurity Scorecard exist to facilitate these assessments.
- All public power utilities should participate in cybersecurity training and scenario exercises. This should apply to anyone with access to the utility's systems and should include both onboarding and periodic refresher training.
- Public power utilities should maximize their awareness of cyberthreats and actively monitor their networks.
- All public power utilities should enroll in the Electricity Information Sharing and Analysis Center (E-ISAC).
- Public power utilities should have a documented plan for escalating notification and reporting on cyber incidents. This should be equally robust as plans for escalating operational incidents.
- Public power utilities should provide pre-incident outreach and education to local government leaders related to cyber. Such education should have two components: how an electric utility works and how cyberattacks can disrupt normal operations.
- Local government leaders must be provided with reporting on cyberthreats and incidents without allowing sensitive information to be inappropriately exposed.

Next Steps for Consideration by the Association and Industry Partners

- Deliver low-cost cybersecurity training and exercises.
- Develop a road map to guide public power utilities in developing their cybersecurity programs.
- Investigate how to develop the future security workforce.
- Develop a public power cyber-response playbook.
- Evaluate and deploy information-sharing tools and technologies.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Introduction

Purpose and Scope

The purpose of this document is to enhance public power providers' and external stakeholders' understanding of the unique needs of such utilities regarding cybersecurity. It provides a conceptual framework, supported by resources, templates, and training materials.

This document helps utilities convey cyber-related threats and consequences to non-expert audiences. It intends to drive information sharing and awareness engagement among utilities' operational staff, other employees, and organizational leadership; with industry organizations and peer utilities; and with federal, state, and local partners (including utilities' governance). The parameters for coordination are described both during "blue sky" conditions and when there are suspected, credible, or confirmed threats.

Specifically, this document supports public power providers as they address the following:

- Defining goals and objectives of information sharing.
- Defining the scope of information-sharing activities.
- Identifying internal and external sources of security information.
- Establishing information-sharing protocols.
- Identifying necessary ongoing activities to support information sharing.

Methodology

The content of this document is drawn from two primary sources during 2016 and 2017:

- Multiple interviews with (a) staff from Association members, including those in operational, IT, and management roles, and across the spectrum of small, medium, and large operations, and (b) representative elected and appointed officials with governance authority over public utilities; to facilitate a frank discussion, these interviews were conducted on the condition that no specific attributions would be made.
- Multiple interactions with public utility staff across the country while conducting Cyber and Physical Preparedness Facilitator-Led Exercise (CAPP-FLEX) tabletop exercises delivered under the Department of Energy (DOE) cooperative agreement, Task 1.5; these discussions were conducted on an Unclassified/For Official Use Only (U/FOUO) basis, meaning no reference to specific instances or sources is made in this report.

Recognizing and Identifying Relevant Risks

The primary outcomes of this Cybersecurity Information Engagement Plan are:

- To lay out programmatic benchmarks for public utilities' internal management and communication of cyber-threats.
- To establish an approach and protocol for exchanging information with external partners and stakeholders related to cybersecurity issues.

These outcomes are addressed under Findings and Recommendations.

Before either of these can be addressed, however, a public power utility must recognize the risks that it faces, both from the primary cyberthreat and from the act of exchanging information outside the utility. These issues are addressed below.

Recognizing Cyber Risks

Across public power utilities, there are many attitudes towards risk from cyberattacks. Below are several classifications of risk that utilities should consider as they evaluate their own risk and establish a readiness posture.[1]

While not every utility is a self-evident prime target for a deliberate, resource-intensive cyberattack, no public power utility is free from risk.

Ambient Risk of Connecting to the Internet

Even in the absence of any risk of deliberate cyberattack, any machine connected to the Internet is at "ambient" risk for automated attack from malware, ransomware, worms, viruses, etc. Such threats know no limitations. Moreover, notwithstanding the attractiveness of operational technology (OT) targets such as supervisory control and data acquisition (SCADA), the greatest risks in cyber relate to intellectual-information theft, specifically employee and customer personal information such as Social Security numbers, bank accounts, and credit card numbers. [2]

Nor does a lack of scale, or SCADA, insulate utility operations from such threats. Even a utility with manual operations and paper maps makes some use of computers. Whether for billing, distribution control, a call center, email or Voice over Internet Protocol (VoIP) communications, no electric utility operates in the modern age without some use of a computer, and computers get hacked.

Some of these baseline cyber risks can be mitigated through the use of robust IT security measures, including firewalls, sound password protocols, anti-phishing training, anti-virus and malware protection, regular system updates, etc. Other risks, however, will be beyond an organization's ability to control (e.g., a "zero day" compromise to a third-party software being utilized by the organization, which will leave the organization vulnerable until a patch is issued).

Other Risks for Cyber Incidents

Some utilities are not likely targets for deliberate, targeted attacks. However, even such smaller utilities can be victimized by unpredictable hackers, whether targeting personal information or OT. Examples include hackers who happen to be local to the utilities, disgruntled former employees, and inside threats.[3] Any of these may target customer or employee data or utility operations.

The American Public Power Association's *Cyber Security Essentials* guidebook details many of these inside threats. However, the latest data show that inside threats are now a much more serious threat than what is depicted in *Cyber Security Essentials*.

Targeted Cyber Attack

There are cases in which a public power utility is an obvious and visible target; in these, risk from cyberattack is clear. This is the case for utilities in large urban areas, with a large number of meters, significant generation or transmission capacity, or heavy reliance on SCADA, or those which power significant or high-visibility critical infrastructure and key resources (CI/KR) in any sector.

Such systems are likely to be at elevated risk of targeted cyberattacks, including customer or employee information theft, in addition to OT attacks such as SCADA disruption, digital denial of service (DDoS) attacks, or others. It should be noted that the threat of a SCADA or DDoS attack is always difficult to quantify, and many OT attacks can be countered by "old-fashioned" workarounds.

Even utilities that do not share the above features may be targeted by malicious actors, in the case that a cyberattack targets assets that can be affected by CI/KR powered by the utility. Examples include Federal Aviation Administration (FAA) beacons, rail crossing or operating signals, natural gas monitoring systems, or hazmat manufacturing, storage, and transport. There is generally little understanding or credence in the industry regarding the potential for this sort of attack vector.

Risk of Unsecured Information

The other major area in which risk must be recognized prior to any recommendations being offered is the potential for disruption caused by unsecured information exchange, especially outside of the utility itself. During an episode of concern regarding cyber risk, threat, or attack, communication may need to take place between operational staff within the utility and local government leadership.

There are many ways in which sensitive information can end up outside the privileged circle for which it is intended:

- Information might be disclosed during a public meeting.
- Information might be accessed via a Freedom of Information Act (FOIA) request or under sunshine laws.
- Recipients of information might deliberately take it to the media, whether on the record, off the record, or as "background," and/or they might anonymously "leak" documents.
- Recipients of information might post it to social media.
- Poor information-security protocols might allow outsiders (e.g., reporters) to access closed conference calls or to overhear conversations in a government building.

The discussion below addresses the risks of unsecured information; methods of securing sensitive information are addressed under Findings and Recommendations.

Operational Risk

The risk of sharing sensitive information in the operational setting is that such information might end up in the hands of the very malicious actors who are causing damage. Any available information about a utility's response strategies, timelines, or countermeasures can be assumed to provide an attacker a tactical advantage.

Political Risk

Sensitive information being released into the political arena can result in an issue being portrayed as larger than it actually is. In some cases, political actors will not understand the issues at hand; in others, they will seek to exploit the issues for personal or partisan advantage; and in still others they might publicize the issues because of a perceived obligation to inform the public. Once issues become linked to political narratives, it becomes increasingly difficult to manage them using a rational, objectives-based tactical response.

Media/ Public Information Risk

Unsecured, sensitive information which the media can access can create immediate reputational and media-management problems. Unlike a loose-lipped politician, the media's job really is to inform the public. If a utility or local government has a close relationship with a responsible media outlet, that outlet may withhold sensitive information if it believes doing so is in the public interest; but it will likely not hold the whole story indefinitely, and it is unlikely to spike a newsworthy story simply because of embarrassment to the utility.

Fiscal/Financial Risk

Information that is inappropriately publicized might also result in fiscal/financial consequences. A utility (or local government) that is perceived to be at risk from cyberthreats might have a more difficult time obtaining commercial credit, and its bond rating may be adversely affected. In fact, to date in 2017, the bond-rating agency Moody's has issued two reports through its Infrastructure and Project Finance desk advising investors of the risks of cyberattacks on utilities, and of the resultant potential for downgrade of bond ratings. Moody's most recent report was on June 16, 2017.

Findings and Recommendations for Public Power Utilities

These findings and recommendations address baseline standards for a cyber program at public utilities, and for development of processes and protocols for internal and external information exchange related to cyber, including securing information in an open environment.

Cybersecurity Program

The first prerequisites to deploying an effective cyber program are to recognize cyber as a per se program area and to consolidate related responsibilities within an accountable organizational structure.

Program Ownership

FINDING 1.A: As concerns over cybersecurity at utilities and other organizations have evolved in recent years, program ownership has not always been consolidated.

Cyber at public power utilities is often scattered across senior management, IT, operations, security, HR, and other functional areas. In our research, we found some organizations with a dozen or more uncoordinated staff "touch points" for cyber issues. In some cases, primary responsibility over cyber issues might not even reside within the utility, but rather at a third-party contractor, or with a non-utility municipal or county IT department.

RECOMMENDATION 1.A: A single individual — a "Cybersecurity Program Lead" — should own the cybersecurity "portfolio" for each public power utility. This is a critical first step in establishing sound protocols and information exchange around cyber. Even if primary technical management of cyber capabilities is external to the organization (whether located elsewhere in a municipal government or contracted to third-party vendor(s)), someone internal to the utility must have unified program ownership (i.e., serve as liaison to the external capability) for the utility itself.

Potential baseline minimum responsibilities for the Cybersecurity Program Lead position include the following:

- Develop and oversee cyber-risk assessment processes and findings, including corrective actions (see Recommendation 2).
- Establish and monitor employee behavioral training related to phishing, Internet use, social engineering (manipulating and deceiving people to get them to reveal confidential information or perform an action they might not otherwise do), etc. (see Recommendation 3).
- Coordination of cyber-risk information with business continuity and disaster recovery plans and capabilities (see Recommendation 4).
- Receive, coordinate, assess, and distribute cyberintelligence from internal and external sources (see Recommendations 5-6).
- Establish and monitor internal and external communications and reporting related to cyberthreats (see Recommendations 7-10).

The Cybersecurity Program Lead position should have a primary and a backup (contingency) staff member fully trained to execute its function.

Note that depending on the size of the utility, the Cybersecurity Program Lead role may be assigned to an existing position in the organization, and it may be only a percentage of his or her overall area of responsibility.

Defining Goals of Information Sharing

RECOMMENDATION 1.B: Prior to any determination of how and when to share information about cyberthreats and attacks, each public power utility should define goals for such information exchange.

This Cybersecurity Information Engagement Plan cannot define such goals for any given utility, as organizations of various scales, locations, and missions will have different goals. However, goals will likely address some variation of the following:

- Establishment and maintenance of internal situational awareness related to cyber risk and threats.
- Transparency to governing entities (boards, city council and mayors, governors and other entities).
- Required reporting to federal and other regulators (state Public Utility commissions, NERC, FERC, etc.).
- Contribution to industrywide situational awareness/common operating picture (joint action agencies, regional

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

cybersecurity groups, the American Public Power Association, E-ISAC, ESCC).

Risk Management

Properly addressing risk, including conducting information exchange related to such risk, first requires a public power utility to understand the various facets of its own risk and vulnerability to cyberthreats.

Self-Assessment of Organizational and IT Risk

FINDING 2.A: In our work in the field, we have encountered few utilities that have applied rigorous risk assessments to their own operations. Many public power utilities may also be subject to risks originating outside their organizations, whereas many share IT environments with other city departments or third-party vendors.

RECOMMENDATION 2.A: Utilities should undertake self-evaluation of risks, vulnerabilities, resiliency, and capabilities related to cyber. Tools exist to facilitate extremely robust and in-depth assessments. These include the Association's Public Power Cybersecurity Scorecard for resilience and security, DOE's more complex ES-C2M2 risk and capabilities evaluation program, and other frameworks referenced in the *Cyber Security Essentials* guidebook and elsewhere.[4] These models support evaluation, baselining, and progress-tracking. They are best practices for assessment of physical, operational, and procedural risk.

(See also relevant actions for the Association, under Next Steps).

Assessing and Mitigating Third-Party and Related Risks

FINDING 2.B: Even a utility with no internal weakness to cyberattack may yet be vulnerable to malicious actors attempting to access its networks and systems. Any other connected network or system, whether hosted by the local government or a vendor, can provide an access point.

RECOMMENDATION 2.B.I: Utilities need to know what systems dovetail with their own, particularly if these are systems over which they have no direct control. They should map what other systems touch those, potentially at a third-degree, or more, away from the utility itself. (This should all be addressed as part of an organization's cyber-risk assessment.)

RECOMMENDATION 2.B.II: Utilities should develop benchmarks for third-party liability and decline to contract with vendors unwilling to meet the criteria. This must extend not just to IT vendors per se, but to any vendor (e.g., HVAC monitoring) that might have access to any part of the organization's network.

The cybersecurity benchmarks adopted by a public power utility — related to training, firewalls, disaster recovery, vendor liability, etc. — should also be adopted across all local government or other systems that intersect with the utility's.

RECOMMENDATION 2.B.III: As a matter of basic IT integration, the various systems across a utility — and any software or firmware that is connected to the utility's IT — need to have seamless interfaces. The related cybersecurity concern is that when such systems do not work well together, patches are typically needed; these can introduce instability and vulnerabilities that can be exploited. Therefore, interdepartmental coordination and quality assurance of IT needs, including identification, scoping, and procurement process, is crucial.[5]

RECOMMENDATION 2.B.IV: A utility's Cybersecurity Program Lead should be responsible for tracking industry-known vulnerabilities for IT systems and products which the utility uses or to which it is exposed. This is an element of ongoing risk awareness.

Employee Behavior

The behavior of employees and other individuals with access to public power utilities' IT or OT presents a risk that should be addressed by utilities and aligned under their Cybersecurity Program Lead.

Phishing Training/Testing Program for Anyone with Access to a Utility's IT or OT

FINDING 3.A: In most cyberattacks, whether targeted intrusions or automated phishing, the weakest point of entry into a system is provided by "social engineering," (i.e., leveraging lax employee behavior regarding cybersecurity).

RECOMMENDATION 3.A: All public power utilities should maintain a two-part training and testing program. This should include both onboarding and periodic refresher training, in addition to periodic testing. Testing should feature random simulated phishing attempts on a regular basis (e.g., monthly). The organization should establish a protocol with consequences for clicking the "bait" email. For example, the first infraction might generate a warning, the second might lock an employee's computer until a required training is completed, the third might call for some specified punitive action, and the fourth would mean a referral to HR.

Furthermore, utilities should consider which other individuals have access to their networks or systems. These might include municipal employees, third-party vendors, and elected or appointed government officials. Public power utilities should explore ways of extending requirements of sound cyber-practices and training to these audiences as well.

There are several off-the-shelf training and testing solutions available on the market that are targeted to phishing and employee behavior; many of these are quite affordable. In some regions, joint action agencies have made licenses to such training programs available to members at discounted rates.

Onboarding Protocol

FINDING 3.B: A common but significant lapse in employee training exists between new hires and onboarding trainings. In many organizations, onboarding cybersecurity training is offered only at designated times (for example, biannually). The result is that new hires are allowed work on machines and connect to enterprise networks, operational systems, and the internet before having cybersecurity training. NERC standards (CIP-004) prohibit this practice, but most public power utilities are not subject to NERC.

RECOMMENDATION 3.B: As a best practice, all employees of public power utilities should receive cybersecurity training before being allowed to access any of the organization's computers or networks.

Business Continuity and Disaster Recovery

Public power utilities should align and integrate their proactive approach to cyber risk with Business Continuity and Disaster Recovery plans and resources.

FINDING 4: Although *prevention* of cyberattacks is a priority, public power utilities must also be prepared for the possibility of a successful attack. At that point, the organization's Business Continuity and Disaster Recovery plans become operative.

RECOMMENDATION 4: Business Continuity and Disaster Recovery plans should be formalized and taught, and procedures for maintaining accessibility to and operability of backup equipment and systems should be regularly exercised.

Although there are no sector-specific continuity and recovery standards for utilities, there are several industry standards, including:

- NFPA 1600
- ISO 22301
- FEMA Continuity Circulars 1 and 2
- BCI Good Practice Guides
- State and local guidance

Real-Time Risk and Threat Awareness

Once a baseline of program ownership and risk awareness has been established (through the preceding Recommendations), an organization can work through how cyber risk, threat, and attack information moves through an organization. Public power utilities have two basic sources for cyberthreat information: awareness of cyber concerns affecting the organization itself (internal), and intelligence provided to the organization from outside sources (external). Management of such information is addressed below.

Internal Awareness

FINDING 5.A: There are several ways utilities may become aware of an internal risk or suspected intrusion. However, these are only useful if there is a protocol in place to ensure that the information moves quickly to the organization's Cybersecurity Program Lead.

In our observations in the field, we saw no indication that employees were reluctant to share suspicions of cyberattacks with IT staff, nor that IT was reluctant to report such concerns up through chain of command.

However, despite their *willingness to report*, not all staff seemed to treat such issues as priorities that were *worthy of reporting*. Also, not all IT departments or staff have the technical expertise to understand the subtleties of utility-sector cyberthreats; in some small organizations, the IT department might be a single person whose main role is to serve as the "help desk."

RECOMMENDATION 5.A.I: Public power utilities should train all employees to immediately report such issues, even if they seem trivial, and to establish clear guidance on who must receive such reports (i.e., the Cybersecurity Program Lead).

RECOMMENDATION 5.A.II: Public power utilities should actively monitor their networks. Such a service would typically be provided by a third-party vendor, whether contracted directly by the utility or by a joint action agency that may then provide licensing to its members. (A model for this, using N-Dimension devices, is currently being piloted under the DOE cooperative agreement, Task 3.1.) However, such services might still require that someone at the utility can interpret the importance (or lack thereof) of malicious code to the particular organization.

External Intelligence and Information

FINDING 5.B: Information regarding threats across the utility industry is available to public power utilities from external sources, including:

- E-ISAC
- Federal agencies including the Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (DHS), and U.S. Department of Energy (DOE)
- State Fusion Centers, including those that have a cyberintelligence center
- Industry periodicals and listservs, such as InfraGard (an FBI public-private alliance)
- IT vendor advisories regarding risks, updates, and patches
- The Association's security forums

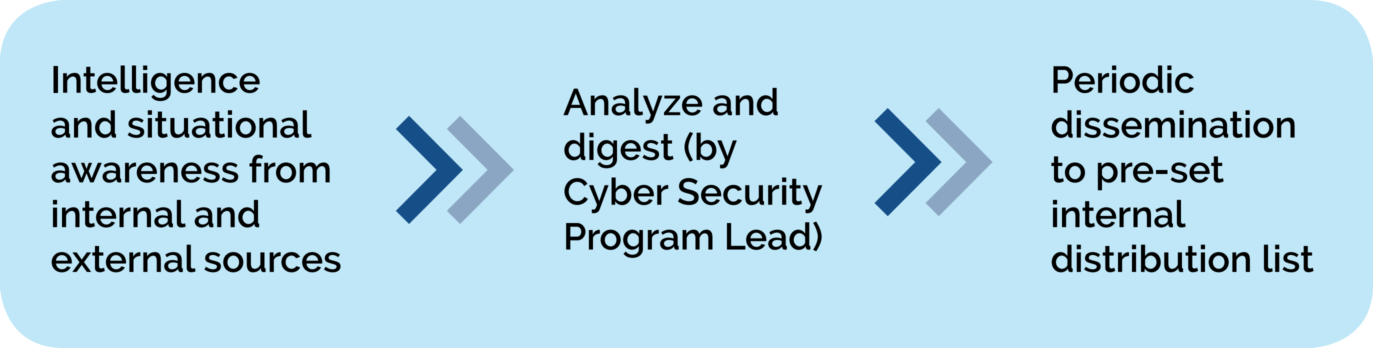
However, many people in the industry have voiced concerns that although the E-ISAC does issue useful information, this is often buried in "information overload," as the E-ISAC also issues a steady flow of notifications on issues of dubious relevance.

RECOMMENDATION 5.B: It is strongly and specifically recommended that all public power utilities enroll in the E-ISAC. However, no single agency or service can be expected or relied upon to possess all relevant intelligence, so redundancy is also recommended.

(See also relevant actions for the Association, under Next Steps).

Internal Information Flow

Although threat information is available, it does not always reach critical audiences. In our research in the field, we encountered many operational and IT staff who had not been aware of either the 2015 Ukraine attack or the 2016-17 Burlington media incident for weeks or months afterwards, if at all — notwithstanding that both incidents had been extensively reported in mainstream and industry



Intelligence and situational awareness from internal and external sources

Analyze and digest (by Cyber Security Program Lead)

Periodic dissemination to pre-set internal distribution list

media, and via cyberthreat notification systems. This section describes intake, analysis, and dissemination of information related to cyber.

Intake

FINDING 6.A: Many utilities already have staff that receive cyber-risk and threat information from one or more of the internal and external sources described in the preceding section. However, such information tends to arrive in a splintered and ad hoc manner. Utilities reported that anywhere from one to 15 staff independently receive various elements of cyber-risk intelligence from various sources. No utility reported any formal process for consolidating such information, relaying it, or preventing overlaps or gaps.

RECOMMENDATION 6.A.I: Public power utilities should designate the Cybersecurity Program Lead to function as a "funnel" for all incoming cybersecurity intelligence, regardless of the original source. Others in the organization should be free to engage cyberintelligence sources on their own, but no information should enter the organization without the awareness of the Cybersecurity Program Lead, who should receive and be accountable for all incoming intelligence.

RECOMMENDATION 6.A.II: Typically, incoming intelligence of this nature is marked "Unclassified" or "FOUO," meaning that no clearances are necessary for the Cybersecurity Program Lead. In the case that a utility has staff with higher security clearances that receive actionable cybersecurity information, the organization should have a protocol directing them to provide direction to the Cybersecurity Program Lead based on this intelligence, without violating the law by directly relaying any classified information.

Analysis

FINDING 6.B: Many utilities currently conduct some level of analysis of incoming cyberintelligence, but this process is often scattered, informal, and lacking accountability.

RECOMMENDATION 6.B: The Cybersecurity Program Lead, once in possession of all incoming cyberintelligence, should be responsible for consolidating, assessing, and analyzing it with reference to the specifics of that organization's operations, equipment, geography, and other particulars. Ideally, this should be performed daily. This can be a manual process to start, but it is recommended that some form of automated process be incorporated to manage the considerable amount of information.

Dissemination

FINDING 6.C: As with intake and analysis, most utilities currently conduct informal distribution of cyberthreat intelligence, but few have set protocols for such distribution, including periodicity or formal distribution lists.

RECOMMENDATION 6.C: The Cybersecurity Program Lead should be responsible for distributing digested intelligence to a preset distribution list, including minimally:

- The general manager (or equivalent)
- The director of utility operations (or equivalent)
- The IT director (or equivalent)

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

- Any individual(s), in addition to the Cybersecurity Program Lead, with direct oversight of cyber and/or physical security programs
- Counsel
- Any other personnel with a valid need for such information

Each utility should establish protocols for when and how often to distribute such information. Consideration should be given to making such distribution periodic and whenever a risk or threat has been identified, depending on organizational preference.

Escalation During Cyber Incidents

Public power utilities should have a plan for escalating the notification and reporting on cyber incidents, both within and outside the organization. This process should address all the topic areas laid out below.

Levels of Escalation

RECOMMENDATION 7.A: Each organization must define and describe the levels of potential escalation for notification regarding cyberthreats and who will be notified at each level, based on the organization's own characteristics, including:

- Scale
- Operational characteristics (e.g., use of SCADA, generation or transmission capability)
- Organizational structure
- Reporting structure
- Expectations of those receiving reports

In a small organization, the levels may include only, for example, the IT manager/Cybersecurity Program Lead, the general manager, and the mayor. In a large or more complex organization, there might be many more potential levels for responding to and/or further reporting an issue.

Triggers

RECOMMENDATION 7.B: Each organization must define and document "triggers" which demarcate conditions under which escalation to various levels is indicated. A few examples are provided below, for consideration:
General threat notification from industry sources, of general concern to all sectors.

- General threat notification from industry sources, specifically applicable to the utility industry.
- The threat specific to technology that is used by the organization.
- Suspicion of direct attempts to penetrate the system.
- Verification of direct attempts to penetrate the system.
- Suspicion of data compromise or that someone has successfully penetrated the system.
- Verification of data compromise or system penetration.
- Observable operational or other impact.

In the field, we also heard some utilities suggest triggering escalation when a situation becomes visible to the public or the media. We would suggest that this is not a viable trigger, because if the situation has reached this point without senior leadership awareness or involvement, it is probably too late for an effective response.

Deadlines

RECOMMENDATION 7.C: Each public power utility should work with potential recipients of reporting to establish deadlines. That is: What is the maximum duration of time after a trigger has been hit before reporting must occur?

Content and media

RECOMMENDATION 7.D: The content and medium for the reporting itself must also be defined. Minimally, any threat reporting should contain the following information:

- What the situation is.
- Who potentially or actually has been affected.
- What is being done in response.
- What additional options are available.
- Time of the next planned update, if applicable.

The media by which reporting takes place should also be described, whether by email, voice, or other means.

Top Level of Organizational Escalation

FINDING 7.E: In many utilities, there is a high level of comfort with escalating the notification and reporting of problems up to the level of general manager. However, for public power utilities, governance goes higher than that — to a board of directors, local government board, appointed city/county administrator, or elected county executive or mayor.

In our work in the field, we observed a broad disconnect between, on the one hand, what utility managers *believe* elected board members and executives want to know and when they want to know it and, on the other hand, the *actual expectations* of those individuals. Such a disconnect could be disastrous for a public power utility and its management if it were to manifest during a cyber incident.

RECOMMENDATION 7.E: Utilities should address governance stakeholders in their plans for escalating cybersecurity concerns and incidents; the general manager must not contain information exchange within the organization. This cannot be stated strongly enough: It is not the role of public power utilities to unilaterally determine what or when to report to local government leaders.

Public power utilities should understand what the individuals at their top level of escalation expect in terms of triggers, content, and timing. The best way to determine these expectations is simply to ask. It should be noted that these issues should be revisited as individuals at the top level are replaced; expectations for information sharing are highly individualized, and there is no industry standard upon which to fall back.

External Reporting

FINDING 7.F: NERC reporting requirements regarding cyberthreats and incidents are clear. The E-ISAC's reporting guidance, regarding what to report and how, is also clearly explained as part of the sign-up process.

Joint action agencies may or may not have reporting expectations; utilities should communicate with their joint action agencies to determine expectations.

RECOMMENDATION 7.F: Additional external reporting should therefore also be part of the process, including, for example, to:

- NERC
- E-ISAC
- A joint action agency
- The American Public Power Association

(See also relevant actions for the Association, under Next Steps).

Delegations

RECOMMENDATION 7.G: Finally, within the organization, any recipient or reporter of critical information must have a pre-delegated backup who is familiar with the issues at hand and trained to execute their role in response to an incident, including escalating reporting.

Implementing a Protocol

Most public power utilities have protocols for escalation of issues relating to normal operational concerns and outages. Every utility should also have a set protocol for escalation of issues related to cybersecurity that matches its operational escalation protocol in detail.

Establishing a Protocol

RECOMMENDATION 8.A: Creation of protocols related to escalation levels, triggers, deadlines, reporting content and channels, external reporting requirements, and delegations should be established. The Cybersecurity Program Lead should take the lead on organizing this effort.

Protocols should be created in dialogue with all stakeholders, and a workshop or tabletop exercise should be conducted to validate the protocols. Job aids such as rosters, contact information, reporting templates, and quick-look decision matrices should also be created.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Testing, Training, and Exercising

RECOMMENDATION 8.B: All primary and backup staff involved in escalation of cybersecurity issues should train on the protocols, and a schedule for testing and exercising should be established and maintained by the Cybersecurity Program Lead.

Communicating under "Blue Skies" with External Partners, Stakeholders, and Governing Oversight

As noted above, expectations from city councils, mayors, and other civil authorities related to communication regarding cyberthreats might not match the assumptions of public power utility general managers and staff. The best way to begin to bridge this gap is for utilities and their local government leaders to increase their communications when there is no crisis — that is, under "blue skies."

The net effect of such outreach and education described below will be that local government leaders attain a better understanding of their power system and a more trusting relationship with the people who manage and operate it. This puts local government leaders in a position to clearly state their expectations regarding notification during the cyber incident escalation process. It also gives them crucial knowledge to help manage communications in a crisis; because they have some understanding of which risks are real and which are not, they can meaningfully add their voices in ways that responsibly manage legitimate public concerns.

Education of Political Leadership

RECOMMENDATION 9.A: Pre-incident education of local government leaders by utility operations staff is crucial for determining mutually agreeable expectations and generally establishing a basis for smooth interactions during a cyber incident. Such education should have two components: how an electric utility works, and how cyberattacks can disrupt normal operations.

- Regardless of concerns about cybersecurity, every utility should educate its local government on the basics of utility processes, operations, and functionality. Leaders should understand what exactly their utility does (e.g., generation, transmission, or distribution), the scale of the utility's system, its assets, and its redundancies (e.g., power bought from the grid). Operational basics should also be covered, such as how a utility uses SCADA (or not), and how substations function and how they may be controlled.
- Once these basics are understood, utility staff can lay out the potential impact of cyber risks, so that local government leaders understand what risks are real and significant, and which are not. For example, in a utility that generates power but also buys off the grid, an attack on the generator might be manageable. Similarly, in a utility that uses SCADA but also has a sufficient labor force to manually reclose breakers, an attack on the SCADA might not result in a major interruption.

(See also relevant actions for the Association, under Next Steps).

Understanding Response Expectations

RECOMMENDATION 9.B: Local government authorities should be treated as partners in response, and therefore as a viable element of pre-incident planning. Public power utilities should, during planning, explicitly query city council members, mayors, etc., regarding their expectations and information needs.

Resources

FINDING 9.C: Cybersecurity is a growing concern, and public power utilities must have the resources to address it. This might imply increases in staffing, training, equipment, IT solutions, and other resources.

RECOMMENDATION 9.C: Utilities must be able to make the case to governing stakeholders for any needed resource increases, but they must do so without divulging specific vulnerability information.

Mutual Assistance

RECOMMENDATION 9.D: Public power utilities should work through their local governments and their industry peers to establish mutual assistance relationships that can be tapped during a cyber incident. Subject-matter expertise in cybersecurity, IT, continuity, recovery, public/media relations, and government relations will all be key roles. The Association has experts available for consultation and support mutual assistance efforts during an incident. The electricity industry's new Cyber Mutual Assistance (CMA) program may also be worth exploring.

Securing Information in an Open Environment

Providing local government leaders with reporting on cyberthreats and incidents is not without complications. Much of such reporting will be best kept internal. But once information enters into the political realm, it can be difficult to manage or contain. People have agendas; people react from fear; people misinterpret complex information. Guidance on potential means to help safeguard such information is provided below.

Understanding Public Meeting, Sunshine Laws, and Related Requirements

RECOMMENDATION 10.A: Before enacting any safeguards on exchange of sensitive information, public power utilities must understand the applicable federal, state, and local public meeting and "sunshine" laws; managers should consult with counsel on all related matters.

Closed-Door Meetings and Trusted Partners

RECOMMENDATION 10.B.I: The preferred venue for sharing sensitive information is in a closed-door meeting, and the preferred recipient of such information is a trusted partner. Closed-door meetings typically cover operational work sessions, including in an emergency operations center (EOC) or other public safety or security context, or in a small (non-quorum) meeting. Utilities should consult counsel for a full consideration of what meetings can be kept private and in what context.

RECOMMENDATION 10.B.II: The more sensitive issue is the proclivities of the recipient regarding such information. It is recommended that utilities work to identify individuals in elected office and oversight roles with whom sensitive information can be safely shared. Their colleagues must agree that these individuals will represent the local government for operational purposes during a cyber incident. These individuals may then opt to brief their colleagues at an appropriate time. Again, utilities should consult counsel to develop an appropriate protocol.

Executive Sessions

RECOMMENDATION 10.C: Although executive sessions are not open to the public or the media, utility managers should assume that information provided in executive session might end up in the media. Therefore, any information provided in this context should already be integrated into a broad and proactive media strategy.

Media and Public Information Strategy

RECOMMENDATION 10.D: When a utility does get in front of the media during a cybersecurity incident, this should be in the context of a well-staffed, strategic, and thorough media engagement plan. It might be appropriate to manage such efforts through a public information officer (PIO), a local government EOC, or counsel; the Association also advises members on media relations during crises.

- At a minimum, anyone talking to the media should receive approved talking points, and media training/coaching from a media professional (e.g., PIO). Utilities should maintain a state of readiness for response to cyberthreats that parallels or improves upon their preparedness for managing media during weather-related outages.
- Media strategy should include technical background briefings to bring nonspecialist journalists up to speed. Complex (and frightening) information, provided without sufficient context to nonspecialists, is a guarantee of misinterpretation and bad press.
- It is a best practice to have a prepared media strategy well in advance of a planned rollout, because there is never a guarantee that the release time of information can be controlled.

(See also relevant actions for the Association, under Next Steps).

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Next Steps for the Association

The following items are recommended as next steps for the American Public Power Association, whether under the DOE cooperative agreement or otherwise.

Provide resources and guidance for conducting self-assessments of cyber risk

Under the DOE cooperative agreement (Task 1.3), the Association is developing a Cybersecurity Scorecard for members to conduct their own internal risk assessments, and it has also directly provided risk assessments under the same DOE program (Task 2.1). As a follow-on to Task 2.1, the Association plans to develop a suite of tools for public power utilities to use to mitigate identified cyber risks.

Such support for utility risk assessments should be expanded and continued by the Association.

Vet external intelligence sources related to cyberthreats

Although E-ISAC intends to be a clearinghouse for cyberthreat information, multiple sources and perspectives always result in more robust intelligence. The Association should therefore evaluate and communicate to its members an array of potential sources for viable, timely, actionable, and reliable cyberthreat information.

Consolidate and streamline risk information from E-ISAC and other sources

Currently, many people in the industry deem E-ISAC notifications to be overly vague and/or prone to causing "information fatigue." Notifications of risk information should be rendered specific and actionable for utilities. The Association is exploring options for achieving this under the DOE cooperative agreement, Tasks 3.2, 4.1, and 4.2.

Specifically, the Association and others in the industry (including joint action agencies or state associations) should consider implementing:

- More aggressive filtering or digestion of the information from E-ISAC.
- Adopting the role of aggregating, analyzing, filtering, and assessing E-ISAC notifications to provide actionable intelligence (including suspect code and applicable patches), and/or issuing "red flag" notices in the case of an immediate concern.
- Convening industry calls when an issue of serious concern emerges, including advising specific actions, mitigation steps, or countermeasures.

Guidance for reporting cyberthreats and incidents to the Association and others

The Association should develop and issue guidance to members regarding the Association's reporting expectations related to cybersecurity threats and incidents. Similar expectations and requirements reflecting the interests of other entities and stakeholders could also be codified.

Member utilities should also be made aware that the Association may be positioned to provide support, guidance, or expertise during a cyber incident and any related media attention.

Tools for supporting outreach and education to local government stakeholders

The Association should develop content and curricula for conducting training and education of municipal boards, mayors, and others with oversight of public power utilities. Such content should address both the normal functioning of an electric utility and its system components (including infrastructure, OT, and IT), and general cyberthreats to those assets and systems. Such outreach and education may emerge from multiple Tasks under the DOE cooperative agreement, including the Information Assurance program (Task 4.4) and others.

Next Steps for the Association

Resources to support media interactions

Public power utilities would benefit from the Association providing the following resources to support media interactions:

- Webinars on media training.
- Pre-written scripts targeted to cyber scenarios, to be prepared and circulated to members for use during a cyber incident (e.g., data breach or SCADA exploitation).

Develop a secure cybersecurity information-sharing mechanism

To minimize the risk and effects of cyber incidents becoming known to the public, the Association might develop a secured and trusted mechanism for sharing information among utilities and other stakeholders. Under another task within this project, the Association is evaluating secure information sharing.

Updates to the Cyber Security Essentials Guidebook

The following suggestions are offered to update the Association's *Cyber Security Essentials* guidebook:

- Consider adopting the recommendations presented in this plan for presentation in future revisions of the guidebook.
- Develop and include additional case studies with realistic scenarios that will have an effect on small, medium, and large utilities. These will allow readers to better visualize the impact of an incident.
- The "defense in-depth" content (p. 12) should be expanded to include an outermost ring consisting of "outside the fence" intelligence and external liaison programs to agencies and industry associations. The Association should:
    - Direct all members to sign up for the E-ISAC.
    - Recommend sources with whom utilities can work directly or indirectly regarding cyber issues.
    - Act as an intermediary by assessing and digesting incoming threat intelligence for distribution to its members.
- Update statistics and charts/tables (e.g., p. 16 chart regarding the frequency of initiation of cyberattack from various vectors is out of date).
- The section on third-party management (p. 37) should be expanded.

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

End Notes

1. American Public Power Association, *Cyber Security Essentials*, p. 18
2. For customer personal-information security standards, see also the PCI-DSS Standard v3.2 (2016)
3. American Public Power Association, *Cyber Security Essentials*, p. 16
4. American Public Power Association, *Cyber Security Essentials*, p. 26; NIST Cyber Security Framework; guidance from NERC, IEEE, and ANSE
5. American Public Power Association, *Cyber Security Essentials*, p. 37

APPENDICES

Acronyms and Abbreviations

ANSE
BCI
CAPP-FLEX
CARVER
CI/KR
CMA
DDoS
DHS
EEI
E-ISA
EOC
ES-C2M2
FAA
FBI
FEMA
FOIA
FTE
DOE
IEEE
ISO
IT
NERC
NFPA
NIST
NRECA
OT
PCI-DS
PIO
SCADA
U/FOUO

American National Standards Institute Business Continuity Institute
Cyber and Physical Preparedness Facilitator-Led Exercise
Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability
Critical Infrastructure and Key Resources
Cyber Mutual Assistance
Digital Denial of Service
Department of Homeland Security
Edison Electric Institute
Electricity Information Sharing and Analysis Center
Emergency Operations Center
Electricity Subsector Cybersecurity Capability Maturity Model
Federal Aviation Administration
Federal Bureau of Investigation
Federal Emergency Management Agency
Freedom of Information Act
Full-Time Equivalent
Department of Energy
Institute of Electrical and Electronic Engineers
International Standards Organization
Information Technology
North American Electric Reliability Corporation
National Fire Protection Administration
National Institute of Standards and Technology
National Rural Electric Cooperative Association
Operational Technology
Payment Card Industry Data Security Standard
Public Information Officer
Supervisory Control and Data Acquisition
Unclassified/For Official Use Only

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

References to Other Publications

This document references several existing publications and resources, as described below.

Cyber Security Essentials (2012)

The Association's ***Cyber Security Essentials*** is referenced multiple times in this Cybersecurity Information Engagement Plan (see following appendix for excerpts from *Cyber Security Essentials*). The publication provides an excellent overview of issues and concerns related to cybersecurity for public power utilities. It educates utilities on essential cyber concepts, including:

- Enterprise versus operational security
- Risk equation
- Cyber vulnerabilities
- Defense in-depth
- Use of countermeasures
- Attack surface
- Exploitation of social engineering

In fact, many member utilities have voiced their desire for a document of guidance that provides precisely this sort of information — apparently unaware of this resource. Therefore, one of the Cybersecurity Information Engagement Plan's outcomes will be to drive utilities to use *Cyber Security Essentials*. Additionally, whereas the landscape of cyberthreats has evolved considerably since the guidebook's publication in 2012, the Association should consider an update to this valuable resource (see more under Next Steps).

Public Power Cybersecurity Scorecard

The Association is developing a Public Power Cybersecurity Scorecard under the DOE cooperative agreement. This tool will facilitate utilities in conducting their own internal risk assessments using a streamlined and simplified methodology derived from DOE's more complex ES-C2M2 risk and capabilities evaluation program. This Cybersecurity Information Engagement Plan recommends utilities conduct risk assessments to fully understand their own risks and vulnerability from cyberthreats.

Physical Security Essentials (2016)

The Association's *Physical Security Essentials* provides a basis for the approach and strategies described in this Cybersecurity Information Engagement Plan. *Physical Security Essentials* instead presents an overview of:

- Threat assessments, including CARVER (a tool developed by the U.S. military for target prioritization, which can be used "in reverse" for vulnerability assessments).
- Risk analysis, which assists a utility in identification of its threat(s).
- Identification of physical countermeasure best practices that are used throughout the utility industry.
- Support for prioritization of mitigation strategies and actions within a utility.

Physical Security Essentials further highlights the importance of coordination and information sharing, recognizing both as "key elements of a successful physical security program because they increase situational awareness, improve emergency response, and enhance each participant's understanding of the criminal landscape."

The Media Communications section of *Physical Security Essentials* emphasizes that "providing external stakeholders with accurate and timely information is important for maintaining trust and accountability with customers and the general public."

NIST *Cybersecurity Framework* (2017)

The National Institute of Standards and Technology (NIST) *Cybersecurity Framework* presents an extremely in-depth cyber evaluation. (NIST is a nonregulatory U.S. government agency that sets industry best practices.) This Cybersecurity Information Engagement Plan refers to the NIST *Framework* primarily in the context of best practices for baseline assessment of risk. The *Cyber Security Essentials* guidebook also references the NIST guidance (p. 26).

NIST *Guide to Cyber Threat Information Sharing* (2016)

The NIST *Guide* to Cyber Threat Information Sharing provides background on the approach to information sharing described in this Cybersecurity Information Engagement Plan. The NIST Guide promotes the sharing and exchange of cyberthreat information to assist organizations as they "identify, assess, monitor, and respond to cyber threats."

The publication also describes the benefits to organizations that share and receive cyberthreat information, while also emphasizing the importance of establishing a culture and environment of trust around sharing information. The *Guide* states, "The goal of the publication is to provide guidelines that improve cybersecurity operations and risk management activities through safe and effective information sharing practices, and that help organizations plan, implement, and maintain information sharing."

Cyber Security Essentials Guidebook

Below are excerpts from the *Cyber Security Essentials* guidebook, which can be purchased from the Association's Product Store using the link below:

https://ebiz.publicpower.org/APPAEbiz/ProductCatalog/Product.aspx?ID=4909

The publication provides an excellent overview of issues and concerns related to cybersecurity for public power utilities. It educates utilities on essential cyber concepts, including:

- Enterprise versus operational security
- Risk equation
- Cyber vulnerabilities
- Defense in-depth
- Use of countermeasures
- Attack surface
- Exploitation of social engineering

Enterprise versus Operational Security

This section states, "To illustrate the different 'bottom lines' between IT systems and utility operations systems, consider a common practice in IT software security: 'three wrong password entries and screen is locked.' The 'three strikes you're out' policy makes sense for IT environments, where it keeps unauthorized users out. But in a control room, during an emergency, with alarms going off, an operator under pressure could easily mis-key the password three times and be locked out of a critical control screen just when he or she needs to access the work station to adjust a critical parameter. A rule that makes sense in the IT environment may conflict with safe and reliable operation in the utility operations environment."

Risk equation

The Cyber Security Essentials guidebook educates the reader on the risk equation. It details:

"The risk equation, which governs physical or cybersecurity assets, has been written many different ways by various sources. One commonly used equation relates these terms:

- Threats: Who or what is attacking your system, either intentionally or accidently?
- Assets: The thing of value you want to protect, whether a substation, the data in a database, etc.
- Vulnerabilities: 'Chinks in your armor,' which may be exploited to do harm
- Consequences: Negative outcomes, such as loss or damage to your assets; and
- Risk = Consequence x Threat x Vulnerability"

Cyber vulnerabilities

"A software vulnerability, the 'chink in the armor,' is a way to force a software program to do things it was never intended to do. For instance, a hacker accessing a banking website could enter a certain sequence of characters by using an exploit called cross-scripting (XSS) and look at accounts of other users and perhaps change their account values. The hacker has just successfully exploited a vulnerability. With an exploit called a buffer overflow, by entering a specially crafted series of characters, a hacker could go from becoming an average user of software with no special privileges to one having the powers of a systems administrator, and could change the software on the computer in ways that only the IT staff should be able to do."

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Defense in-depth

“Defense-in-depth is the best practices approach to protect assets using overlapping and complementary modes of protection. These modes could be preventive (to deter and delay an attack), or detective (to warn of an attack in progress), or mitigative (to repair damage and restore to normal operation).”

Use of countermeasures

“At any stage in a physical or cyber attack, security controls may be introduced that: a) deter and delay the attack; b) detect the attack; or c) mitigate the attack.”

Attack surface

“An ‘attack surface’ refers to the components of the power system that expose hardware, software, and networks to vulnerabilities to someone who might want to perpetrate destruction. For example, in a typical electric distribution network, the attack surface could be:

- Substation electronics, relays, remote terminals units, sensors and SCADA interfaces
- Pole-top electronics, transformer, reclosers, etc. (distribution automation)
- Advanced meters on houses
- Wireless HAN within houses, using wireless protocol
- Wireless collection point for neighborhood smart meters, again on pole-tops”

Exploitation of social engineering

“Social engineering involves manipulating and deceiving people to get them to reveal confidential information or perform an action they might not otherwise do. Famed hacker Kevin Mitnick was a master of social engineering. His philosophy of hacking might be stated as ‘Why should I spend time on the computer hacking into a system, when I could trick users into giving up their passwords?’”

AMERICAN PUBLIC POWER ASSOCIATION™

Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804
PublicPower.org

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.