ASSESSMENT OF CYBERSECURITY FRAMEWORKS AND TOOLS FOR PUBLIC POWER

AMERICAN PUBLIC POWER® ASSOCIATION

Powering Strong Communities

ACKNOWLEDGEMENTS

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

The American Public Power Association thanks the members of the Cybersecurity Defense Community Working Group for their essential role in informing this report. We thank them for taking the time to discuss their experiences, needs, and practices. Support for the development and editing of this report was provided by:

CHRIS CHING
American Public Power Association

ANNA DETLOFF
American Public Power Association

RICHARD CONDELLO
American Public Power Association

ROB DENABURG
American Public Power Association

With assistance from Beam Reach Consulting Group

TABLE OF CONTENTS

1. INTRODUCTION

The Cyber Pathways program — a four-year cooperative agreement between the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and the American Public Power Association (APPA) — is a series of initiatives to help public power entities of all sizes and maturities on their cyber journey. An objective of this program is to evaluate and recommend effective cybersecurity assessment tools and frameworks that can be adopted by public power utilities, with a particular focus on options that are accessible to smaller, resource-constrained utilities. As such, the selected cybersecurity assessments must strike a balance between thoroughness and feasibility, enabling utilities to measure and track cybersecurity progress without imposing excessive burdens.

To effectively identify and analyze these tools, the team:

A. Surveyed public power utilities on the frameworks, standards, and assessment tools they use in their cybersecurity efforts.

B. Developed review and evaluation criteria for the cybersecurity frameworks and assessment tools based on the capabilities that public power utilities identified as important.

C. Engaged with APPA's Cybersecurity Defense Community Working Group to gain input throughout the process.

D. Assessed the burden and complexity of cybersecurity standards (such as NIST CSF, CIS Controls, C2M2) and assessment tools (such as CSET, CIS NCSR, C2M2 Self-Evaluation Tool, and APPA's proprietary tools).

E. Determined the most effective and practical assessment tools for this program with particular consideration for small and limited resource utilities, ensuring that the tools balance the time and effort required to complete them with the quality of data delivered.

This report summarizes the analysis of the most popular cybersecurity frameworks and security controls and evaluates the most popular tools based on survey data, feedback from the working group, and independent research and analysis by cybersecurity experts.

This analysis found that APPA's Cybersecurity Accelerator Program (CAP) provides the best balance of detail, flexibility, ease of use, and ability to support meaningful, repeatable assessments that map back to a range of frameworks. As a result, the CAP question set is the most suitable to measure the cybersecurity maturity of public power utilities, including resource-limited utilities.

Additionally, this report concludes with several recommendations for further action, including developing an instruction guide for the CAP question set and building more objective measurements for assessments, including examples and evidence to back scoring.

2. SURVEY METHODS

Between January 2025 and August 2025, APPA conducted a survey of its members to better understand their cybersecurity assessment needs. The survey was distributed broadly to include members from utilities, joint action agencies, and state and regional associations.

The Public Power Cybersecurity Frameworks, Standards, and Tools Survey consisted of eight questions, including demographics. The survey goal was to gain an understanding of which frameworks and tools public power utilities currently use, what elements are most important to public power utilities in their selection of and satisfaction with a cybersecurity tool, and how well the tools satisfy their needs or expectations. (For a complete list of survey questions, see Appendix A.)

The survey was conducted in two rounds. In the first round, APPA attempted to direct the survey to member representatives best qualified to understand and respond to the questions for their organizations. Individuals targeted in the first round had fit at least one of the following characteristics:

- Membership in the Cybersecurity Defense Community, security, or information technology (IT) groups on APPA Engage (APPA's online member community)
- Job function or role related to cybersecurity or IT
- Job title containing variations of "cybersecurity" or "information technology"
- Attended APPA events or event sessions relating to cybersecurity in the past five years
- Purchased a cybersecurity product from APPA in the past five years

For organizations who didn't have anyone that matched the above criteria, the primary contact for APPA at the organization received the survey. In the second round, the survey was sent to members participating in APPA's OT Insight and ICS CyberShield cooperative agreements.

The survey received 87 responses, representing organizations ranging from those serving fewer than 2,000 meters to more than 500,000 meters. APPA received 19 responses from utilities with fewer than 4,000 meters, which was identified in the cooperative agreement's Statement of Project Objectives as the threshold for resource-limited utilities. APPA did not include responses from generation/transmission utilities and joint action agencies in the response set for resource-limited utilities, as the workforce size and cybersecurity maturity of these organizations is often significantly higher than their meter count would suggest. (For a breakdown of survey participants by meters served, see Appendix B.)

3. CYBERSECURITY FRAMEWORK AND CONTROL SET REVIEW AND EVALUATION

A cybersecurity framework outlines a set of guidelines and best practices that can support organizations looking to improve their information security and reduce their cybersecurity risk. Control sets detail specific action steps or tasks organizations can implement. The use of cybersecurity frameworks and control sets is critical for public power utilities to manage cyber risks, protect assets, and meet compliance requirements. It allows for a structured, comprehensive approach to identifying expected cybersecurity program elements and industry-recognized best practices.

Based on the survey responses, the five most commonly used frameworks/control sets were: the NIST Cybersecurity Framework (CSF), CIS Critical Security Controls (CIS Controls or CSC), NERC Critical Infrastructure Protection (CIP), NIST SP 800-53, and DOE's Cybersecurity Capability Maturity Model (C2M2).

The results were similar when the dataset was limited to utilities that serve fewer than 4,000 meters, with only the MITRE ATT&CK framework replacing the DOE C2M2 as the fifth item on the list. The NIST CSF, CIS CSC, and NERC CIP had equal responses for the most used cybersecurity framework among small utilities. However, unlike the combined list, "None" accounted for a plurality of the participants in this utility size range, demonstrating the resource challenges facing small utilities.

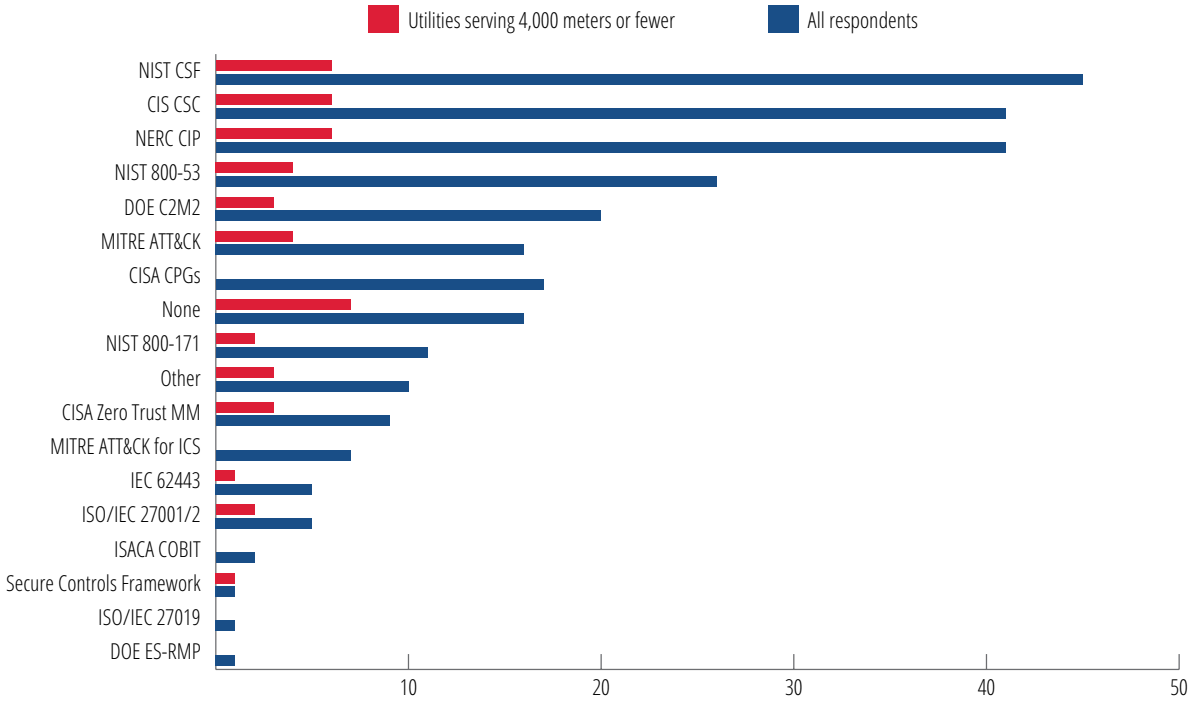


Figure 1. Cybersecurity Frameworks/Control Sets by Popularity. Five cybersecurity frameworks/control sets emerged as the most popular among survey respondents, with three emerging as the most popular among utilities that serve fewer than 4,000 meters.

3.1 Analysis of Cybersecurity Frameworks and Control Sets

Each of the most popular frameworks and control sets (according to the survey results) were reviewed and evaluated in terms of complexity, burden, and effectiveness for smaller utilities.

3.1.1 NIST Cybersecurity Framework

Published by the National Institute of Standards and Technology (NIST), the Cybersecurity Framework (CSF) is intended to provide guidance on risk management and cybersecurity best practices across public and private sectors to organizations of any size and at any level of cybersecurity maturity. Version 2.0 of the CSF focuses on six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. It articulates a set of high-level cybersecurity outcomes that organizations can use to better understand, assess, prioritize, and communicate their cybersecurity effort; however, it is not prescriptive in how organizations should accomplish these outcomes. The CSF is one of the most widely adopted frameworks throughout many industries.

Strengths

- Designed specifically for cybersecurity maturity measurement and improvement.
- Comprehensive and flexible, making it suitable for organizations of all sizes.
- Provides clear guidance on risk management.
- Appropriate for assessing both IT and operational technology (OT) controls.
- Supports risk modeling and assessments.

Challenges

- Lack of prescriptive guidance for organizations that may need assistance to address shortcomings identified by the framework.
- Implementation can be resource intensive, especially for smaller utilities with limited technical staff.
- The complexity of the framework can pose challenges for organizations without dedicated cybersecurity expertise.

Analysis: While NIST CSF is ideal for larger, more mature utilities, smaller utilities may find it burdensome without dedicated resources. It may be more effective when used as a complement to lighter alternatives such as CIS Controls for initial assessments.

3.1.2 CIS Critical Security Controls

The Center for Internet Security's Critical Security Controls (CIS Controls or CSC) is a set of 18 prioritized cybersecurity controls designed to provide actionable, high-priority security practices. Version 8.1 includes a total of 153 specific safeguards organized into Implementation Groups that begin with "essential cyber hygiene" and build on each other, allowing smaller organizations to identify the set of safeguards relevant to their needs and maturity. In contrast to NIST CSF, the CIS Controls are meant to be prescriptive, offering a structured path toward improving an organization's cybersecurity. CIS Controls are valued for their practical and prioritized approach to implementing foundational cybersecurity practices and for their focus on the most critical controls needed to protect IT systems and data.

Strengths

- Highly practical, providing clear, prioritized actions that can be implemented incrementally.
- Adaptable for varying amounts of available resources, particularly suitable for smaller utilities with limited cybersecurity resources.
- Regularly updated to reflect evolving cybersecurity threats.

Challenges

- While less intensive to implement, some utilities may still find it difficult to address all 18 controls, especially without a dedicated cybersecurity team.
- IT-centric model that does not support OT control assessment.
- Risk modeling and assessment support is not directly provided.

Analysis: CIS Controls is an excellent choice for smaller utilities as it offers a simpler, actionable approach to improving cybersecurity posture without overwhelming staff or resources. It's a good starting point for many utilities before advancing to more comprehensive frameworks like NIST CSF.

3.1.3 NERC Critical Infrastructure Protection

The North American Electric Reliability Corporation (NERC) established a set of mandatory standards for electric entities operating within North America that own, operate, or control any part of the bulk electric system (BES). These standards focus on protecting critical infrastructure from cyber threats and are highly detailed. NERC Critical Infrastructure Protection (CIP) is primarily used by electric utilities that are obligated to comply with regulatory requirements for protecting critical infrastructure.

Strengths

- Provides a clear, regulatory framework for utilities in the energy sector.
- Focuses heavily on critical infrastructure protection and developed specifically for the electricity sector, making it vital for utilities with significant OT environments.

Challenges

- Highly complex and often requires substantial resources for full compliance, making it especially burdensome for smaller utilities and utilities with limited staff.
- OT-centric model that does not support IT control assessment.
- Risk modeling and assessment support is not directly provided.

Analysis: NERC CIP is mandatory for entities that own, operate, or otherwise manage BES assets, including transmission owners and operators, balancing authorities, and generation owners. Most small utilities are not required to comply with NERC CIP, making it an unlikely choice for public power utilities. For those that are required to comply with NERC CIP, implementing can be challenging due to how resource-intensive it is, and smaller utilities may need to adopt a phased approach to compliance if required.

3.1.4 NIST SP 800-53

NIST SP 800-53 is an extensive set of security and privacy controls oriented towards helping organizations protect their operations and assets from a variety of threats and risks — including

cyberattacks, human errors, natural disasters, and structural failures. NIST SP 800-53 provides safeguards across multiple domains, from physical security to incident response. The controls are meant to be flexible to fit the needs of the organization implementing them and can be customized as needed. NIST SP 800-53 is not widely adopted in its entirety. It is primarily used by federal agencies or contractors and may be used in more complex or larger utilities for detailed security controls and risk management.

Strengths

- Highly detailed and thorough in its coverage of all aspects of cybersecurity.
- Comprehensive controls can be applied across various environments, including OT and IT systems.
- Supports risk modeling and risk assessment.

Challenges

- Has more than 1,000 controls and a deep structure consisting of control families, base requirements, and control enhancements, making it complex and impractical for small utilities with limited cybersecurity expertise.
- Requires ongoing maintenance and documentation, which can strain resources.
- IT-centric model that does not support OT control assessment.

Analysis: Due to its detailed security controls, while NIST SP 800-53 is an excellent framework for large utilities or those in highly regulated sectors, its complexity and breadth make it less suitable for small utilities.

3.1.5 DOE Cybersecurity Capability Maturity Model (C2M2)

Initially released by DOE in 2012 and focused on the electricity sector, C2M2 has since developed and expanded over the years into a model that organizations in any industry can use to assess and improve their cybersecurity maturity. It focuses on strategic cybersecurity governance and provides a structured framework for building and evaluating cybersecurity capabilities over time. Organizations of any size can use C2M2, which has the benefit of covering both IT and OT assets. The C2M2 guidance is provided at a high level of abstraction, increasing its applicability for organizations in a variety of situations, and avoids being prescriptive in nature. C2M2 is popular for assessing the maturity of cybersecurity practices, especially in utilities with more established cybersecurity programs.

Strengths

- Ideal for organizations looking to measure maturity and improve over time.
- Provides actionable insights and recommendations based on maturity levels.
- Supports both IT and OT controls assessments.
- Supports risk modeling and risk assessment.

Challenges

- Can be resource intensive, especially for smaller utilities, as it requires periodic reassessments and ongoing improvements.
- May be less applicable to utilities that are just beginning their cybersecurity journey and need more foundational support.

Analysis: C2M2 is highly beneficial for utilities with established cybersecurity programs ready to assess and improve their maturity. However, smaller utilities may find the model too complex unless they already have a basic cybersecurity framework in place.

3.1.6 MITRE ATT&CK

The MITRE ATT&CK framework, released in 2013 by the MITRE Corporation, is a knowledge base that documents adversary tactics, techniques, and procedures derived from real-world cybersecurity incidents. Initially developed to support adversary emulation and red team exercises, ATT&CK has evolved into a foundational resource for entities seeking to analyze attacker behavior, enhance threat detection, and strengthen security postures with matrices addressing enterprise, mobile, and industrial control system (ICS) environments. ATT&CK's adaptability and real-world basis make it a useful component in both public and private sector cybersecurity strategies, particularly in critical infrastructure protection with its ICS-specific matrix.

Strengths

- Comprehensive threat modeling.
- ICS matrix for organizations with extensive ICS assets.

Challenges

- Complexity and depth with hundreds of techniques and sub-techniques to understand.
- Limited prescriptive guidance compared to frameworks such as NIST CSF or DOE C2M2 as it does not prescribe specific controls or maturity goals.

Analysis: MITRE ATT&CK framework is beneficial for utilities to understand adversary behavior to improve their cybersecurity maturity, especially for ICS implementations. However, its complexity, lack of prescriptive guidance, and resource demands pose challenges for utilities with limited cybersecurity staff.

3.2 Cybersecurity Framework and Control Set Evaluation Results

The evaluation of the cybersecurity frameworks demonstrates wide variation in the level of complexity, resource requirements, and applicability for small utilities. For various reasons, NERC CIP and NIST SP 800-53 may be too burdensome for smaller utilities. C2M2 provides a robust maturity model but is better suited for utilities with established cybersecurity programs. Based on the analysis detailed above, CIS CSC and NIST CSF offer the best balance of effort and effectiveness for improving cybersecurity posture and are likely to be the most viable frameworks for public power utilities. CIS CSC should be noted for being particularly practical and actionable.

Notably, a plurality of small utilities reported not using a cybersecurity framework internally, highlighting the lack of resources and experience these utilities face. This also indicates that small utilities might benefit from support from more mature organizations, as well as resources to familiarize them with the concept and use of cybersecurity frameworks.

4. CYBERSECURITY ASSESSMENT TOOL EVALUATION

A variety of tools are available for assessing the implementation of a selected cybersecurity framework. Commonly available tools include the C2M2 Self-Evaluation Tool, CISA Cyber Security Evaluation Tool (CSET), CIS Nationwide Cybersecurity Review (NCSR), MITRE ATT&CK Navigator, Axio360, CyberSaint, RiskWatch, ISMS.online, and Stern Security Velocity. Additionally, APPA members have access to APPA's Cybersecurity Scorecard. Each of these has inherent advantages and disadvantages. To determine which tool would be most effective and practical for public power utilities, particularly smaller utilities, APPA and the working group created an objective system for assessing the value of each in a way that would be meaningful to help utilities winnow the options.

4.1 Selection of Cybersecurity Assessment Tools to Evaluate

Per the survey, the most common tools APPA members use are CIS NCSR (39%) and the C2M2 Self-Evaluation Tool (33%). CISA CSET was a close third, with 24% of survey respondents indicating using the tool. APPA's Cybersecurity Scorecard was used by 20% of respondents, and 41% of respondents reported using other commercial tools. Fifty-one of 87 respondents indicated they perform self-assessments.

Among utilities with fewer than 4,000 meters, only seven out of 18 reported using a cybersecurity assessment tool (and some reported using multiple tools). Of these respondents, three indicated they used the DOE C2M2 Self-Evaluation Tool (43%), three used other commercial tools (43%), two used the CIS NCSR (29%), and one used the APPA Cybersecurity Scorecard (14%).

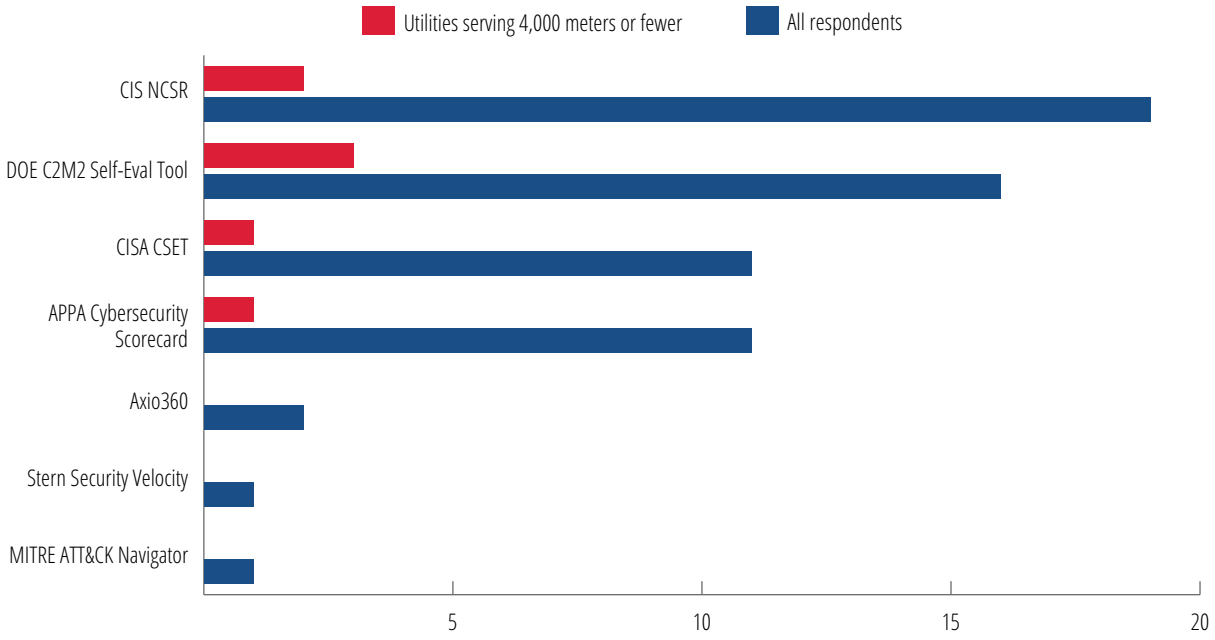


Figure 2. Most Common Cybersecurity Assessment Tools Used by Public Power (according to survey).

The top four tools most commonly used by the utilities surveyed were selected for evaluation (CIS NCSR, C2M2, CISA CSET, Cybersecurity Scorecard). Notably, the top four most-used tools are or were all available at no cost to public power utilities, indicating a preference for free tools in cybersecurity assessments.

4.2 Prioritization of Tool Evaluation Criteria

Prioritized criteria for assessing the value of the tools were also determined based on the survey results, ensuring that each tool was assessed based on qualities that would be most important to a public power utility.

Survey participants were asked to rate the importance of 12 different elements in the selection and satisfaction of a cybersecurity program self-assessment tool on a 1-5 Likert scale, where 1 was not at all important and 5 was extremely important. (For a complete list, see Appendix C.) Responses indicated that usability capabilities ranked highest in importance, with actionable data, clarity of questions, improvement measurements, and framework alignment taking the next four top places (in that order).

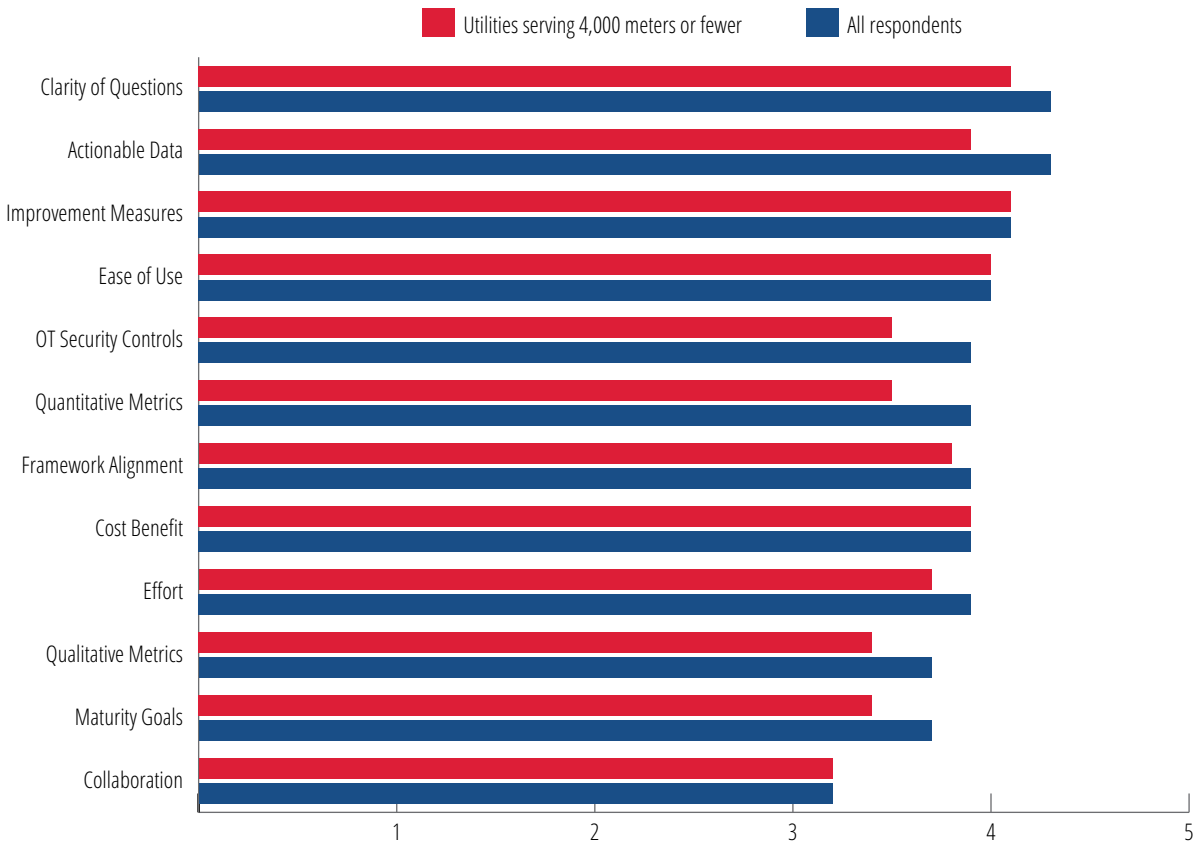


Figure 3. Cybersecurity Maturity Assessment Tool Criteria. Based on survey responses, usability capabilities ranked highest on importance. Scores indicated above were calculated by averaging survey responses on a 1–5 Likert scale.

These top five criteria, as selected by APPA members, were used to build a rubric against which the cybersecurity tools could be evaluated.

Comparing utilities with fewer than 4,000 meters against the wider pool of respondents, it is notable that smaller utilities placed a higher relative priority on ease of use and cost-benefit and a much lower priority on OT security controls and quantitative metrics. This indicates small utilities prioritize tools that work best for their limited resources while deprioritizing features that may not be applicable, such as OT security controls.

4.3 Evaluation of Cybersecurity Assessment Tools

The most used cybersecurity assessment tools identified by survey respondents (CIS NCSR, C2M2 Self-Evaluation, CISA CSET, APPA Cybersecurity Scorecard) were evaluated against the criteria identified as priorities (clarity of questions, actionable data, improvement measurements, ease of use, and framework alignment). This process ensured that the results are relevant to public power and practical for smaller utilities.

4.3.1 Clarity of Questions

The clarity of questions refers to how easily a tool's questions are understood and answered, especially by users with varying technical expertise. Clear and concise questions help users focus on key issues, reducing confusion and errors. For smaller utilities with limited technical staff, tools that use simple language and provide definitions are essential for accurate assessments. Well-structured questions lead to more reliable results, while poorly worded questions can cause frustration and delay.

The assessment tools were rated on clarity of questions based on three elements: easy-to-understand questions, links to source requirements, and expanded guidance on the requirements. The rating was assessed using a 5-point scale with:

- 2 points for covering one of these elements
- 4 points for covering two of these elements
- 5 points for covering all three elements

Only CSET had all three elements and received five points while all other tools each earned two points.

4.3.2 Actionable Data

Actionable data is the tool's ability to provide clear, practical steps for improving cybersecurity based on its findings. Effective tools not only assess the current state but also offer specific recommendations for addressing vulnerabilities. This ensures that the assessment is more than just diagnostic and becomes a guide for tangible improvements. Without actionable insights, the assessment remains a snapshot rather than a tool for progress.

The assessment tools were rated for providing actionable data based on five elements: identification of gaps, descriptive and actionable recommendations, links to useful resources, impact and complexity of remediation, and cost estimates of remediation. This rating was assessed using a 5-point scale with one point given for each of the elements.

Only CSET had all five elements; while CIS NCSR and the C2M2 Self-Evaluation Tool each only received one point for identifying the gaps.

4.3.3 Improvement Measurements

Improvement measurements track progress enhancing cybersecurity over time. Tools that support these measurements offer insights into how well an organization is addressing gaps and implementing best practices and when to change tactics because something is not working. These tools help utilities set baselines, track progress, and prioritize cybersecurity efforts, ensuring resources are allocated efficiently and effectively.

The assessment tools were rated for the quality of their improvement measurements based on three elements: maturity levels, score tracking, and peer comparison. Peer comparison (how well the organization completing the assessment rates against similar organizations) is particularly helpful to gain external perspective on the utility's relative cybersecurity maturity. The rating for improvement measurements was assessed using a 5-point scale, with:

- 2 points for including one of the elements
- 4 points for including two of the elements
- 5 points given for all three elements

CSET and CIS NCSR each received five points in this category.

4.3.4 Ease-of-Use

Ease-of-use refers to how intuitive and simple the tool is to navigate and complete. Tools with a clear interface, organized questions, and simple instructions minimize the effort required, especially for nontechnical staff. A tool that is easy to use helps utilities quickly complete assessments and ensures consistent engagement, making it ideal for smaller utilities with limited resources.

The assessment tools were rated on ease-of-use based on four elements: having less than 200 questions, good tool navigation, the ability to add notes for each question, and the ability to attach evidence to each question. This rating was assessed using a 5-point scale, with:

- 1 point given for one of the elements
- 2 points given for two of the elements
- 4 points given for three of the elements
- 5 points given for all four elements

Only CSET had all four elements and received five points, while CIS NCSR and the C2M2 Self-Evaluation tool each received two points for having less than 200 questions and good navigation.

4.3.5 Framework Alignment

Framework alignment refers to how well a tool integrates with recognized cybersecurity frameworks. Strong alignment ensures that the assessment is based on proven industry standards, helping utilities assess their maturity and comply with regulations. It also supports the development of cybersecurity practices that align with industry benchmarks and best practices.

The assessment tools were rated on framework alignment based on their alignment with the five frameworks identified as most popular (see Section 3 of this report): NIST CSF, CIS CSC, NERC CIP, NIST SP 800-53, and C2M2. The tools were rated on a 5-point scale for each of the five frameworks with:

- 5 points if the framework's controls are built into the tool as native content (e.g., selectable as an assessment basis)
- 4 points if the tool does not contain the framework natively but includes an official crosswalk or mapping to it
- 3 points if the tool provides informal or partial mapping, often community-developed or approximate
- 2 points if the framework is not mapped in the tool, but some questions or categories generally align in scope or terminology
- 1 point if there is no mapping or integration of the framework within the tool

Each of the tools received a 5-point rating for at least one of the frameworks, with CSET receiving 5-point ratings for four out of the five frameworks, excluding C2M2.

4.4 Evaluation Scores

Tool	Clarity of Questions	Actionable Data	Framework Alignment					Framework Alignment Overall	Improvement Measures	Ease-of-Use	Overall Score
			NIST CSF	CIS CSC	NERC CIP	NIST 800-53	DoD C2M2				
CIS NCSR	2	1	4	4	2	4	2	3.2	5	2	2.64
C2M2 Self-Eval Tool	2	1	4	3	2	3	4	3.2	2	2	2.04
CISA CSET	5	5	5	5	5	5	3	4.6	5	5	4.92
APPA Cybersecurity Scorecard	2	N/A	3	3	2	3	4	3	N/A	N/A	N/A

Figure 4. Cybersecurity Assessment Tool Scores: The top four cybersecurity assessment tools were assessed against the top criteria. CSET had consistently high marks across all categories. Other tools had some significant low marks in clarity of questions, actionable data, framework alignment, improvement measures, and ease-of-use.

5. VALIDATING RESULTS

To ensure that this analysis and evaluation is based on representative underlying survey data and that the findings both reflect experiences and add practical value, APPA asked the Cybersecurity Defense Community Working Group to review and validate the results. The response to this report's findings and recommendations was positive.

While the working group members agreed no tool is perfect, they also agreed upon the value of conducting an accurate cybersecurity assessment. A common theme among the comments from the working group members was that these assessments are quite challenging to complete and that they have struggled with both self-assessments and with hiring third-party vendors to do thorough assessments. This highlights the need for this report analysis as well as for potential additional support.

Additionally, the working group members offered the following valuable advice to guide other utilities in planning and executing cybersecurity assessments:

- **Be honest:** The working group members repeatedly mentioned the need to be honest in conducting an assessment, warning that if a utility "sugarcoats" the data, there will be missed vulnerabilities.
- **Take your time:** To get good results from an assessment, utilities have to allow the necessary amount of time — rushing through will only lead to having to retake the assessment.
- **Keep it consistent:** Choose one tool and framework and stay with it over time to enable year-over-year comparisons and clear progress tracking.
- **Plan for reassessment:** Reassessments provide richer insights as understanding matures. Scores may fluctuate as teams become more self-critical, but this reflects true progress.
- **Use common controls:** For complex organizations, define baseline common controls (applicable organization-wide) and tailor additional questions for specific lines of business.
- **Start small:** For comprehensive models like C2M2, begin with the foundational maturity level (MIL1) as a target to manage effort and avoid burnout.
- **Hire wisely:** The working group members recounted various recommendations for finding adequate third-party assessors and suggested seeking out firms that use data to justify their metrics, provide an adequate amount of time to conduct a thorough assessment, are independent and able to provide objective assessments, and will not try to sell additional products (which may bias assessment results).

6. RECOMMENDATION

The purpose of this report was to determine the most effective assessments for public power, particularly small utilities with limited resources. Based on the research, CISA's CSET was identified as the most appropriate program to measure progress that is not too onerous for the small utilities to complete, as they will likely have to complete the assessment more than once.

However, the survey results from public power utilities that serve fewer than 4,000 meters indicated no clear winner in terms of a cybersecurity framework or assessment tool (with a roughly even split between NERC CIP, CIS Controls, and NIST CSF among frameworks and between DOE C2M2, CISA CSET, and CIS NCSR for assessment tools). The optimal framework and assessment platform for smaller utilities would need to map to multiple frameworks while maintaining ease of use and accessibility, including for utilities that have not adopted any cybersecurity frameworks or assessment tools, and help familiarize them with common cybersecurity standards.

In response, the APPA team evaluated the question set for its Cybersecurity Accelerator Program (CAP) and determined that it meets these suggested criteria. Specifically, the CAP question set:

- Includes 27 questions across four primary domains, with an additional 53 clarifying sub-questions for greater detail. This provides a balance between usability and detail, being shorter and less burdensome than the question sets for NIST CSF and DOE C2M2 and therefore easier for resource-limited utilities to complete, while still capturing enough information to measure program progress.
- Maps back to common frameworks, including NIST CSF, CIS Controls, DOE C2M2, and the National Association of Regulatory Utility Commissioners' Cybersecurity Baselines for Electric Distribution Systems, maintaining familiarity for users of these frameworks.
- Is relevant to utilities from a range of sizes – including small, resource-limited utilities – as verified by a working group of public power utilities of various sizes.
- Follows a familiar model for public power utilities as a designation program, similar to APPA's Reliable Public Power Provider (RP3) and Smart Energy Provider (SEP) designations.

In addition, APPA is developing an online platform for the CAP question set, which will focus on ease of use for public power utilities based on APPA's experience in other designation programs and past cybersecurity cooperative agreements.

Given the preference to reduce assessment burden and complexity together with its coverage of multiple cybersecurity frameworks, APPA's CAP question set and platform is recommended as the assessment tool for the Cyber Pathways program.

Appendix E includes the request for proposals requirements issued by APPA for the CAP application platform, which includes usability requirements to ensure the platform is usable by resource-limited utilities that may not have familiarity with existing assessment platforms or tools. It also includes security requirements for data protection.

6.1 Recommendations for Further Action

ACTION 1: **Adopt the CAP question set as the assessment tool for the Cyber Pathways program.** Based on a review of existing frameworks, this question set strikes the best balance between usability and detail.

ACTION 2: **Develop a guide for completing the CAP assessment.** Given that the most significant burden in completing an assessment is the data collection, public power utilities would likely benefit from a guide explaining how to gather and properly input data related to the question set, including where the information aligns with other frameworks and strategies with which they might be familiar. This would assist organizations in a more effective use of the tool and its outputs.

ACTION 3: **Ensure clarity on question requirements and evidence necessary to satisfy each response.** Organizations often overestimate their cybersecurity controls during self-assessments, leading to inaccurate results. To improve accuracy, public power utilities would benefit from clear scoring rubrics with examples, requiring objective evidence for each response and prompting for common overconfidence areas.

APPENDICES

APPENDIX A:

PUBLIC POWER CYBERSECURITY FRAMEWORKS, STANDARDS, AND TOOLS SURVEY

Thank you for participating in the American Public Power Association (APPA)'s Cybersecurity Frameworks, Standards, and Tools Survey!

This survey has been released as part of our Cyber Pathways program, a $4 million cooperative agreement with the U.S. Department of Energy to improve the public power community's cybersecurity maturity. In order to measure the program's impact and effectiveness, we are looking for a cybersecurity framework and assessment tool that participating utilities can use to assess outcomes from program activities. To minimize the time and effort required of participating utilities, we would like to select a framework and assessment tool already in widespread use by public power utilities and are thus asking for your feedback as to which assessments (if any) are in use at your utility.

If you have any interest in the other offerings of the Cyber Pathways program, you can read more from our Physical and Cybersecurity page.

Please direct questions to Christopher Ching at (202) 467-2907 or Cybersecurity@PublicPower.org.

1. What cybersecurity framework(s) or control sets, if any, does your organization use to evaluate its cybersecurity maturity? Please select all that apply.

Center for Internet Security (CIS)

☐ Critical Security Controls

Cybersecurity & Infrastructure Security Agency (CISA)

☐ Cross-Sector Cybersecurity Performance Goals (CPGs)

☐ CISA Zero Trust Maturity Model

U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2)

☐ DOE Energy Sector (ES) C2M2

☐ DOE ES-Cybersecurity Risk Management Process (RMP)

Information Systems Audit and Control Association (ISACA)

☐ Control Objectives for Information and Related Technologies (COBIT)

International Standards Organization / International Electrotechnical Commission (IEC)

☐ ISO/IEC 27001 and 27002

☐ ISO/IEC 27019 Information Security for Energy Utilities

☐ IEC 62443

National Institute of Standards & Technology (NIST)

☐ Cybersecurity Framework (CSF)

☐ NIST 800-53 Security and Privacy Controls for Information Systems and Organizations

☐ NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

North American Electric Reliability Corporation (NERC)

☐ Critical Infrastructure Protection (CIP) Standards

The MITRE Corporation

☐ MITRE ATT&CK Framework

☐ MITRE ATT&CK Framework for ICS

Other Organizations

☐ Secure Controls Framework

☐ Other (Please specify)

Our organization does not have a cybersecurity framework or control set

☐ Our organization does not have a cybersecurity framework or control set

2. Does your organization perform self-assessments?

☐ Yes

☐ No

3. If so, what tools or platforms does your organization use to conduct these assessments? Please select all that apply.

Government Tools

☐ DOE Energy Sector (ES) C2M2 Self-Evaluation Tool

☐ CISA Cyber Security Evaluation Tool (CSET)

☐ CIS Nationwide Cybersecurity Review (NCSR)

Organization and Association Tools

☐ APPA Cybersecurity Scorecard

☐ APPA Cybersecurity Guidance and Tool

☐ MITRE ATT&CK Navigator

Commercial Tools

☐ Axio360 Platform

☐ CyberSaint

☐ RiskWatch

☐ ISMS.online

☐ Stern Security Velocity

Other (Please specify) _____

4. How much time is expended annually to perform a cybersecurity self-assessment within your organization? Include preparation, tool use, and assessment results/report creation in your estimate. Provide total combined hours spent among staff.

- ☐ Greater than 0 but less than 10 hours
- ☐ 10–16 hours
- ☐ 17–24 hours
- ☐ Greater than 24 hours
- ☐ N/A: My organization does not spend time on cybersecurity self-assessments

5. Using a 1–5 scale where 1 is strongly disagree and 5 is strongly agree, indicate how well the assessment tool you use satisfies the following parameters:

	Strongly Disagree (1)	Somewhat Disagree (2)	Neutral (3)	Somewhat Agree (4)	Strongly Agree (5)
Framework Alignment: The assessment tool and the result from its use aligns with our cybersecurity standards and frameworks					
Actionable Data: We gain useful insights and actionable recommendations from the use of the tool					
Ease of Use: The tool is easy to use with an intuitive user interface and easy navigation					
Clarity of Questions: The assessment questions are clear and easy to understand					
Improvement Measurements: The tool provides accurate and useful measurements of our cybersecurity program maturity					
Collaboration: The tool supports multi-user collaboration					
Cost Benefit: The value of each assessment outweighs the cost of the tool					
Effort: The value of each assessment outweighs the assessment effort					

6. Using a 1–5 scale where 1 is not at all important and 5 is extremely important, how important are each of the following elements in the selection and satisfaction of a cybersecurity program self-assessment tool:

	Not At All Important (1)	Slightly Important (2)	Moderately Important (3)	Highly Important (4)	Extremely Important (5)
Framework Alignment: The assessment tool and the result from its use aligns with our cybersecurity standards and frameworks					
Actionable Data: We gain useful insights and actionable recommendations from the use of the tool					
Ease of Use: The tool is easy to use with an intuitive user interface and easy navigation					
Clarity of Questions: The assessment questions are clear and easy to understand					
Improvement Measurements: The tool provides accurate and useful measurements of our cybersecurity program maturity					
Collaboration: The tool supports multi-user collaboration					
Cost Benefit: The value of each assessment outweighs the cost of the tool					
Maturity Goals: The assessment has the ability to set maturity goals					
Qualitative Metrics: The assessment has qualitative risk metrics					
Quantitative Metrics: The assessment has quantitative risk metrics					
OT Security Controls: The assessment includes OT security controls					
Effort: The value of each assessment outweighs the assessment effort					

7. What is your utility's meter count?

☐ 0–2,000
☐ 2,001–4,000
☐ 4,001–10,000
☐ 10,001–25,000
☐ 25,001–50,000
☐ 50,001–100,000
☐ 100,001–500,000
☐ 500,001 or more

8. Would you like to be contacted regarding future training or participation opportunities under the Cyber Pathways Program? If yes, please provide the following contact information:

First Name: _____

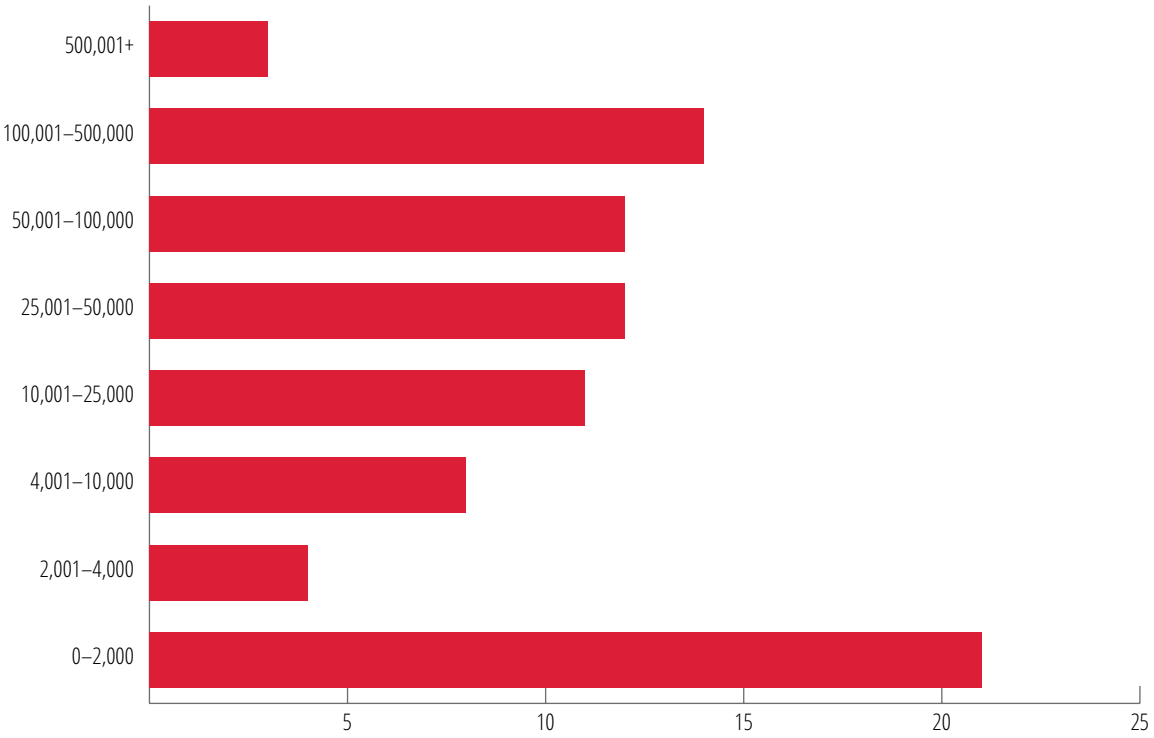
Last Name: _____

Utility: _____

State: _____

Email: _____

APPENDIX B:
SURVEY PARTICIPANTS BY METER COUNT



A total of 87 surveys were received. Two participants did not respond to this question.

APPENDIX C:
ASSESSMENT TOOL CRITERIA

Tool Criterion	Description	Importance
Clarity of Questions	How clearly are questions presented and understandable for users with varying technical expertise?	Tools with clear, straightforward questions are more accessible, especially for utilities with limited staff or technical expertise.
Actionable Data	Does the tool provide useful data that can be directly applied to improve cybersecurity practices?	Actionable data enables utilities to implement meaningful changes to their cybersecurity practices, making a tool more valuable and practical.
Framework Alignment	How well does the tool align with preferred cybersecurity frameworks?	Alignment with trusted frameworks ensures that utilities follow proven guidelines, enhancing the effectiveness of the tool.
Improvement Measurements	Does the tool track improvements and provide insights into cybersecurity maturity over time?	Improvement measurements provide ongoing insights and allow utilities to track progress and adjust strategies accordingly.
Ease of Use	How user-friendly is the tool? Can utilities use it with minimal training or technical knowledge?	Tools that are easy to use are more likely to be adopted and consistently used by utilities with limited resources or technical staff.
Cost-Benefit	Does the tool provide good value relative to its cost, particularly for utilities with limited budgets?	Since many utilities have limited budgets, the cost-benefit is a critical factor in choosing tools that provide the most value without overburdening financial resources.
Effort Required	How much time, resources, and personnel are needed to implement and use the tool effectively?	Small utilities with limited staff need tools that require minimal effort and are easy to implement.
OT Security Controls	Does the tool address the security of OT systems like SCADA and ICS?	OT security is crucial for utilities in the energy and public infrastructure sectors, as a significant portion of their operations relies on these systems.
Quantitative Metrics	Does the tool provide measurable data (e.g., risk scores, maturity levels) that can be tracked over time?	Quantitative metrics allow utilities to objectively measure their cybersecurity posture and track improvements in a data-driven manner.

Cybersecurity Maturity Assessment Tool Criteria. The rubric the team used to assess selected cybersecurity maturity tools. Criteria are based on experience and discussions about what is most important for public power utilities.

Tool Criterion	Description	Importance
Qualitative Metrics	Does the tool provide narrative insights or recommendations to guide decision-making?	Qualitative metrics are essential for understanding the context behind the data, helping utilities take targeted actions based on expert insights.
Maturity Goals	Does the tool assess cybersecurity maturity and offer improvement goals or roadmaps?	Tools that incorporate maturity models help utilities set clear goals and track long-term improvements, enhancing their ability to measure progress.
Collaboration (Multi-User)	Does the tool allow multiple users to collaborate on assessments and track progress?	Collaboration is important for larger teams and utilities that need cross-departmental engagement in cybersecurity assessments.

Cybersecurity Maturity Assessment Tool Criteria. The rubric the team used to assess selected cybersecurity maturity tools. Criteria are based on experience and discussions about what is most important for public power utilities.

APPENDIX D:
CYBERSECURITY ACCELERATOR PROGRAM QUESTION SET

	Question	NIST CSF	CIS	C2M2	NARUC Base
Internal Controls					
1.	**Does your utility inventory the organization's IT assets?**	ID.AM-01; ID-AM-02	1.1	ASSET-1a:g	1.A
1.a.	If yes, does your utility also inventory the organization's OT assets?				
1.b.	If yes, how frequently do you inventory assets?				
	■ Periodically				
	■ Only log known changes				
1.c.	If yes, do you identify your organization's critical or 'crown jewel' assets?	ID.AM-05		ASSET-1c	
2.	**Does your utility inventory important data, including customer information, financial data, and internal system settings?**	ID.AM-07	3.2	ASSET-2a	2.O
3.	**Does your utility establish configuration baseline(s) for assets?**	PR.PS-01; PR.IP-01	4.1	ASSET-3a	
3.a.	If yes, do you apply the configuration baseline(s) to all assets at deployment?			ASSET-3b	
4.	**Does your utility back up data for critical systems?**	PR.DS-11	11.1	RESPONSE-4b	2.R
4.a.	If yes, does your utility also backup configurations for critical systems?				
4.b.	If yes, how frequently do you perform backups?		11.2		
	■ More than once a day				
	■ Daily				
	■ Periodically, but less than daily				
	■ Ad hoc				

	Question	NIST CSF	CIS	C2M2	NARUC Base
4.c.	If yes, do you store at least one complete backup in an alternate location?		11.4	RESPONSE-4k	
4.d.	If yes, do you maintain multiple copies of backups?		11.4		
4.e.	If yes, do you store data in multiple forms of media?		11.4		
4.f.	If yes, do you encrypt backups?		11.3	RESPONSE-4j	
4.g.	If yes, how long do you retain backups?		3.4		
	■ <30 days				
	■ 1-3 months				
	■ 4+ months				
5.	**Does your utility have an identity and access management (IAM) program?**				
5.a.	Does your utility create individual user accounts for people and application services that require access to:	PR.AA-01	5.1	ACCESS-1b	2.C
	■ Your IT systems?				
	■ Your OT systems?				
5.b.	Does your entity use multi-factor authentication for digital access?	PR.AA-03	6.3 - 6.5	ACCESS-1i	2.H
5.b.i.	If yes, what proportion of your IT systems use multi-factor authentication?				
	■ Some IT systems?				
	■ Most IT systems?				
	■ All IT systems?				
5.b.ii	If yes, what proportion of your applicable OT systems use multi-factor authentication?				
	■ Some OT systems?				
	■ Most OT systems?				
	■ All OT systems?				
5.b.iii	Does your utility require multi-factor authentication for privileged accounts?		6.5	ACCESS-1h	
6.	**Does your utility have physical access controls to limit who is able to physically access critical or sensitive assets?**	PR.AA-06		ACCESS-3a; 3d	

	Question	NIST CSF	CIS	C2M2	NARUC Base
7.	**Does your utility use a software or service to block potentially malicious interactions? Check all that apply:**		9.3 - 9.7	ARCHITECTURE-2g	2.M
	■ An e-mail filtering solution that blocks potentially malicious attachments				
	■ An e-mail filtering solution that has the ability to run suspicious attachments in a sandbox				
	■ An e-mail filtering solution that blocks suspicious messages based on their content or sender attributes				
	■ A web filtering solution which stops employees from visiting suspicious and known malicious websites				
	■ A web filtering solution that blocks suspicious or known malicious downloads				
8.	**Does your utility logically segment IT and OT systems?**	PR.IR-01	12.2	ARCHITECTURE-2b; 2h; 2i; 2j	2.F
8.a.	Does your utility segment systems within your IT environment?				
8.b.	Does your utility segment systems within your OT environment?				
9.	**Does your utility log IT network activity?**	PR.PS-04; DE.CM-01	8.1 - 8.2	SITUATION-1a	2.T
9.a.	If yes, do you also log OT network activity where possible?		8.11	SITUATION-2a	
9.b.	If yes, do you (or a third party on your behalf) review logs periodically?		8.11	SITUATION-2a	
9.c.	If yes, how long do you maintain logs for key systems?		8.10		
	■ Less than one month				
	■ Between one month and a year				
	■ More than one year				
10.	**Does your utility have anyone (internal or external) monitoring the organization's security operations?**	DE.CM-01		SITUATION-2a	
10.a.	If yes, does your utility have 24/7 monitoring (internal or external)?				
10.b.	If yes, do you have any automated systems (e.g., SIEM) in place to detect irregular or anomalous activity that may be indicators of a cyber incident?		13.1	SITUATION-2e; 2f	
10.b.i.	If yes, is your utility collecting data from (select all that apply):			SITUATION-2b	

	Question	NIST CSF	CIS	C2M2	NARUC Base
	■ Endpoints		13.2		
	■ Network traffic		13.3		
10.c.	If yes, are the people monitoring operations able to take action to resolve potential incidents in real time?				
11.	**Do you test or audit the effectiveness of your cybersecurity controls?**		18.1	PROGRAM-2h	1.F
11.a.	If yes, who performs the cybersecurity audits?				
	■ Internal				
	■ Third party				
	■ Both internal and third party				
11.b.	If yes, how frequently do you audit control effectiveness?				
	■ Annually				
	■ Quarterly				
	■ Monthly				
Cybersecurity Governance and Training					
12.	**Does your utility have a cybersecurity program?**	GV.PO-01		PROGRAM-1a	
12.a.	If yes, does your cybersecurity program team have sufficient resources (personnel, funding, and tools) to achieve the strategy's goals?				
13.	**Does your utility's cybersecurity program have senior management sponsorship?**	GV.RR-01		PROGRAM-2a; 2c; 2d	
14.	**Does your utility have formally assigned roles and responsibilities for cybersecurity?**	GV.RR-02		WORKFORCE-3a:d	
14.a.	Does your utility perform background checks or other methods of personnel vetting for employees and contractors with cybersecurity responsibilities?			WORKFORCE-1c	
15.	**Does your utility have password policies for IT systems?**		5.2	ACCESS-1d	
15.a.	If yes, do these policies include (select all that apply):				
	■ Minimum requirements for user-generated passwords				2.B
	■ A requirement to change default passwords in systems and applications				2.A
	■ Use of unique passwords				2.C

	Question	NIST CSF	CIS	C2M2	NARUC Base
15.b.	If yes, does your utility also have password policies for OT systems?				
15.c.	If yes, do you provide a password manager for employees?				
16.	**Do you have a cyber access control management policy for IT systems?**	PR.AA-05	6.1	ACCESS-2a	
16.a.	If yes, do you also have a cyber access control management policy for OT systems?				
16.b.	If yes, does your utility have a policy for revoking access when no longer needed?		6.8	ACCESS-2b; 1f	2.D
16.c.	If yes, how frequently do you review access permissions to ensure policy compliance?		6.8	ACCESS-2h	
	■ Less than annually				
	■ Annually				
	■ Quarterly				
	■ Monthly				
17.	**Does your utility share cybersecurity information with relevant organizations (e.g., E-ISAC, APPA)?**			THREAT-1i	
18.	**Does your utility provide role-based cybersecurity training to employees with cybersecurity responsibilities?**	PR.AT-02	14.9	WORKFORCE-4a; 4f	2.J
18.a.	Does your utility also provide role-based cybersecurity training to contractors?				
19.	**Does your utility provide cybersecurity awareness training to all employees?**	PR.AT-01	14.1-14.8	WORKFORCE-4d	2.I
19.a.	If yes, how often do you conduct training?				
	■ At least quarterly				
	■ Annually				
	■ Less than annually				
19.b.	If yes, how frequently do you incorporate any testing (e.g., simulated phishing attacks)?			WORKFORCE-4e	
	■ Monthly				
	■ Quarterly				
	■ Annually				
	■ Less than annually				

	Question	NIST CSF	CIS	C2M2	NARUC Base
19.c.	If yes, does your utility also provide cybersecurity awareness training to all contractors (or verify that contractors otherwise receive awareness training)?				
Cyber Incident Response and Management					
20.	**Does your utility have a cyber incident response plan?**	RS.MA-01	17.4	RESPONSE-3d	2.S
20.a.	Does your utility have criteria in place to assess whether cybersecurity events constitute an incident?	DE.AE-08	17.9	RESPONSE-2d	
20.a.i.	If yes, does your utility have established criteria for when it must report a cyber incident to relevant regulatory or other bodies?	RS.CO-03		SITUATION-3d; RESPONSE-2g; RESPONSE-3c	4.A
20.b.	If yes, does that plan include roles and responsibilities for specific personnel in cyber incident response?		17.5	RESPONSE-3a	
20.c.	If yes, does that plan include processes for tracking and logging progress?			RESPONSE-2f	
20.d.	If yes, does that plan identify third parties that your utility might call on to support response efforts?			RESPONSE-3j	
20.e.	If yes, does that plan include emergency contact information for internal and/or external points of contact?		17.2		
20.f.	If yes, does that plan include a playbook or guideline of recommended actions for certain scenarios?		17.3		
20.g.	If yes, does that plan have processes and procedures specific to responding to incidents in your OT system(s)?				
20.h.	If yes, how frequently does your utility exercise that response plan?		17.7	RESPONSE-3g	
	■ Annually				
	■ Every two years				
	■ Less than every two years				
21.	**Is cybersecurity and cyber incident response part of your utility's continuity of operations (COOP), business continuity, or disaster recovery planning?**			RESPONSE-4a; 4d	5.A

	Question	NIST CSF	CIS	C2M2	NARUC Base
Cyber Risk Management					
22.	**Does your utility gather information on threats (e.g., threat actors and common tactics, techniques, and procedures) and review it for applicability to your organization?**	ID.RA-02; ID.RA-03		THREAT-2b	3.A
22.a.	If yes, how does your utility approach managing threats (including strengthening security protections, increasing monitoring activities, and/or raising awareness throughout the organization)?			THREAT-2d	
	■ Policy				
	■ Ad hoc				
23.	**Does your utility gather information on vulnerabilities and review it for applicability to your assets and systems?**	ID.RA-01	7.1	THREAT-1a:b	1.E
23.a.	If yes, does your utility proactively scan for potential vulnerabilities?		7.5; 7.6	THREAT-1c; 1f	
23.a.i.	If yes, how frequently does your utility conduct vulnerability scans?		7.5; 7.6		
	■ At least weekly				
	■ Monthly				
	■ Quarterly				
	■ Less than quarterly				
23.b.	If yes, how does your utility approach managing applicable vulnerabilities (e.g., patching or other changes)?		7.2; 7.7	THREAT-1d	
	■ Policy				
	■ Ad hoc				
24.	**Does your utility identify and assess cybersecurity risks to your organization?**	ID.RA-05		RISK-2a; 3a	
24.a.	If yes, does the risk assessment process include the identification of critical assets and systems?				
24.a.i.	If yes, does your utility prioritize resources and risk management activities for those assets and systems?	ID.RA-06		RISK-4b	
24.b.	If yes, does your utility manage those risks with some combination of acceptance, transference, avoidance, or mitigating activities?	ID.RA-06		RISK-4a	

	Question	NIST CSF	CIS	C2M2	NARUC Base
25.	**Does your utility vet third-party suppliers for potential cybersecurity risks?**	ID.RA-10; GV.SC-06	15.5	THIRD-PARTIES-2d	1.I
25.a.	If yes, does your utility have established cybersecurity requirements for third-party service providers?	GV.SC-05		THIRD-PARTIES-2a	
25.b.	If yes, does your utility have established cybersecurity requirements for third-party products (e.g., hardware, software, firmware) providers?	GV.SC-05		THIRD-PARTIES-2b	
25.c.	If yes, do you conduct any risk assessments before procuring IT or OT systems or services?				
26.	**Does your utility assess potential cybersecurity risks from the compromise of a third-party provider?**	GV.SC-07	15.3; 15.6	RISK-2k	
27.	**Does your utility have a cyber-specific insider threat program?**				
27.a.	If yes, do you monitor for indicators of potential malicious activity (e.g., unauthorized remote access, repeated failed access attempts, communication with known malicious websites or IP addresses)?	DE.CM-03		SITUATION-2d; ACCESS-2i	2.G

APPENDIX E:
CAP PLATFORM REQUEST FOR PROPOSALS REQUIREMENTS

- **'Off-the-Shelf' Application Platform.** APPA aims to procure a pre-configured, off-the-shelf SaaS solution to provide a more suitable application platform that meets both current and future application needs while minimizing complexity and development time.
- **Automate and Standardize the Scoring Process.** APPA seeks to automate and standardize most of the scoring process with the new solution. In addition, incorporating features like direct file viewing should significantly reduce manual tasks for graders where manual review is necessary.
- **Improve Process Efficiency.** Reduce the needs for manual recordkeeping, system data exports and imports, travel for signatures, redundancies, and enable better analytics of customer factors around program success and failure.
- **Enhance Security Measures..** Given the importance of security, the solution must incorporate robust security protocols and should leverage existing industry standards (e.g., NIST 800-171, SOC 2). With a recent migration to Azure, APPA aims to enhance its existing measures and ensure the platform is equipped to protect sensitive data effectively.
- **Ensure Scalability and Flexibility.** The solution should be scalable to accommodate future growth and changing organizational needs, potentially including the addition of other application-based programs to the platform. Recognizing that each application may have unique requirements, the new solution should also offer flexibility in security options and data handling.
- **Support Platform Integration.** The solution should support integration with other platforms such as Salesforce and Snowflake, enabling the import of existing data and historical records while preserving future client interactions, including questions and responses.
- **Facilitate Automated Reporting.** The platform should include automated reporting capabilities, allowing APPA to generate reports without manual intervention, supporting data analysis and informed decision-making.

Security Considerations

Given the importance of protecting sensitive data and safeguarding CAP information from evolving threats, APPA is seeking a vendor and solution that follows an industry-accepted security framework or control set (e.g., NIST 800-171 or Cybersecurity Framework, Cybersecurity Maturity Model Certification Level 2, CIS Controls, ISO 27001, FedRAMP High) and can demonstrate third-party validation of effective control implementation for that framework or control set.

General Description

APPA Cybersecurity Accelerator Program Assessment Platform – DE-CR0000026

Under the project plan for APPA's Cyber Pathways cooperative agreement with DOE, APPA will develop a cybersecurity maturity assessment platform for APPA members that choose to participate.

Proposed Contractor Scope of Work:

1. Provide a full-service SaaS platform that hosts the APPA CAP assessment questionnaire, allows participating members to fill out and submit applications, conducts automated scoring for questions that do not require interpretation, and allows for basic reporting.
2. Provide continued support to APPA for back-end operation of the platform.

Deliverable 1: Application Platform

Overall APPA Objective: Provide an assessment application platform that member utilities can use to apply for the CAP designation program, with the potential to support additional APPA designation programs in the future.

APPA Technical Approach: Table 1 contains APPA's platform requirements for deployment. The questionnaire for the CAP application is likely to include approximately 75 individual questions (including sub-questions) in varying formats.

Table 1: Functional and Security Requirements

Functional Requirements	
1.	**Automated Application Access**
1.1.	The platform allows applicants to request access directly and agree to terms and conditions.
1.2.	Upon approval, the platform automatically grants access and sends a confirmation email, reducing manual intervention in the process.
2.	**Single Sign-On**
2.1.	The platform supports Single Sign-On for platform management.
2.2.	If APPA adds additional programs to the platform in the future (outside of the scope of this RFP), the platform will enable users to access multiple applications on the platform using a single profile.
3.	**User Roles**
3.1.	The platform has the ability to configure role-based permissions (e.g., applicant, grader, approver) for system use.
4.	**Flexible Question Formats**
4.1.	The platform supports various question formats (e.g., true, or false, multiple choice, select all that apply, table, text box) to allow for a dynamic and adaptable application process.
5.	**Question Branching Logic**
5.1.	Answers direct users to the relevant questions based on their previous answers.
6.	**Upload and Attachment Capabilities**
6.1.	The platform allows applicants to upload or attach supporting documentation.
6.2.	The platform automatically scans attachments for potential malicious files or code.

7.	**Auto-Grading Functionality**
7.1.	The platform incorporates auto-grading capabilities for questions that do not require review of attachments or written responses, streamlining the evaluation process.
8.	**Customizable Scoring Rubrics**
8.1.	The platform allows the ability to adjust scoring criteria based on specific application requirements.
9.	**Collective Answer Viewing**
9.1.	Graders can view all answers collectively to simplify the review process.
10.	**Progress Saving and Tracking**
10.1.	All users (APPA staff, graders, and applicants) are able to save their in-process applications and return later to complete and submit them.
10.2.	All users can see their progress in completing the application.
11.	**Reporting Capabilities**
11.1.	The platform offers enhanced reporting features to analyze trends and provide valuable insights into application submissions.
11.2.	The platform includes automated reporting capabilities, allowing APPA to generate reports without manual intervention, supporting data analysis and informed decision-making.
11.3.	The platform provided direct file viewing that significantly reduces manual tasks for graders where manual review is necessary.
12.	**User-Friendly Design**
12.1.	The platform offers a highly intuitive interface that enhances usability for both applicants and graders.
12.2.	The platform is compliant with the Web Content Accessibility Guidelines to ensure accessibility for all users.
13.	**User Support Resources**
13.1.	Built-in training materials or help resources (e.g., user manuals, training videos) assist users in navigating the system.
13.2.	Error messages are provided when fields are not filled out properly, guiding users to correct their submissions and enhance overall usability.
14.	**API or System Integration Capabilities**
14.1.	The platform supports Application Programming Interfaces (APIs) or integration with other software applications or systems (e.g., Salesforce, Snowflake) to enable secure data exchange.
14.2.	The platform utilizes modular design principles to allow independent development, testing, and maintenance.
15.	**Historical Application Access**
15.1.	Users can easily access and reference previous years' applications for smoother reapplications.
15.2.	Contractor can describe their data migration strategies, API documentation standards, and data mapping requirements.
16.	**Attachment Access**
16.1.	Graders can access attachments directly within the application without needing to download them.
17.	**Printing Capabilities**
17.1.	Applicants can print their applications (completed or not).

Security Requirements	
18.	**Authentication and Access Management**
18.1.	The platform supports strong authentication protocols such as SAML 2.0 or multi-factor authentication and utilizes role-based access controls.
19.	**Audit Logging and Monitoring**
19.1.	The Contractor conducts regular audits at agreed intervals of all user and administrator account activity to ensure security of the platform and compliance with cybersecurity requirements. APPA also will have the ability to access logs and conduct their own audits.
19.2.	Logs are retained for a minimum of 180 days.
19.3.	The platform is capable of integration with a security information and event management system or other monitoring tools.
20.	**Security Framework Alignment**
20.1.	Contractor articulates its alignment to industry security standard(s).
20.2.	The platform incorporates robust security protocols and leverages industry standards and frameworks (e.g., NIST 800-171 or Cybersecurity Framework, Cybersecurity Maturity Model Certification Level 2, CIS Controls, ISO 27001, FedRAMP High).
20.3.	Security controls for the platform include FIPS 140-2-compliant encryption of data at rest and in transit.
20.4.	The Contractor demonstrates third-party validation of effective control implementation for that framework or control set through independent audits, including but not limited to SOC2.
21.	**Incident Response**
21.1.	Contractor has an incident response plan for the platform and reviews on an annual basis, at a minimum.
21.2.	Contractor has defined recovery time objective (RTO) and recovery point objective (RPO).
22.	**Data Retention**
22.1.	Contractor implements a data retention policy for the platform that describes the approach for data lifecycle management and establishes a clear retention period.
22.2.	Only data essential for application functionality and security shall be collected and retained for only as long as necessary based upon the purpose it is collected, and the policy should include a secure disposal method.
22.3.	Contractor has a process for data transition or handover in case of future vendor change (if required).
23.	**Other**
23.1.	Contractor demonstrates how the platform incorporates a secure architecture to minimize risk.
23.2.	The platform allows for customizable security configurations, allowing for future APPA programs (if added, outside of the scope of this RFP) to have different security settings.
23.3.	Contractor is obligated to notify APPA of any cyber incident that impacts the application or any related data within 48 hours.

APPA has also identified additional platform features that would be "nice-to-have," and inclusion of these features in initial deployment would be a bonus.

Table 2: Additional Features

"Nice-to-Have" Features	
1.	**Real-Time Notifications**
1.1.	Alerts for users regarding application status updates or important deadlines.
2.	**Feedback Mechanism**
2.1.	A feature that allows users to provide feedback on their experience to inform future improvements.

Overall APPA Expected Outcomes: Public power utilities will have a single platform through which they can easily and securely fill out applications for multiple APPA designation programs.

Role of Contractor:

1. Contractor will customize a SaaS offering to meet APPA's needs.
2. Contractor will work with APPA program managers and other staff to identify and account for designation program-specific requirements.

Role of APPA:

1. APPA will provide the questionnaire (question language, scoring, etc.) and other information as required for Contractor to finalize platform customization.
2. APPA will be the primary daily user of the platform and will oversee its use by applicants and graders.

Deliverable 2: Ongoing Maintenance and Support

Overall APPA Objective: Ensure that the platform remains operational and make updates as necessary to accommodate changes to the program or questionnaire and user feedback. Contractor will also continue to apply security updates, as necessary.

APPA Technical Approach: Contractor will service the platform.

Overall APPA Expected Outcomes: Platform will remain reliable and secure through the program lifecycle.

Role of Contractor:

1. Contractor will maintain basic functioning of the platform, including security updates.
2. Contractor will provide technical support, as necessary, to ensure the platform operates as intended.
3. As APPA provides requests for changes to the platform or any of its functions, Contractor will consider requirements and inform APPA of feasibility and cost (if any).

Role of American Public Power Association (APPA):

1. APPA will interface with members using the platform for any programmatic and technical issues and inform Contractor.
2. APPA will document any desired changes and provide requirements to Contractor.

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, Virginia 22202-4804

www.PublicPower.org

202.467.2900