AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Public Power Cybersecurity Scorecard 2019 Annual Report

December 2019

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

Prepared for American Public Power Association by Axio Global, Inc.

Program Lead: Nathan Mitchell, American Public Power Association

Cybersecurity Scorecard Architect: Axio Global, Inc.

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

In 2016, the American Public Power Association funded the creation of a cybersecurity self-assessment to aid small and medium public power utilities in consistently measuring their cybersecurity capabilities, benchmarking to their peers, and tracking progress to more mature cybersecurity practices. The resulting Cybersecurity Scorecard is accompanied by an online platform, also funded by APPA through a cooperative agreement with the US Department of Energy (DOE). In 2019, 328 utilities interacted with the Cybersecurity Scorecard. This represents an 82.2% increase in the number of utilities using the Scorecard in 2019 compared to 2018.

This report is an update to the 2018 Public Power Cybersecurity Scorecard Pilot Benchmark Report and creates an overall picture of the cybersecurity capabilities of public power utilities. Moreover, this report supports the previous year's findings and provides a consistent approach for supporting DOE's Multiyear Plan for Energy Sector Cybersecurity.

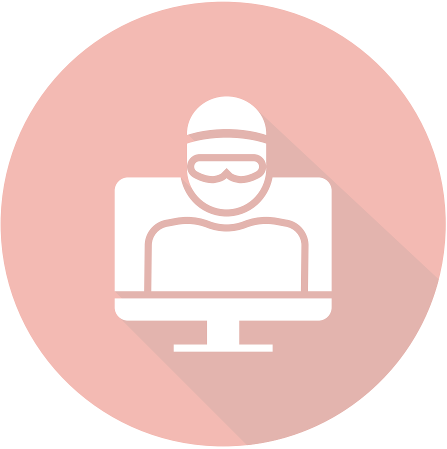
Adoption of the Cybersecurity Scorecard

- The target for 2019 was to reach 400 utilities by the end of the calendar year. As of the publication of this document, 328 utilities completed at least one assessment, and many have completed more than one assessment, resulting in 688 total assessments.
- Even though the 2019 goal of 400 was not reached, the 328 signups show the capability of the program to reach the target audience and deliver resources to geographically diverse utilities.
- Based on the trends in scorecard use after a workshop, a minimum of eight regional workshops in 2020 are required to meet the desired target.

Key Findings and Recommendations

A 2017 report identified the following five recommendations for the overall APPA-DOE program based on the initial findings from regional workshops:

- Provide resources and information to utilities on cybersecurity program development, risk management, and supply chain management.
- Provide guidance on cybersecurity workforce management, including recruitment and training insights as well as guidance on how to leverage managed security providers.
- Create templates for incident response documents, tabletop exercises, and training.
- Pull insights from onsite vulnerability assessments, like those provided by APPA in its cooperative agreement, to examine best practices in logging and monitoring activities.
- Create training efforts on cybersecurity program and policy development, incident response, risk assessments, cybersecurity awareness, and information sharing.



Introduction

Public power utilities are facing real and escalating cyber threats across the country. These utilities generate roughly 10% of the power in the United States and serve 15% of electric power customers nationwide. The resilience and security of these entities is vital to the national and economic interests of the United States. To help its members navigate the increasingly complex cybersecurity landscape, APPA partnered with DOE and Axio to create the Public Power Cybersecurity Scorecard, which offers maturity model guidance based on popular standards.

The scorecard adopts recommended target profiles for APPA members based on cybersecurity practices in the DOE Cybersecurity Capability Maturity Model (C2M2).[1] The Cybersecurity Scorecard provides a staged approach for public power utilities to adopt and benefit from the C2M2. Any public power utility can follow the stages in the Cybersecurity Scorecard, regardless of the utility's size or reliability function in the nation's electric grid.

In 2019, APPA members completed the Public Power Cybersecurity Scorecard using the online platform powered by Axio360—an all-in-one cyber risk management tracking tool with benchmarking, dashboards, and reporting. The standardized data collection and measurement creates a combined picture of public power utilities and their cybersecurity capabilities. This report is an update to the 2018 Public Power Cybersecurity Scorecard Pilot Benchmark Report.

Overview of the Model

The Public Power Cybersecurity Scorecard is based on C2M2 Version 1.1 and incorporates elements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 1.1 and other relevant industry standards and guidelines. The model is intended to be flexible, technology neutral, and scalable across organizational boundaries. It adopts target profiles for public power utilities to help these organizations to measure maturity and prioritize cybersecurity investments.

Building on these concepts, the scorecard can be used to:

- Establish the current state of a utility cybersecurity program;
- Enable consistent and effective benchmarking of cybersecurity capabilities across internal business units or objectives—and even with other public power utilities;
- Guide cybersecurity program improvement;
- Share knowledge and best practices across public power utilities;
- Enable public power utilities to prioritize investments to improve cybersecurity; and
- Communicate targets and priorities to both internal and external stakeholders.

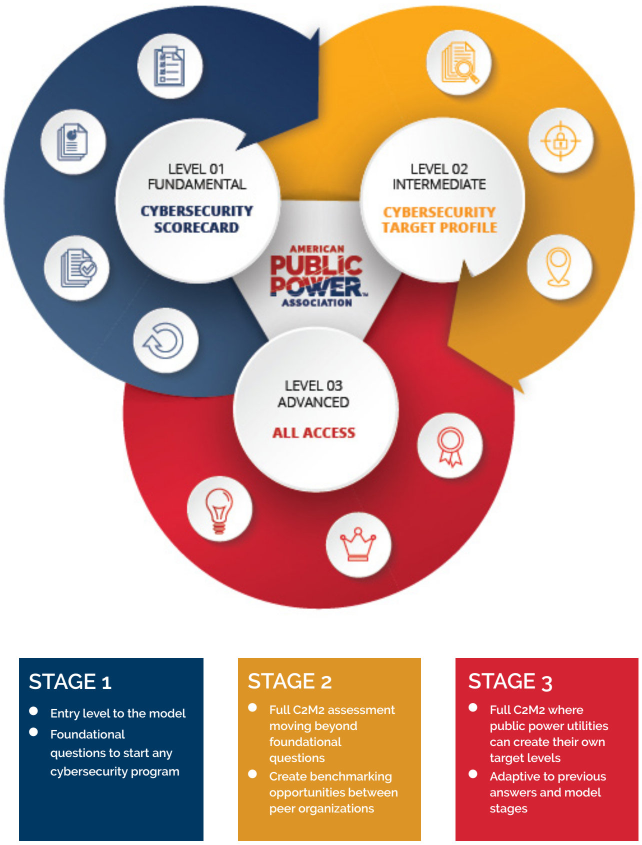
In 2019, DOE published updates and enhancements to the C2M2 model and released the model for public comment (C2M2 v2.0 comment period closed September 13, 2019).[2] To align with the NIST v1.1 Framework and accounting for public comments, Version 2.0 updates include the following:

- Establishing a Cybersecurity Architecture domain;
- Separating the MILs from the Information Sharing and Communications domain to include sharing practices in the Threat and Vulnerability Management and Situational Awareness domains;
- Movement of Continuity of Operations MILs from the Incident and Event Response domain to the Cybersecurity Program Management domain to account for continuity activities beyond response events; and
- Increasing the use of common language throughout the model.

[1] The C2M2 v1.1 was developed by the DOE in 2012 and has been widely adopted in the energy sector by both the electricity subsector and the oil and natural gas subsector. C2M2 is a 312-practice maturity model with four maturity indicator levels (MIL0 through MIL3).

[2] https://www.federalregister.gov/documents/2019/08/14/2019-17446/request-for-comment-on-the-doe-cybersecurity-capability-maturity-model-version-20

FIGURE 1. THE PUBLIC POWER CYBERSECURITY SCORECARD STAGES



STAGE 1

- Entry level to the model
- Foundational questions to start any cybersecurity program

STAGE 2

- Full C2M2 assessment moving beyond foundational questions
- Create benchmarking opportunities between peer organizations

STAGE 3

- Full C2M2 where public power utilities can create their own target levels
- Adaptive to previous answers and model stages

Key elements of the DOE proposed path forward, which inform further development and expansion of the Cybersecurity Scorecard, are as follows:

- Revitalize industry engagement by strengthening DOE outreach efforts within the sector;
- Make C2M2 the best cybersecurity maturity model, for example, perform technical sweeps of the model to ensure the current threat landscape and emerging technologies are adequately addressed in Version 2.0;
- Use the C2M2 program to better understand industry needs and inform prioritization of CESER CEDS Research & Development efforts; and
- Improve mapping, interoperability, and reciprocity with other models, e.g., NIST Cybersecurity Framework, TSA Pipeline Security Guidelines, or DoD's CMMC — to support framework adoption and increase the value of C2M2 for the Energy Sector.

Axio has been instrumental in the development of the C2M2 v2.0 and the Axio360 platform will be able to seamlessly incorporate any enhancements to the Scorecard when DOE officially releases the updated model.

The Cybersecurity Scorecard is intended to complement ongoing risk management processes. However, while the model is useful for discussing compliance activities, it is not a replacement for a compliance program. Utilities should discuss questions around compliance, including the mandatory North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, with the appropriate compliance authorities.

Public power utilities can use the scorecard to (1) identify security gaps within their security programs and (2) create a roadmap to improvement while leveraging industry standards. Even utilities without a formal security program can use the scorecard as a tool to help them create one.

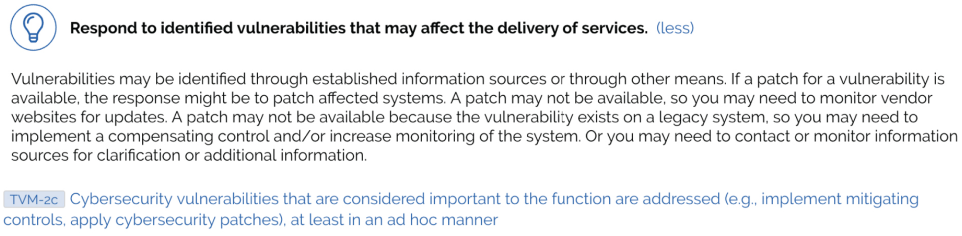
The three stages are listed in Figure 1.

Thanks to the model's unique structure, utilities that are new to the C2M2 can assess and prioritize their cybersecurity program in under an hour, using only the Stage 1 questionnaire. Stages 2 and 3 involve more mature practices and will require up to one day of evaluation time to complete.

Online Platform

The online Cybersecurity Scorecard platform offers customized reporting, dashboards, and self-assessment techniques for Stage 1 and the full C2M2. The full C2M2 platform has detail-oriented dashboards including benchmarks, target profiles, and implementation levels for each practice. The Stage 1 Cybersecurity Scorecard, on the other hand, is a lightweight survey covering the basic steps from the C2M2. As such, it is designed to get a utility from virtually no cybersecurity program to something that covers the fundamental steps. This means that additional analytics, like benchmarking, are not a focal point for the Stage 1 dashboard.

FIGURE 2. EXAMPLE CYBERSECURITY SCORECARD RECOMMENDATION



Respond to identified vulnerabilities that may affect the delivery of services. (less)

Vulnerabilities may be identified through established information sources or through other means. If a patch for a vulnerability is available, the response might be to patch affected systems. A patch may not be available, so you may need to monitor vendor websites for updates. A patch may not be available because the vulnerability exists on a legacy system, so you may need to implement a compensating control and/or increase monitoring of the system. Or you may need to contact or monitor information sources for clarification or additional information.

TVM-2c Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches), at least in an ad hoc manner

When launched in early 2018, the platform was envisioned to be a hub of activity for APPA members. By linking training, improvement efforts, task tracking, and action items into one platform, users can guide their cybersecurity efforts to an improved state. Beyond task management, the platform offers recommendations for utilities about how to move forward, such as the example in Figure 2.

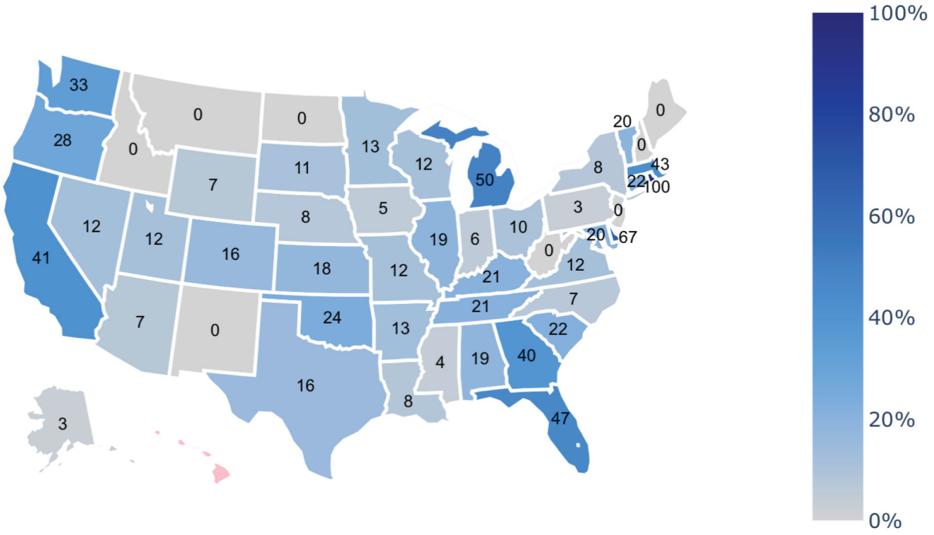
For utilities that are ready to move beyond Stage 1, additional features include target profiles for more mature practices, as outlined in the C2M2.

Adoption of the Cybersecurity Scorecard

In 2017, Axio performed a rigorous data analytics study on the demographics of all public power utilities, including clustering by size based on generation capacity, number of customers, and additional utility services provided (such as water, gas, and broadband communications). In 2019, Axio used that information to drive adoption of the Cybersecurity Scorecard through industry events and online campaigns. As of December 2019, the percentage of public power utilities using the scorecard has increased, but there is still effort needed to understand current state, improve preparedness/reliability, and develop resilience to cyber/physical attacks.

Figure 3 shows the percent of public power utilities using the Cybersecurity Scorecard by state. In 2019, regional workshops were held in the Northeast, Southeast, Midwest, and Western states, which corresponds to the color saturation on the map. For example, there is one public power utility in Rhode Island, and that utility completed the Cybersecurity Scorecard, therefore the saturation is 100% in the state. In Michigan, Florida, and Georgia, multiple outreach events have increased the saturation to 50%, 47%, and 40%, respectively.

FIGURE 3. CYBERSECURITY SCORECARD USERS IN THE UNITED STATES



Outreach Impact

The formal launch of the Cybersecurity Scorecard as a program occurred in 2018and began with outreach efforts to build awareness and encourage utilities to rate their implementation of basic cybersecurity practices through the assessment. In 2018, utilities completed 186 Cybersecurity Scorecard assessments. The target for 2019 was to reach 400 utilities by the end of the calendar year. As of the publication of this document, 328 utilities completed at least one assessment, and many have completed more than one assessment, resulting in 688 total assessments.

The upward trend in Figure 4 demonstrates that outreach plays a significant role in acceptance and adoption of the Cybersecurity Scorecard. Continued resources, marketing, and workshop efforts are needed to reach the nearly 400+ remaining targeted utilities that have not yet used the Cybersecurity Scorecard. Based on the trends in scorecard use after the conclusion of a workshop, indications are that a minimum of eight regional workshops in 2020 are required to meet the desired target. In addition to regional workshops, there is a need for scorecard facilitation training in the regions to increase information sharing and support cyber mutual aid, if needed.

Additional funding and resources are needed to encourage the remaining public power utilities to prioritize cybersecurity by assessing themselves with the Cybersecurity Scorecard. Even though the 2019 goal of 400 was not reached, the 328 signups shows the capability of the program to reach the target audience and deliver resources to geographically diverse utilities. An increased number of regional events and dedicated support activities to follow up to ensure completion of the assessment would help reach this goal.

FIGURE 4. IMPACT OF WORKSHOP OUTREACH EFFORTS ON CYBERSECURITY SCORECARD ADOPTION

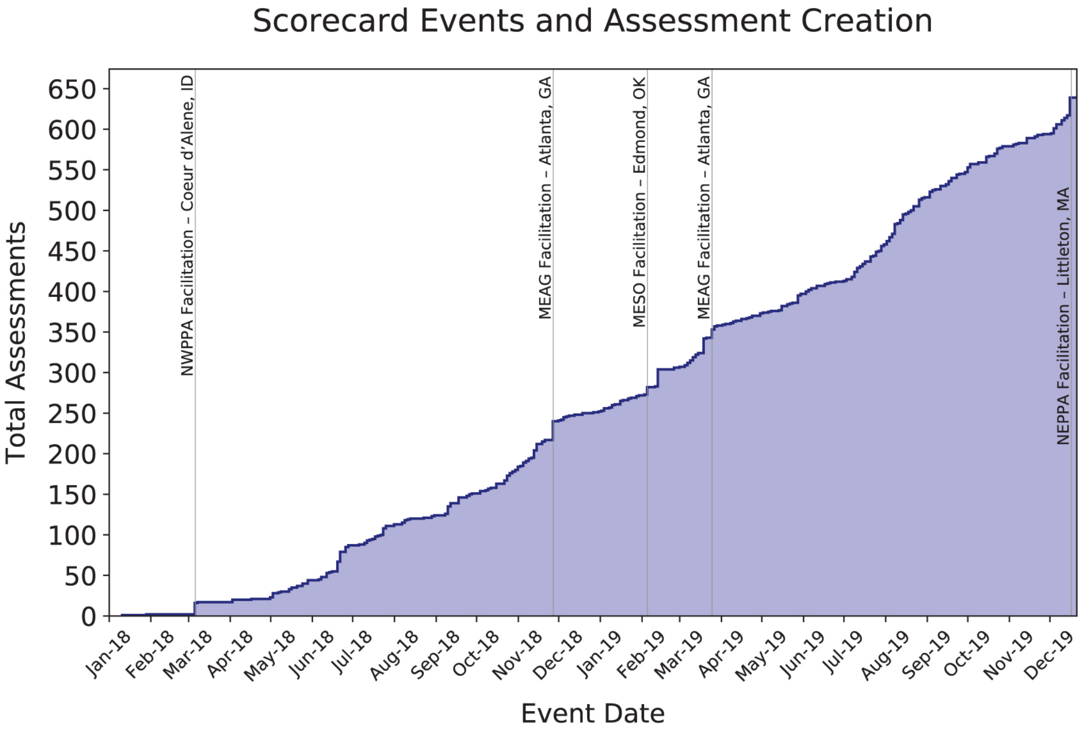
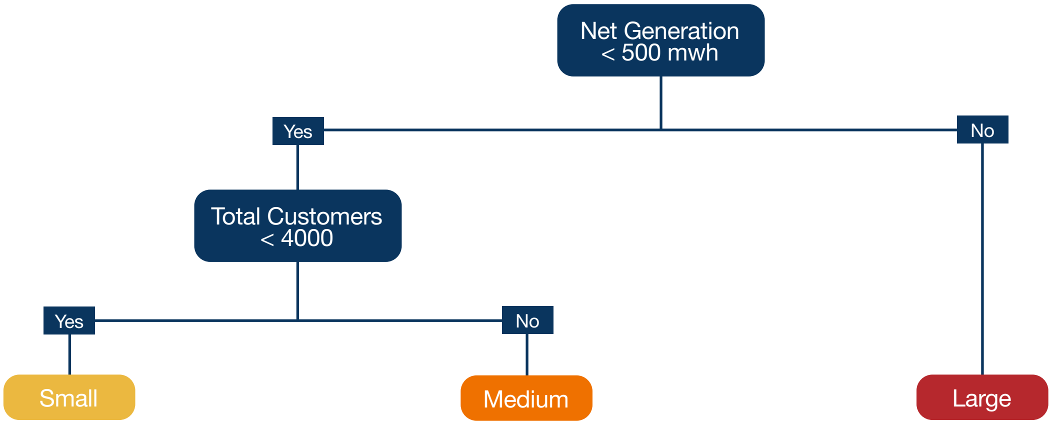


TABLE 1: COUNT AND CHARACTERISTICS OF UTILITIES IN EACH CLUSTER



Utility Size	Number of Public Power Utilities	Customer Count	NERC-Registered Entities
Small	1255	0 to 3,995 Average = 1,314	14
Medium	461	4,015 to 408,411 Average = 15,156	88
Large	290	0 to 1,458,330 Average = 49,575	157

Targeting the ~750 utilities with ICS on distribution systems

A 2017 demographics study identified a breakdown of large, medium, and small public power utilities based on data from the Energy Information Administration (EIA) and Platts. Using a machine learning clustering method that grouped utilities based on characteristics, Axio identified the above decision tree and table to describe what constitutes the size of a public power utility, based on the 2,007 such organizations in the United States.

The utilities that used the Cybersecurity Scorecard platform in 2019 include 130 large utilities, 132 medium utilities, and 59 small utilities.

The utilities using the platform also have a variety of characteristics worth noting:

- 45% are NERC registered entities
- 72% provide water services
- 58% provide telecommunication services
- 15% provide natural gas services

Most users perform multiple Cybersecurity Scorecard assessments. Out of 328 total utilities on the platform (as of the writing of this report), there are 688 completed assessments.

Out of those 688 assessments, more than 30% have moved beyond the scorecard and are working with the full C2M2, in support of DOE's Multiyear Plan for Energy Sector Cybersecurity. Unsurprisingly, larger utilities are more likely to perform multiple assessments—two to three, on average—while most medium and small utilities use only one Cybersecurity Scorecard assessment. Since larger utilities may have multiple information technology or operational technology systems and facilities, they frequently perform assessments across different scopes.

Cybersecurity Benchmarks

Benchmarks for the Cybersecurity Scorecard are measured both at an aggregate level, based on an index related to the Stage 1–3 assessments, and at a "domain," or topic, level. For the scorecard and this report, the domains are based on the C2M2 v1.1.

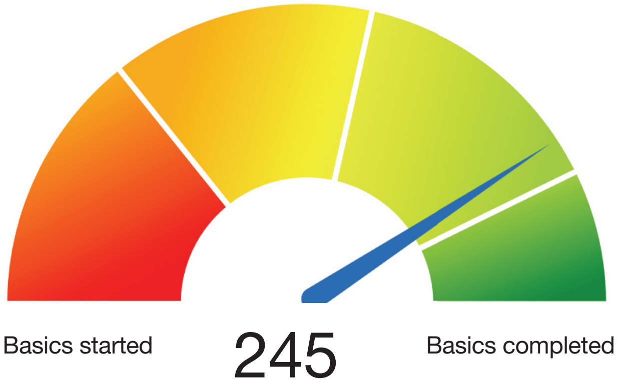
Cybersecurity Scorecard Benchmarks

The Cybersecurity Scorecard is a simple survey comprising 14 questions that map to 51 practices in the C2M2 (at the fundamental Maturity Indicator Level (MIL) 1). As such, the index is only from 0–300 with a very simple graphical interface for the Cybersecurity Scorecard dashboard, as seen in Figure 5.

This provides users with an aggregate score that is both easy to report and compare to others, including those using the full C2M2 (where the index is 0–1000).

The 2017 report highlighted various trends based on pre-Cybersecurity Scorecard data. In 2018, the transition to the Cybersecurity Scorecard software platform was completed. In 2019, the Cybersecurity Scorecard software platform allowed for standardized and consistent measurement of public power cybersecurity programs and facilitated improvement. The 2019 findings are similar to previous years' reports, highlighting a need for better risk management techniques, situational awareness, and supply chain risk management.

FIGURE 5. EXAMPLE SCORECARD GRAPHIC FROM A STAGE 1 SURVEY



The scorecard is broken into multiple stages, allowing an easy entry for utilities with no security experience to assess their capabilities and make planned improvements. Stage 1 of the scorecard is accessed through a web-based interface that allows utilities to assess their current state of cybersecurity by answering a set of 14 multiple-choice questions in the areas of Asset and Access Management; Change Management; Incident Response; Threat, Vulnerability, and Risk Management; Supplier/Vendor Management; Information Sharing; Situational Awareness; Workforce Management; and Cyber Program Management. The questions are written in accessible language and facilitate an assessment of a utility's current state of practices and activities for both the traditional IT and OT environments.

The practices are measured on an index of 0–300. To reach Stage 1, which involves meeting practices considered to form the basic elements of any cybersecurity program, users will score at least 240 out of the total possible score of 300. During pilots and demonstrations, utilities were able to understand and plan for the implementation of all Stage 1 Cybersecurity Scorecard practices in less than a year.[3]

Once a utility's score passes 240, the utility is encouraged to engage with the additional practices in Stage 2, which expands the index to 0–1000. Stage 2 of the Scorecard introduces additional capabilities as a new "target profile" within the DOE Cybersecurity Capability Maturity Model (C2M2). Among the public power utilities on the Cybersecurity Scorecard platform, most appear ready for Stage 2, as the median score is above 240.

Similar to 2018, the journey from the Cybersecurity Scorecard to full C2M2 is a seamless process. To-date, roughly 30% of all public power utilities that started with the Scorecard have since converted to the full C2M2, which supports the DOE Multiyear Plan for Energy Sector Cybersecurity.[4]

[3] More information about the Cybersecurity Scorecard can be found at: https://www.publicpower.org/resource/cybersecurity-scorecard

[4] More information can be found at: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

Figure 6 represents the achievement of the public power target profile across all APPA full C2M2 assessments. Of the 182 practices in scope for the target profile, an assessment is considered to have attained all of the ones where the practice is rated at either Largely Implemented or Fully Implemented. See the Appendix for further explanation on target profiles.

FIGURE 6. ACHIEVEMENT OF APPA TARGET PROFILE

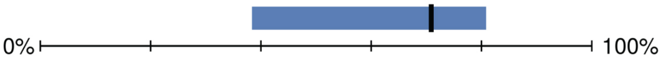


Table 2 shows the percentage of the 182 targeted practices that each full C2M2 assessment has attained. The minimum achievement is 2% of the APPA target profile. 87% of assessments achieved at least 25% of the APPA target profile. 65% of the assessments achieved 50% or more of the APPA target profile, and 38% of the assessments achieved 75% or more of the APPA target profile. 27% of the assessments have achieved at least 80% of the APPA target profile, 7.5% of the assessments have achieved 90% or more of the APPA target profile, and 1% have achieved 100%.

Once a utility has reached the APPA target profile, they are ready to go on to Stage 3, which is the full C2M2. Using the full C2M2, utilities can select additional target practices that go beyond the target profile in Stage 2 and a date by which they are aiming to improve their implementation level on that practice. This graduated maturity path is intended to accommodate the diversity in the utilities and the energy sector as a whole.

TABLE 2. NUMBER OF UTILITIES REACHING 50% OR GREATER OF THE PUBLIC POWER TARGET PROFILE

Number of utilities	Percentage of public power target profile attained
1	100%
8	90%
28	80%
40	75%
68	50%

In 2019, DOE completed the development of C2M2 version 2.0 and released the model for public comment.[5] Proposed updates include the following:

- Establishing a Cybersecurity Architecture domain
- Separating practices from the Information Sharing and Communications domain to include sharing practices in the Threat and Vulnerability Management and Situational Awareness domains
- Moving Continuity of Operations practices from the Incident and Event Response domain to the Cybersecurity Program Management domain to account for continuity activities beyond response events
- Increasing the use of common language throughout the model

The Cybersecurity Scorecard activities completed to date show the continued need for meeting utilities where they are on their cyber journey while having a growth plan to continue to identify and mature cyber programs for public power in alignment with DOE. Currently, the scorecard program serves the utilities that are early in the cyber program maturity lifecycle and assists them in a path of growth and capability development that culminates in establishing and maintaining the Stage 2 APPA target profile.

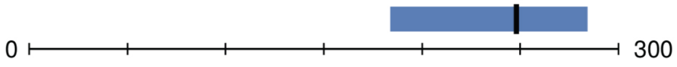
Aggregated Index Benchmark

Figure 7 shows the middle 50% of the scores for the overall Stage 1 Cybersecurity Scorecard assessments, with the black line representing the median score.

The current set of 328 utilities using the Cybersecurity Scorecard had a median score of just under 250, which is a good initial value. It is important to note, however, that 25% of the data set is below 200, indicating that these utilities need more resources and training.

The following subsections examine each domain and the Stage 1 benchmarks.

FIGURE 7. AGGREGATED INDEX BENCHMARK

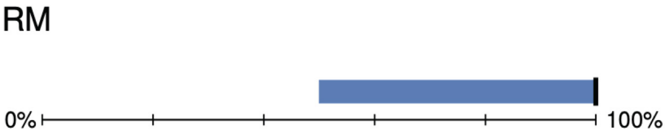


[5] https://www.federalregister.gov/documents/2019/08/14/2019-17446/request-for-comment-on-the-doe-cybersecurity-capability-maturity-model-version-20

Risk Management (RM)

The goal of the RM domain is to establish, operate, and maintain an enterprise cybersecurity risk management practices to identify, analyze, and mitigate cybersecurity risk to the public power utility.

The box plot and median score (out of 100%) is below.

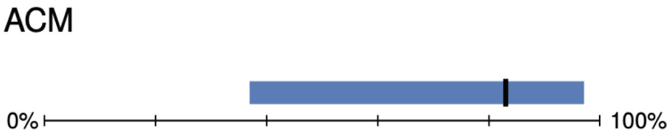


At Stage 1, RM is only two (2) cybersecurity practices on identifying and then handling identified cybersecurity risks. The median is at 100%, but several utilities still need help with the basic concepts on cyber risk management, integration into the larger enterprise risk management program (if such a program exists), and increasing understanding of the financial impact from a cybersecurity risk.

Asset, Change, and Configuration Management (ACM)

The goal of the ACM domain is to manage the public power utility's OT and IT assets, including both hardware and software.

The box plot and median score (out of 100%) is below.



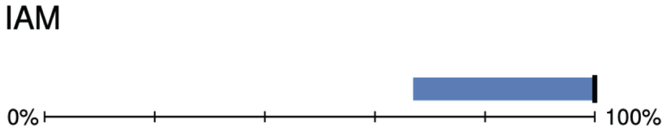
ACM is one of the foundational elements of any cybersecurity program—understanding your assets is key to keeping them protected. The strong score in ACM here could be an indicator of the high percentage of OT-based personnel using the Scorecard, which we uncovered during our outreach.

One of the key things worth mentioning is that the scope of an assessment may often include OT and IT assets. One goal for outreach in 2020 would be to assist Cybersecurity Scorecard users in differentiating between OT and IT scopes and when it makes sense to have a separate assessment for OT and IT respectively. The different scopes could help with ensuring that all assets that contribute to the cybersecurity profile are accounted for, even when managed by an outside vendor.

Identity and Access Management (IAM)

The goal of the IAM domain is to create and manage identities for employees or contractors that may be granted logical or physical access to the public power utility's assets and to control access to those assets.

The box plot and median score (out of 100%) is below.

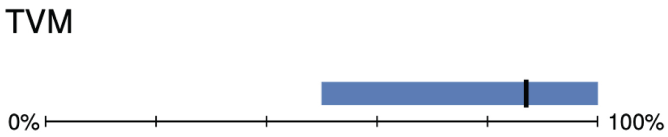


IAM, much like ACM, is a foundational element to any cybersecurity program, and covers the need to know who is using your assets and managing his or her access. OT environments tend to have higher self-assessment scores in this domain because there are a limited number of employees and contractors working in engineering environments, and utilities tend to know who each of those people are. There is also a need to distinguish OT practices from IT practices to ensure that identities are managed consistently whether or not the utility or a third-party vendor or service provider manages the identities.

Threat and Vulnerability Management (TVM)

The goal of the TVM domain is to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities.

The box plot and median score (out of 100%) is below.

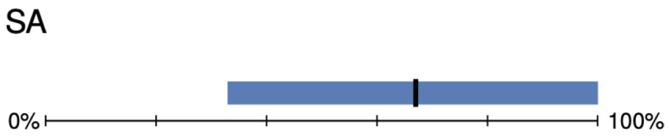


The TVM domain is where many utilities focus their cybersecurity efforts. Some of these efforts may be very rudimentary and rely on vendors for vulnerability information and patch management. At Stage 1, these efforts will be minimal. While the median may be high (100%), there are still many utilities—primarily smaller ones—that struggle in this area.

Situational Awareness (SA)

The goal of the SA domain is to establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information.

The box plot and median score (out of 100%) is below.

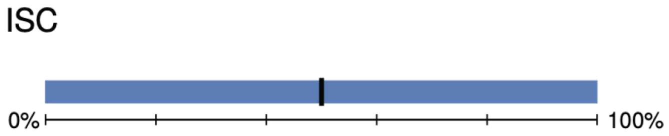


The SA domain has some of the lowest scores across the Cybersecurity Scorecard, which has some cause for alarm. It implies that many utilities lack the ability to detect cybersecurity incidents. While other scores indicate that public power utilities can manage their assets, people, and vulnerabilities, detection and situational awareness is a key initial step to any security program.

Information Sharing and Communications (ISC)

The goal of the ISC domain is to establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threat and vulnerability information, to reduce risks and to increase operational resilience.

The box plot and median score (out of 100%) is below.

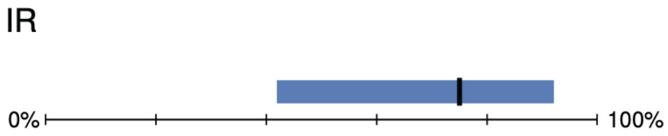


Information sharing in the ISC domain is largely related to how US-CERT, ICS-CERT, the E-ISAC, and APPA coordinate with public power utilities (and vice versa). Again, a high median score indicates relatively healthy practices, but the range of the box plot also indicates that many utilities need help on how to communicate and work with information sharing organizations. In 2020, the focus will be on bringing together the resources of joint action agencies to increase awareness and act as an information sharing community.

Event and Incident Response, Continuity of Operations (IR)

The goal of the IR domain is to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.

The box plot and median score (out of 100%) is below.

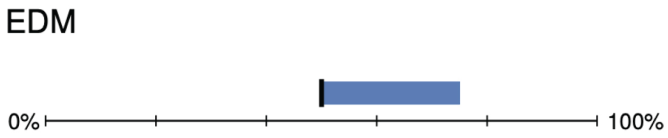


The IR domain has, by far, the most practices in the Cybersecurity Scorecard at all stages. This is because incident response and the ability to recover from a cyber incident quickly are vitally important to reliable operations for public power utilities. Because there are so many practices in IR, this range may be deceptive—while it looks to be similar to SA or another domain, there are many more practices in IR not being performed, on average, across the utilities who completed the scorecard. The development of the Public Power Cyber Incident Response Playbook in 2019 is a good start to supporting this practice.

Supply Chain and External Dependencies Management (EDM)

The goal of the EDM domain is to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities.

The box plot and median score (out of 100%) is below.

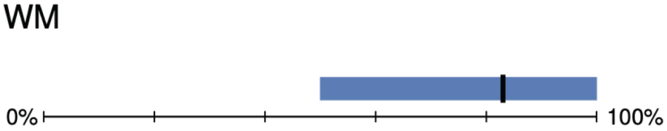


Supply chain risk within EDM is one of the largest gaps in public power utilities and will require a significant focus for APPA to help improve scores. This is not, however, unique to public power. Many utilities are struggling with how to evaluate contractors, suppliers, and even customers on their cybersecurity capabilities to ensure that an attack on the supply chain will not negatively impact reliable operations. A recommended continued next step for 2020 should include distilling guidance, such as the DOE Procurement Guidelines for Energy Delivery Systems, for small utilities that need help in this area.

Workforce Management (WM)

The goal of the WM domain is to establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of employees and contractors.

The box plot and median score (out of 100%) is below.

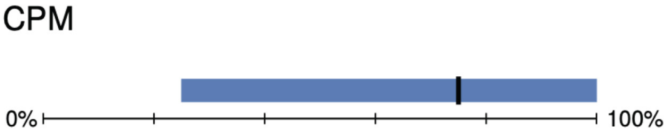


Our previous surveys have shown a consistent and strong set of capabilities in public power utilities for workforce management. While the median is lower than some areas (such as IAM), the overall range is consistent with the 2018 benchmark report. The strength in the WM domain will be further highlighted across the Stage 2 and Stage 3 benchmarks, covered in the next section.

Cybersecurity Program Management (CPM)

The goal of the CPM domain is to establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the public power utility's cybersecurity activities.

The box plot and median score (out of 100%) is below.



The CPM domain range here shows that there are many utilities that do not manage a cybersecurity program—rather, in subsequently stronger cybersecurity practices like ACM and IAM, those activities appear to happen without a cohesive strategy element, which could impede the effectiveness of the overall program. Some public power utilities might never be able to implement their own cybersecurity strategy. In those cases, APPA should consider providing templates for security strategies to help smaller members mature in this area.

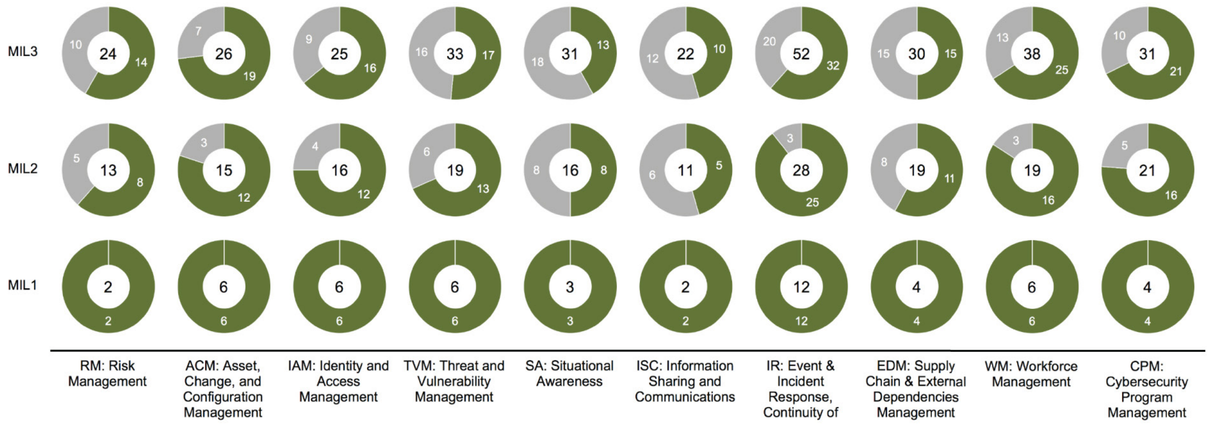
C2M2 Benchmarks and the Target Profile

Within the Cybersecurity Scorecard, Stage 2 introduces more advanced practices from the C2M2. These are captured through the use of MIL 2 and MIL 3 capabilities from the original DOE model. As discussed in Section 2.3 on adoption and use, nearly one third of all public power utilities on the platform have moved beyond Stage 1 and are measuring their cybersecurity program against the larger set of more mature practices. This section explores how those utilities compare to the public power target profile, with recommended improvements both to the profile and the educational outreach APPA should explore.

In 2017, APPA leveraged a subject-matter expert working group to analyze all of the practices within the C2M2 and evaluate which practices a utility member should target after Stage 1 levels have been achieved. Out of the 312 practices, 182 were selected, as outlined in Figure 8.

(Note: Grey is used to indicate those practices that are not targeted for implementation under this stage of the Scorecard model.)

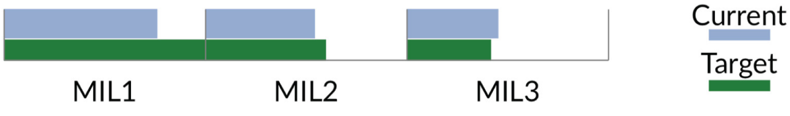
FIGURE 8. THE CYBERSECURITY SCORECARD TARGET PROFILE



In Figure 8, each omitted C2M2 practice from the target profile is greyed out. Using the Cybersecurity Scorecard Target Profile, utilities can better focus their limited resources and attention on closing the most meaningful gaps in their cybersecurity practices.

These 182 practices are considered the building blocks for public power utilities seeking to advance their program beyond the 51 practices in Stage 1. Figure 9 compares these 182 targeted practices to the self-assessed practices from Stage 2 public power utilities. The green bar, which represents the 182 targeted practices, is compared to the aggregated and anonymized utility data. Overall, it appears that utilities in Stage 2 are performing more MIL3 practices than the Cybersecurity Scorecard Target Profile contains; however, those utilities might not be performing more basic MIL2 activities, which are a prerequisite to achieving MIL3. It is notable that there are a few domains in which the utility data indicates that members, on average, are above the Cybersecurity Scorecard Target Profile for Stage 2.

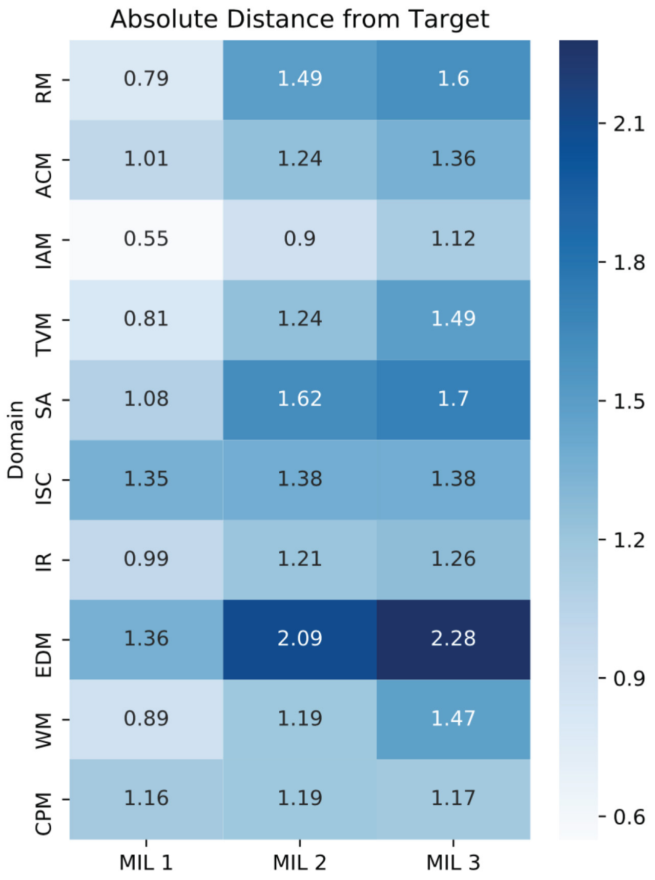
FIGURE 9. STAGE 2 CYBERSECURITY SCORECARD UTILITIES COMPARED TO THE TARGET PROFILE



A detailed breakdown per domain is included in the Appendix. The comparisons, unsurprisingly, shadow the results from Stage 1. In particular, there is additional need for situational awareness, supply chain, and overall cyber program management education and resources for public power utilities. Figure 10 shows the absolute distance from the anonymized average at Stage 2 and the target levels. The Cybersecurity Scorecard offers four levels, Not Implemented, Partially Implemented, Largely Implemented, and Fully Implemented. For these graphics, each level can be treated as an integer, with a caveat.[6] For each practice in the Cybersecurity Scorecard Target Profile, the total number of levels between the current level and the target level is calculated across all assessments to get the mean distance between the current and target profiles by MIL/domain. The larger the number, the more distance needs to be covered to meet the target. For MILs 2 and 3, only practices that are targeted by APPA are included.

[6] It is worth noting that these response levels are not numeric, so the distance between Not Implemented and Partially Implemented may mean something different than the distance between Largely Implemented and Fully Implemented, yet this method of representation will not distinguish between the categories.

FIGURE 10. AGGREGATED STAGE 2 UTILITY SCORES COMPARED TO THE CYBERSECURITY SCORECARD TARGET PROFILE



This once again highlights the overall gaps in situational awareness, supply chain, and risk management practices. More mature practices in workforce management, threat and vulnerability management, and information sharing are also not being performed compared to the Stage 2 target profile.

FIGURE 11. PERCENTAGE OF AGGREGATED STAGE 2 UTILITIES' SCORES BELOW THE CYBERSECURITY SCORECARD TARGET PROFILE

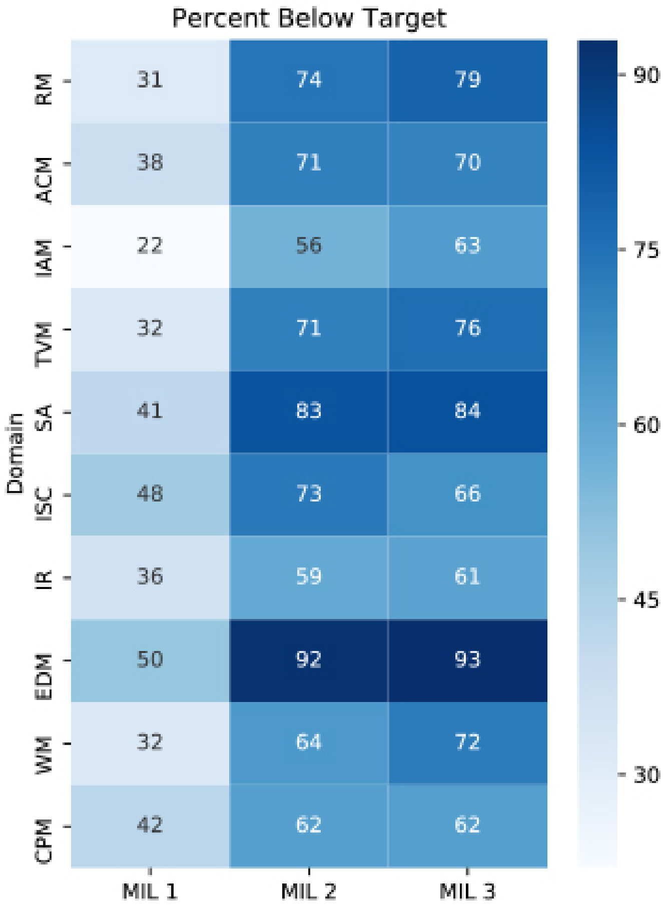
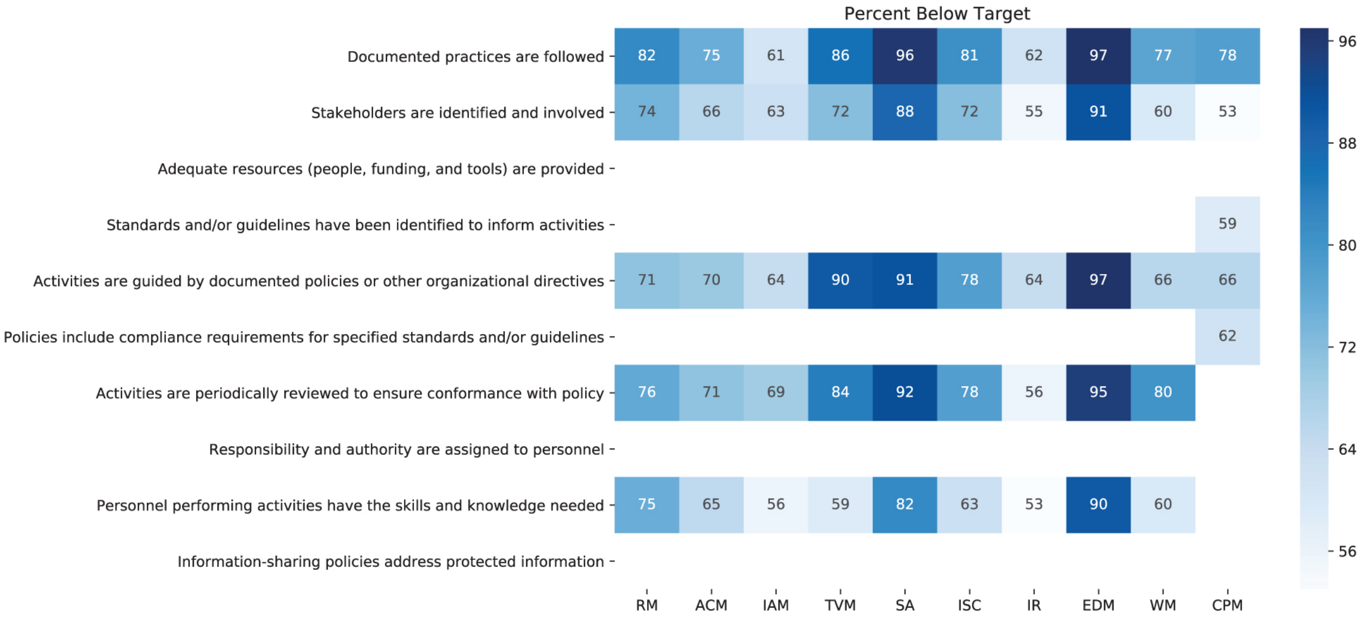


Figure 11 shows the percentage of utilities that are below the target profile.

As with Figure 10, this shows the need for additional guidance and resources across supply chain and situational awareness.

FIGURE 12. PERCENTAGE OF UTILITIES IN STAGE 2 BELOW TARGET



	RM	ACM	IAM	TVM	SA	ISC	IR	EDM	WM	CPM
Documented practices are followed	82	75	61	86	96	81	62	97	77	78
Stakeholders are identified and involved	74	66	63	72	88	72	55	91	60	53
Adequate resources (people, funding, and tools) are provided										
Standards and/or guidelines have been identified to inform activities										59
Activities are guided by documented policies or other organizational directives	71	70	64	90	91	78	64	97	66	66
Policies include compliance requirements for specified standards and/or guidelines										62
Activities are periodically reviewed to ensure conformance with policy	76	71	69	84	92	78	56	95	80	
Responsibility and authority are assigned to personnel										
Personnel performing activities have the skills and knowledge needed	75	65	56	59	82	63	53	90	60	
Information-sharing policies address protected information										

Management Benchmarks

One concept introduced in Stage 2 is that of management practices. These practices build on each other to create an overall management plan for each domain in the C2M2 and Cybersecurity Scorecard. Each domain repeats the management practices, recognizing that the allocation of resources to certain areas will differ across domains. The original C2M2 guidance had between 6 and 10 management practices for each domain, depending on the area. It is important to note that not every management practice was selected for the 2017 Cybersecurity Scorecard Target Profile—most notably, the subject matter experts believed that standards, compliance, assigned responsibilities, and adequate resources should not be measured in the target profile. Figure 12 shows the percentage of utilities in Stage 2 below the target level for each management practice.

Key Findings and Recommendations

The 2017 benchmarking report identified the following five recommendations for the overall APPA-DOE program based on the initial findings from regional workshops:

- Provide resources and information to utilities on cybersecurity program development, risk management, and supply chain management.
- Provide guidance on cybersecurity workforce management, including recruitment and training insights as well as guidance on how to leverage managed security providers.
- Create templates for incident response documents, tabletop exercises, and training.
- Pull insights from onsite vulnerability assessments, like those provided by APPA in its cooperative agreement, to examine best practices in logging and monitoring activities.
- Create training efforts on cybersecurity program and policy development, incident response, risk assessments, cybersecurity awareness, and information sharing.

Many of these recommendations continue to be addressed and do not change significantly based on the 2019 findings. This report also supports the findings of several working groups within the other CEDS programs, such as implementing and testing the Public Power Cyber Incident Response Playbook and meeting the stages as described in the Public Power Cybersecurity Roadmap.

The Scorecard provides recommendations to the utility based on any identified gaps and allows tracking and assigning of actions to close these gaps. For example, many utilities identified the lack of a documented incident response plan as a gap in their cyber programs. When APPA published the Public Power Cyber Incident Response Playbook[7] in August 2019, many utilities that had previously identified a gap in this area completed the playbook templates, thus developing a relevant set of response contacts and prepared actions in the event of a cyber incident. Subsequently, a utility could then mark the practices that addressed its incident response plans as complete within the Scorecard assessment and increase its score in the platform. In the case of Incident Response, findings from the Scorecard directly influenced the development of the Playbook. This demonstrates that using the Scorecard data to identify areas in which there is a collective need in the community helps to raise the bar on cybersecurity for all.

[7] https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

As demonstrated by the increase in Cybersecurity Scorecard participants directly related to the conduct of a regional training and workshops, the need for continued outreach in the public power community is critical to increase awareness of and participation in improving cybersecurity. Community outreach assists with information sharing and exchange among constituents in the same region and can encourage cooperation in the event of a cyber attack.

The Public Power Cybersecurity Roadmap[8] is a strategic plan designed to help public power utilities develop a stronger, sustainable state of security that is continually monitored and improved upon. Developed with input from public power utilities' security, information technology, operational technology, and leadership experts, the roadmap breaks down how a public power utility can develop and implement an action plan to improve its cybersecurity practices into four manageable stages. The scorecard is the foundation to achieving the vision in the Roadmap.

Continued investment in the Cybersecurity Scorecard serves as the initial starting point for all utilities, no matter their level of cybersecurity maturity at the beginning of their journey. Moving the needle on the collective maturity of public power is vital to our community. The scorecard is the basis for a common understanding of the state of cybersecurity, solutions and challenges for all utilities, and a common language that is accessible to all constituents. Cyber threats will not decrease in the foreseeable future so efforts must be continued and increased so that we are fighting together.

As the adoption of the scorecard increases and the community matures its cyber practices, a clear analysis and path is required to support the larger strategic view of the energy sector. Key elements of the DOE's proposed path forward, which inform further development and expansion of the Public Power Cybersecurity Scorecard program, are as follows:

- Revitalize industry engagement by strengthening DOE outreach efforts within the sector;
- Make C2M2 the best cybersecurity maturity model, for example, perform technical sweeps of the model to ensure the current threat landscape and emerging technologies are adequately addressed in Version 2.0;
- Use the C2M2 program to better understand industry needs and inform prioritization of CESER CEDS Research & Development efforts; and
- Improve mapping, interoperability, and reciprocity with other models, e.g., NIST Cybersecurity Framework, TSA Pipeline Security Guidelines, or DoD's CMMC — to support framework adoption and increase the value of C2M2 for the Energy Sector.

Now that 328 public power utilities have leveraged the Cybersecurity Scorecard online platform, and taking into account the published direction from DOE, Axio would recommend the following to APPA to support the DOE vision:

- Use uniform messaging and marketing on the C2M2-based Public Power Cybersecurity Scorecard to drive increased participation in the program. This increases alignment between DOE and APPA on the use of the C2M2 as the basis for the Cybersecurity Scorecard and not a separate cybersecurity model or product.
- Expand both the number of utilities participating in the scorecard and the scope of the assessment areas to include all IT and OT assets under management.
- Establish user group outreach to address common challenges and solutions for utilities, particularly in the areas of threat and vulnerability management and documenting primary suppliers, to provide feedback to DOE on the current threat landscape and emerging technologies. This could also provide insights to policy makers on any concentration risk that could materialize from increased dependence on too few suppliers or service providers in the utility sector.

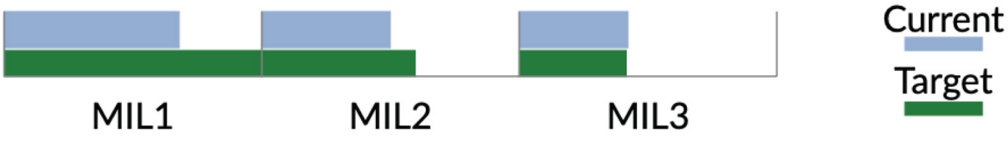
[8] https://www.publicpower.org/resource/cybersecurity-roadmap

- Conduct risk quantification scenario workshops to identify the cyber threats that could have the greatest impact on utilities and to better understand industry needs. Impact criteria in financial terms (dollars) and effect on utility delivery/business interruption (availability) are the recommended initial starting criteria. The risk factors documented in the quantification workshop could be directly related to the presence or absence of cyber practices, processes, or procedures, and serve as a source of continuous feedback to inform future investments in cybersecurity.
- Survey members on the types of services being delivered to their constituents and convene periodic working sessions with the Department of Commerce (NIST and Manufacturing Extension Programs), Department of Homeland Security, Department of Defense (CMMC), and the Environmental Protection Agency (Water). This could improve interoperability and reciprocity with other models because many public power utilities provide multiple municipal services (e.g., water, public works) and there is growing evidence that the C2M2 model works well for other these other services.

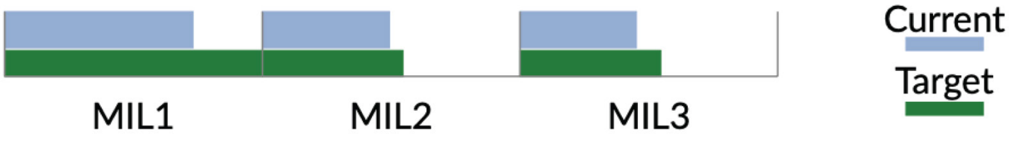
Appendix: C2M2 Benchmarks

Below are the C2M2 benchmarks and averages for pubic power utilities that have gone beyond the Stage 1 Cybersecurity Scorecard practices. The blue “current” score is compared to the green “target profile” established for Stage 2. Gaps in the bar chart represent either non-implemented (blue) or non-targeted (green) practices.

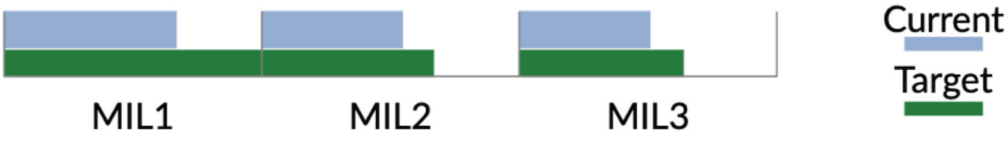
Overall



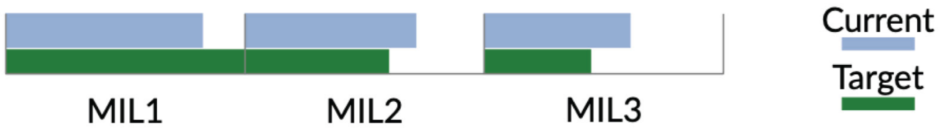
RM



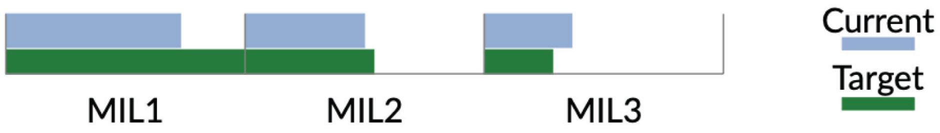
ACM



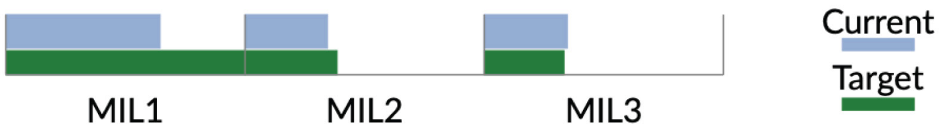
IAM



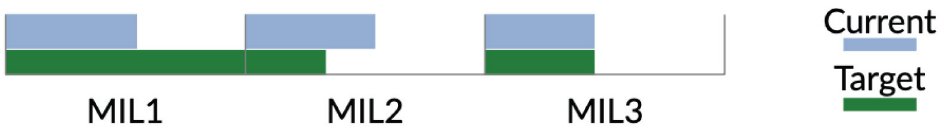
TVM



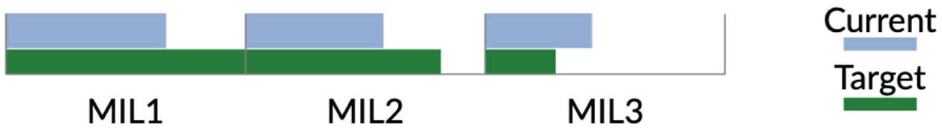
SA



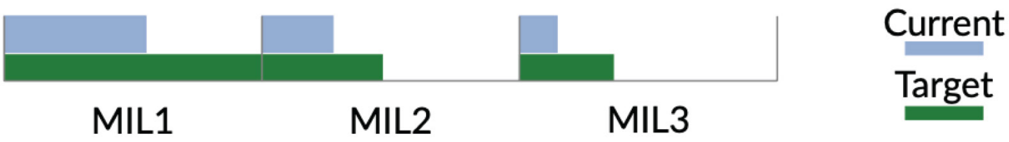
ISC



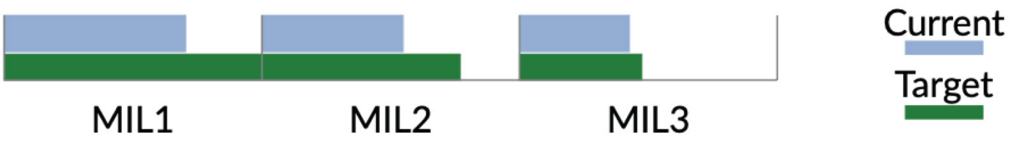
IR



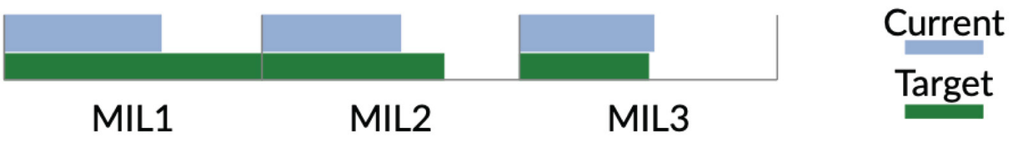
EDM


MIL1
MIL2
MIL3
Current
Target

WM


MIL1
MIL2
MIL3
Current
Target

CPM


MIL1
MIL2
MIL3
Current
Target

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

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