Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities

Michael Ingram and Maurice Martin
National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Technical Report
NREL/TP-5C00-67669
January 2017

Contract No. DE-AC36-08GO28308

NREL
NATIONAL RENEWABLE ENERGY LABORATORY

Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities

Michael Ingram and Maurice Martin
National Renewable Energy Laboratory

Prepared under Task No. EPSA.Z120

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

Technical Report
NREL/TP-5C00-67669
January 2017

Contract No. DE-AC36-08GO28308

NOTICE

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.

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Available electronically at SciTech Connect http:/www.osti.gov/scitech

Available for a processing fee to U.S. Department of Energy and its contractors, in paper, from:

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831-0062
OSTI http://www.osti.gov
Phone: 865.576.8401
Fax: 865.576.5728
Email: reports@osti.gov

Available for sale to the public, in paper, from:

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312
NTIS http://www.ntis.gov
Phone: 800.553.6847 or 703.605.6000
Fax: 703.605.6900
Email: orders@ntis.gov

Cover Photos by Dennis Schroeder: (left to right) NREL 26173, NREL 18302, NREL 19758, NREL 29642, NREL 19795.

NREL prints on paper that contains recycled content.

Acknowledgments

This document was prepared for Greg Singleton at the U.S. Department of Energy's Office of Energy Policy and Systems Analysis. The National Renewable Energy Laboratory (NREL) acknowledges the Office of Energy Policy and Systems Analysis encouragement and support throughout the process. In addition, the authors especially thank Anita J. Decker from the Northwest Public Power Association, Robert C. Jagusch from the Minnesota Municipal Utilities Association, and Gian Porro from NREL for their thoughtful comments.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Table of Contents

1 Introduction 1
1.1 Small Utilities 1
1.2 Reliability, Resilience, and Cybersecurity 2
1.3 Methodology 3
1.4 Prior Work 4
1.5 Specificity of Challenges to Small Utilities 5
2 Challenges 7
2.1 Scalability of Existing Guidance Documents 8
2.2 Governance 9
2.3 Risk Management 9
2.4 Asset, Change, and Configuration Management 9
2.5 Time Management 10
2.6 Metrics 10
2.7 Cost Recovery 11
2.8 Labor Pool 11
2.9 Technology Information 12
2.10 Siloed Information 12
2.11 Undocumented Processes 13
2.12 Summary 13
3 Applying Reliability, Resilience, and Cybersecurity, ... 15
3.1 Scaling Available Guidance 15
3.1.1 Tailoring 15
3.1.2 Phasing 15
3.2 Practical Examples 16
3.2.1 Governance 17
3.2.2 Risk Management 17
3.2.3 Asset, Change, and Configuration Management (ACM) 18
4 Federal Support for Improvement Efforts 20
4.1 Further Develop the NIST Cybersecurity Framework 20
4.2 Guide the ES-C2M2 20
4.3 Assist with Vulnerability and Risk Assessments and Emergency Restoration Plans 20
4.4 Stand Up a Distribution-Specific ISAC 21
4.5 Nurture Grassroots Efforts 21
5 Mutual Assistance 23
6 Conclusion 25
6.1 Process 25
6.2 Observations 25
6.3 Opportunities 26
6.4 Final Thoughts 26
References 28
List of Acronyms 29
Appendix A: Resources 30
Reliability 30
Resilience 30
Cybersecurity 31
Risk 33

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

List of Figures

Figure 1. Footprint of cooperative utilities throughout the United States. ***Image from the National Rural Electric Cooperative Association (2016)*** **2**
Figure 2. CMOM score compared to annual IT budget for five interviewed utilities **6**
Figure 3. Organization-level implementation model **7**
Figure 4. Challenges faced by the small utilities that were interviewed mapped to the organizational-level implementation model for improvement **8**
Figure 5. Project portfolios at large and small utilities **10**
Figure 6. Illustration of siloed information and communication challenges. **13**
Figure 7. Dependencies for the development of strategic goals and priorities **14**
Figure 8. Challenges faced by the small utilities that were interviewed mapped to the organizational-level implementation model for improvement **25**

List of Tables

Table 1. Format for example challenges **16**
Table 2. Example approach to addressing governance challenges **17**
Table 3. Example approach to addressing risk management challenges **18**
Table 4. Example approach to addressing ACM challenges **19**

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

1 Introduction

Small electricity utilities—those with less than 100 employees or 50,000 meters—provide essential services to large parts of the United States while facing a number of challenges unique to their mission. For instance, they often serve areas that are sparsely populated, meaning that their per-customer cost to provide service is higher. At the same time, they often serve customers that have moderate or fixed incomes, meaning that they are under strong pressure to keep costs down. This pressure puts them on a strict budget and creates a need for innovative solutions to common problems. Further, their service areas may include extreme climates, making severe weather events more frequent and their aftermaths more expensive to address.

This guide considers the following:

- Challenges that small utilities face while ensuring the reliability, resilience, and cybersecurity of their electric service
- Approaches for addressing those challenges using existing guidance documents
- Ways that the federal government could provide support in these areas.

Existing literature that focuses on small and under-resourced utilities is scarce (see Section 1.4); therefore, information developed for this guide was largely gathered through discussions held with a small set of utilities. These discussions uncovered interesting observations; but given the small sampling size, these observations should be considered only suggestive of possible findings for the broader small-utility population rather than decisive evidence of such findings.

1.1 Small Utilities

A review of the attributes of utilities interviewed in creating this guide illustrates what it means to be a "small utility." Most have less than 100 employees and less than 50,000 meters. They include rural electric cooperatives, municipal utilities, and tribal utilities. Cross-referencing counties served (according to each utility's annual report) with census data shows that the average per-capita income for these counties was less than $40,000 in 2014—compared to a national average of $46,000. Also according the utilities' annual reports, most had a line density of less than 12 customers per mile and a peak load of less than 190 MW. Their median annual revenue was less than $30 million according to information provided in the interviews. Collectively, their service areas included regions often hit by ice storms, desert areas subject to damaging microbursts of straight-line winds, and states that are hit by more than 45 tornadoes per year on average [1].

Because of their limited budgets and formidable challenges, small utilities tend to be under-resourced relative to larger utilities. At the same time, note that small utilities (as defined by the number of employees and meters) are actually very big when considering the total service areas. The map in Figure 1 shows the service areas of the 840 distribution cooperatives in the United States. The shaded area of the map covers three-quarters of the nation's landmass. The average electric co-op on this map operates only 13,000 meters [2]; however, collectively, electric cooperatives own and maintain 2.5 million miles of distribution lines (42% of all U.S.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

distribution lines) [3]. If municipal and tribal utilities were added to the map, the coverage would be even greater.

Therefore, the individual footprints of these utilities may be small, but in aggregate they cover more than 75% of the nation's landmass [3]. For this reason, strides in reliability, resilience, and cybersecurity on a national scale cannot be achieved without addressing the needs of small utilities in these areas. This requires, among other things, a new and deeper understanding of the challenges faced by small utilities.

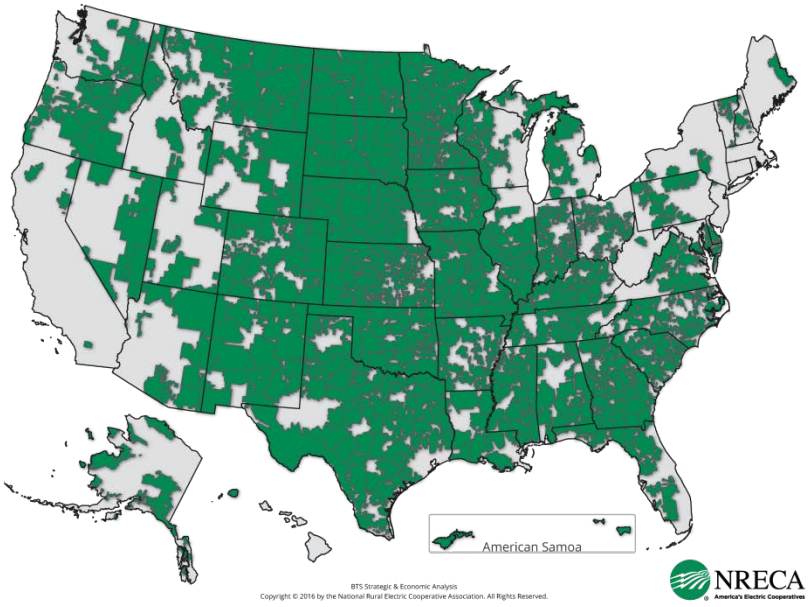

Figure 1. Footprint of cooperative utilities throughout the United States. ***Image from the National Rural Electric Cooperative Association (2016)***

1.2 Reliability, Resilience, and Cybersecurity

Small utilities enable the economies of hundreds of small towns, farming communities, and tribal nations covering a large swath of the United States. Small utilities also power hundreds of manufacturing facilities, dozens of military bases, and most of U.S. agriculture—facilities vital to national productivity and defense. Without the services provided by these small utilities, the citizens in these areas could not participate in the 21st century economy. Consequently, it is in the national interest to ensure reliable, resilient, and cybersecure electric service to these areas.

As in urban areas of the country, consumers in rural areas are increasingly demanding improvements in service reliability, and they want assurances that their service is resilient to evolving threats and is also cybersecure; however, because of their constrained resources, the utilities serving these areas may have challenges meeting these goals. This guide discusses how small utilities face challenges and expectations for maintaining service and protecting their systems through reliability, resilience, and cybersecurity.

As a starting point, this guide defines these three topic areas as follows:

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

- Reliability: the ability of the grid to resist interruptions
- Resilience: the ability of the grid to respond to and recover from disruptions, minimizing their magnitude and duration
- Cybersecurity: the ability of the grid to resist, respond to, and adapt to attacks on its computer systems.

Linking these three areas together is an emphasis on maintaining electricity service to customers. In many cases, reliability and resilience are both advanced by automation; however, this automation may also introduce cybersecurity vulnerabilities. For instance, sensors and remote switching enable system operators to detect and respond to events that could lead to outages, and auto-sectionalizing equipment can be used to isolate faults and restore power as quickly as possible to as many customers as possible, thus advancing resilience; however, these same devices may introduce new cybersecurity vulnerabilities into the grid. For example, as automation and interconnectedness increase, so might the opportunities for cyber attacks that could disrupt service.

So although reliability, resilience, and cybersecurity may seem to be independent areas of study, they actually have common ground. Ensuring electric service to customers requires balancing risk-management efforts to ensure reliable, resilient, and cybersecure electric systems.

1.3 Methodology

In developing this document, the National Renewable Energy Laboratory (NREL) began by conducting a series of interviews to assess the state of reliability, resilience, and cybersecurity at smaller utilities. The utilities selected for interviews represent a wide geographic range throughout the United States and include municipal utilities, electric co-ops, and tribal utilities. The objective of the interviews was to identify aspects of reliability, resilience, and cybersecurity that smaller utilities are already addressing well and aspects where significant challenges remain. NREL interviewed six utilities in our target group—specifically, utilities that are not required to comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) plan. Because of the relatively small sample size, observations from these interviews should be considered illustrative and not representative of the broader population of small utilities.

Each interview session was embedded in a half-day discussion between the utility and NREL about reliability, resilience, and cybersecurity. A set of discussion questions served as a springboard to engage utility staff on a wide range of related topics—exploring challenges resulting from utility size, customer profiles, climate, governance model, and other factors. These extended discussions proved at least as informative as the structured data that were gathered.

When possible, NREL conducted two interview sessions at each utility, with different utility employees in each session. This approach provided an interesting glimpse into how reliability, resilience, and cybersecurity efforts were perceived by different groups within the utility. Finally, NREL also engaged in informal discussions with other small utilities that did not go through the interview process but expressed interest in the work (including some that attended NREL's workshop on "Security and Resilience of Grid Integration with Distributed Energy

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Resources," which was held July 13–14, 2016). These discussions helped to stress-test the insights gleaned from the interviews.

Reliability and resilience questions for the interview were composed by NREL, and cybersecurity questions were supplied by a tool called the Cybergovernance Maturity Oversight Model (CMOM), produced by a company called Cybernance. The CMOM question set combines elements from both the U.S. Department of Energy's (DOE's) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. CMOM includes a proprietary algorithm that ranks unimplemented security controls according to potential impact (how much damage could result by not addressing the control) and centrality (interaction and dependence with other controls). This CMOM ranking of individual utility controls also proved useful in creating this guide.

Several excellent resources already exist on reliability, resilience, and cybersecurity (see the section on "Prior Work" below); however, our interviews indicated that these standards, guides, and industry references often seem to be left on the library shelf. Rather than create a new stand-alone guide, the approach in this guide is to identify challenges common to small utilities and show ways that existing documents can be applied to address these challenges. Small utilities may find it useful to take what they need from a number of these resources and decide for themselves which ones to pursue in more detail.

1.4 Prior Work

A literature review on guidance in reliability, resilience, and cybersecurity for utilities of any size revealed considerable useful material; a list of references and resources is presented in the bibliography. However, narrowing the scope to guidance that is specific to small utilities produced a much shorter list.

- The National Rural Electric Cooperative Association (NRECA) produced a *Guide to Developing Cyber Security and Risk Mitigation Plan*.[4] This document was created for the 840 distribution cooperatives that form the bulk of NRECA's membership (average number of meters: 13,000). The NRECA guide provides an important concept—*continuous improvement*—that informed Section 3 of this guide.

- The Kentucky Association of Electric Cooperatives (KAEC) created the *KAEC Cyber Security Policy Framework*, which supplies a set of policy templates that a utility can implement.[5] During this project, NREL discussed with the KAEC members their motivations and methodology for producing this framework; that information is captured in the sidebar in Section 4. KAEC members' perspectives also provided valuable input to the conclusions of this guide (Section 6).

- The North Carolina Electric Membership Corporation, the power supplier to many of North Carolina's 26 local distribution electric cooperatives, created a set of cybersecurity principles that its members can apply to help guide their cybersecurity efforts. The principles are high level and provide a framework from which member cooperatives can work as they develop and implement principles that fit locally.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

- The Northwest Public Power Association plans to publish a *Cybersecurity Guide for Members of the Northwest Public Power Association* in 2017. Topics include information sharing, risk management, training, and physical security of cyber assets. The guide will be available only to Northwest Public Power Association members (consumer-owned public/people's utility districts, electric cooperatives, municipalities, and Crown corporations in the western states and Canada).

A literature search for the challenges facing small and under-resourced utilities revealed no prior research available to the public. NREL's research represents an initial foray into this area.

1.5 Specificity of Challenges to Small Utilities

This guide is based on insights and data gleaned though interviews and discussions with small utilities. These discussions led to the compilation of the challenges identified in Section 2 and discussed throughout. They are not necessarily unique to small utilities. Any utility may experience issues involving governance, risk management, and other areas identified in Section 2, so there is some commonality among the challenges faced by utilities both large and small.

However, the interviews suggested that the challenges listed below appear frequently at smaller utilities. Figure 2 helps visualize this point by plotting the overall CMOM score (a rating of cybersecurity maturity) compared to the annual information technology (IT) budget (a measure of resource availability) of five of the interviewed utilities. (The sixth utility did not supply IT budget data.)

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

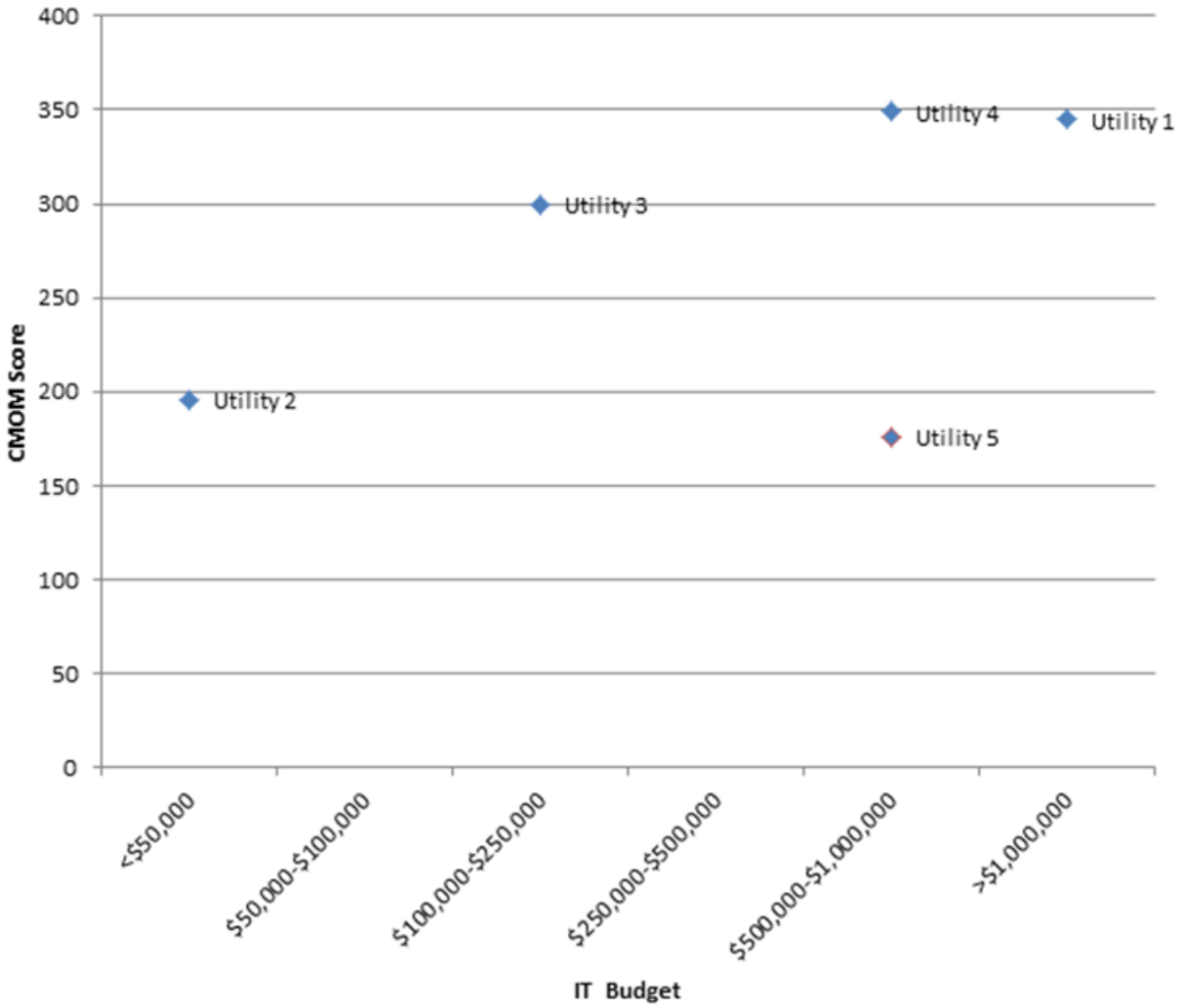

Figure 2. CMOM score compared to annual IT budget for five interviewed utilities

The graph suggests an association between low CMOM scores (low cybersecurity maturity) and low IT budgets; however, this is not a hard-and-fast rule. For example, Utility 5 spends between $500,000 and $1,000,000 on IT, yet it has the lowest CMOM score of the group. This information suggests that a utility that spends less on IT is more likely to have a low level of cybersecurity maturity, but also that low cybersecurity maturity is not limited to utilities that have low IT budgets.

Likewise, small utilities are likely to face the challenges listed in Section 2, even if those challenges are not unique to small utilities. Section 2 explores possible reasons why these challenges may show up consistently at small utilities.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

2 Challenges

The development of a strategy to improve utility reliability, resilience, and cybersecurity can be considered in three stages: planning, executing, and assessing. The basic implementation model is shown in Figure 3; however, as basic as it is, this implementation model faces challenges at every stage. This section seeks to explore those challenges and, when possible, map them to the organizational processes that underlie the challenges.

Real progress toward improvements in reliability, resilience, and cybersecurity depends on the participation of the entire utility organization. The implementation model in Figure 3 (a variation of the Plan, Do, Check, Act cycle created by W. Edward Deming in the 1950s [6]) summarizes the following process: a governing body (or board of directors) sets strategic goals and priorities for the organization; an executive-level staff member allocates resources for projects aligned with these strategic goals and priorities; a staff member works to execute the approved projects; and some metrics are used to measure the success of the effort. These measures of success are then reported back to the board and become inputs for discussions on future strategic goals and priorities.

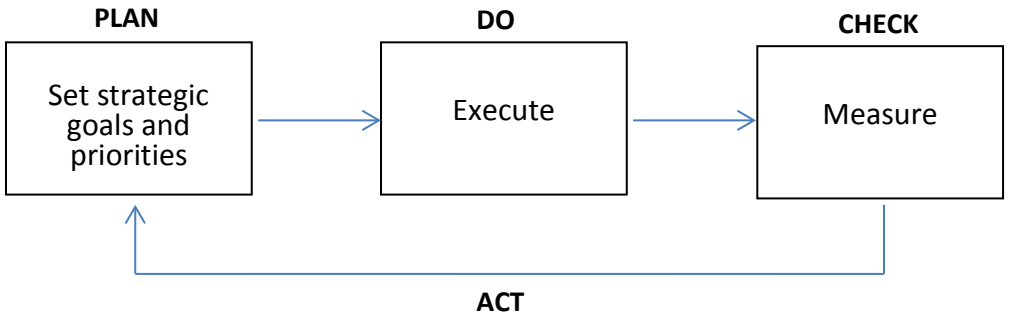

Figure 3. Organization-level implementation model

However, this basic model can break down if all of the elements needed to support the phases of this cycle are not in place. During the course of this work, NREL identified a number of challenges to the simple organization-level implementation model. These challenges include issues with the following: scalability of existing guidance; governance; risk management; asset, change, and configuration management; time management; metrics; cost recovery; labor pool; technology information; siloed information; and undocumented processes. Figure 4 maps the challenges that were uncovered during the discussions with small utilities onto the segments of the organization-level implementation model.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

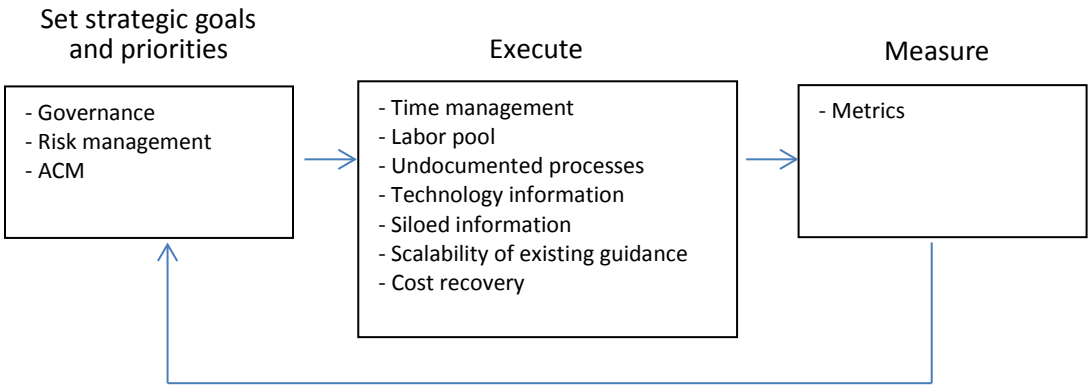

Figure 4. Challenges faced by the small utilities that were interviewed mapped to the organizational-level implementation model for improvement

The remainder of this section explores these challenges and discusses why small utilities may struggle to follow this model.

2.1 Scalability of Existing Guidance Documents

Many guides, standards, and other documents exist that are meant to address reliability, resilience, and cybersecurity. Unfortunately, in the discussions with small utilities, NREL identified cases where such resources were "left on the library shelf." The reason for this situation seems to be encapsulated in a statement made by a small utility (paraphrased):

> The guides assume you already have a large staff and a high level of knowledge in the area addressed. For a small staff, they can be overwhelming. Something smaller would be useful.

In addition, some concepts in the various guides may not scale well to very small utilities. For instance, one concept from DOE's ES-C2M2 is "role-based access." The idea is that access to various digital data or systems should be assigned by role. There might be a role that covers the human resources staff, another for the engineering staff, and another for the administrative staff. The challenge is that the concept of role-based access breaks down when, as at many small utilities, these component roles are filled by one person and that person actually performs many roles. For instance, many small co-ops have a one-person IT department, and sometimes that person has other responsibilities.

Because the controls in many guides and standards may not scale down well, small utilities may feel that these documents were not written for them. Rather than use available guides and standards, small utilities tend to address reliability, resilience, and cybersecurity on the basis of individual projects. For example, someone within the organization may become interested in a particular tool or system upgrade and become a champion for that work. A project-level approach can lead to a patchwork of technologies that do not work well together.

The systemic view offered by guides and standards can help avoid this pitfall. Unfortunately, due to their complexity and the volume of information, whatever benefits that could be derived from existing guides and standards can go largely unrealized by small utilities.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

2.2 Governance

> "The first, most important step [in addressing security and resilience] is to educate and convince the board."—IT manager of a small electric co-op

Small utilities are less likely to have boards of directors (or equivalent governing bodies) with experience in the electrical sector. Relative to a large utility, board members are more likely to be elected or appointed from the customer service area and may include farmers, small business owners, or retirees. These boards may have a passion for serving their community, but they may not necessarily have knowledge of the technical issues around reliability, resilience, and cybersecurity.

In such cases, the board naturally looks to the staff for technical guidance. This can lead to a problem in that staff may tend to think in terms of individual projects (for instance, deploying advanced metering infrastructure or supervisory control and data acquisition) rather than on strategic goals. Strategic thinking is the domain of the board, but if they are addressing challenges on the basis of individual projects, they may not see the big picture or be prepared to assess organization-wide risks.

2.3 Risk Management

Reliability has existed as an area of study since the grid was invented more than 100 years ago, and risk management in this area generally shows more maturity than in other areas. Many risk-management activities that apply to reliability are recognized as traditional utility activities—for instance, vegetation management and placing animal guards.

However, risk management for resilience and cybersecurity is another matter. The issue is that although small utilities may think that they are doing risk management at an acceptable level, they may not be doing it in a structured way that reflects best practices for risk management in general and guidance from industry-specific thought leaders (e.g., NIST, Institute of Electrical and Electronics Engineers, DOE). Small-utility efforts can often be ad hoc. To move up the maturity scale, their efforts need to be documented, more structured, and integrated into strategic planning.

2.4 Asset, Change, and Configuration Management

An often-repeated saying in cybersecurity is some variation of the phrase "you cannot protect what you do not know you have." This could be extended to "you cannot protect what you do not have information about." Asset, change, and configuration management (ACM) provides a framework for recording asset data such as age and condition of equipment, valuation, location, and maintenance records. Knowing such information is vital not only to cybersecurity efforts but also to reliability and resilience.

Cybersecurity data related to asset management gathered from the small-utility interviews were interesting and somewhat paradoxical. On one hand, small utilities are doing much in the area of asset management—it was the second-highest score in the cybersecurity (CMOM-based) assessment. On the other hand, aspects of asset management figured high on the prioritized list of areas that needed to be addressed for cybersecurity.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

ACM is a foundational element in building out efforts in program management, risk management, and many other areas. This centrality makes it deserving of more attention, even if utilities are already investing effort in it.

2.5 Time Management

"Everything is a priority." This statement, or some variation on the theme, was repeated in many of the small-utility interviews. Although it is not surprising to hear this comment in a small organization of any sort, it does have implications for reliability, resilience, and cybersecurity.

Organization-wide improvements in these areas require steady effort across a number of domains. If staff time is focused on responding to day-to-day needs, such effort may not be done. This speaks to the need for setting priorities organization-wide and for allocating adequate funds and staff time for reliability, resilience, and cybersecurity.

Small utilities also have a time management problem arising from the total number of projects underway at any given time. Large utilities tend to have a number of concurrent projects, resulting in overlapping demands on staff. This creates a more or less consistent level of demand for staff hours. On the other hand, small utilities will have fewer projects, which will be spaced discretely. This creates irregular demand for staff hours—sometimes more hours are needed, sometimes less. Figure 5 illustrates this point, wherein each rectangle represents the time and resources required for a project within a utility's portfolio.

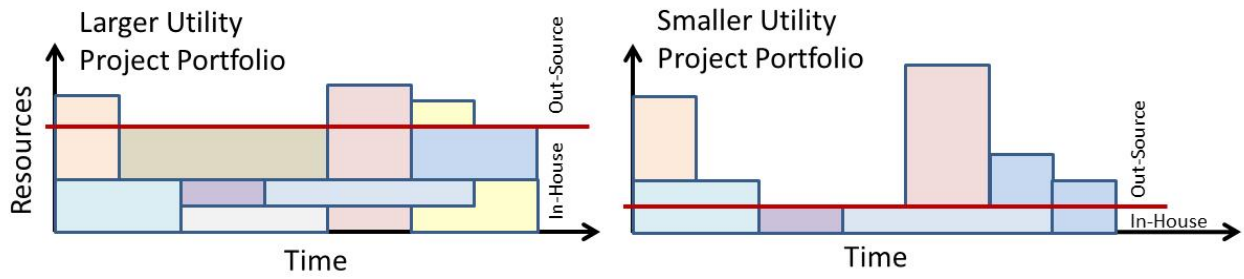

Figure 5. Project portfolios at large and small utilities

Rather than staff up to meet every peak, small utilities often decide to outsource some of their project work. This can create a problem if the utility fails to develop the deepest level of knowledge about its own systems.

2.6 Metrics

The reliability indicator used by all small utilities interviewed is the System Average Interruption Duration Index (SAIDI). This metric was generally reported to the utility board and/or in the utility annual report, and it may be required by a state utility regulator.

SAIDI has the advantage of being relatively simple to calculate and to explain to a nontechnical audience; however, as a picture of system performance, it is incomplete. Further, unfortunately, the utilities interviewed more or less stopped there.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Another common metric, the System Average Interruption Frequency Index (SAIFI), was not used, nor were other indicators that focus on feeder-level measurements and voltages. Such metric gaps make robust reliability tracking and improvement difficult. Without these other measurements, it is difficult to assess what needs to be done to improve reliability.

As revealed by the interviews, the utilities did not use or report any resilience metrics or cybersecurity metrics. This result might be expected because such metrics and measurements are not as mature and well-known as reliability metrics; however, the absence of measurement makes improvement even more challenging.

2.7 Cost Recovery

The interviews indicate that among these small utilities cybersecurity efforts are generally funded out of IT budgets. Sometimes cybersecurity is called out as a separate line item, but sometimes it is not. This means that there is no clear path for investment or cost recovery for new cybersecurity initiatives—no surcharge can be added for a cybersecurity project if the project is not budgeted separately. In larger utilities, the necessity of NERC CIP compliance serves as a driver for cybersecurity investment. No similar distribution-level regulatory requirement around cybersecurity exists to drive improvements and cost recovery for most small utilities. (NERC reliability standards do not apply to lower-voltage lines such as those typical of a local distribution system [7].)

2.8 Labor Pool

Nationwide, there is a shortage of employees skilled in cybersecurity [8]. The shortage is even more pronounced for employees that have both cybersecurity skills and knowledge of the electric sector [9]. In addition to these challenges, often small utilities cannot pay the level of salaries that would entice in-demand workers to relocate from an urban area.

Another labor-related challenge is illustrated by one interviewed utility wherein fully two-thirds of all employees are of retirement age (55 or older). This utility faces a serious “brain drain” as those employees begin to retire. In addition to the challenges discussed above, how does an organization cope with that kind of talent loss? How does it capture that much institutional knowledge? Small towns and rural communities have a tough time luring young people, and this has consequences for the utilities that serve them. Small utilities will likely face challenges with workforce recruitment and development in the years ahead.

To their credit, small utilities have shown pluck in doing more with less. An employee of the same utility mentioned above noted that its customer base had tripled in the 38 years that she had been employed there, whereas staff size had remained the same. Her observation was that technology has helped considerably in this regard; however, there will always be a minimum staffing requirement to operate a utility, no matter how much automation it adopts.

The same challenges apply to the engineering staff, which is responsible for reliability and resilience efforts. As the average age of employees increases, these challenges will continue to increase.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

2.9 Technology Information

Gathering accurate, unbiased information on technology that can improve reliability, resilience, and cybersecurity can be challenging. All utilities face challenges around assessing the potential severity of threats and vulnerabilities, identifying requirements, and assessing the suitability of solutions. As the information gathered through interviews shows, small, understaffed organizations often outsource many functions, making them dependent on vendors for technical expertise. Because these vendors have a vested interest in promoting their own products, utilities that follow this policy can be overbuilt in domains for which vendors supply products and underbuilt in other domains. This is also supported by research results presented in the National Association of Regulatory Utility Commissioners (NARUC) report on *Cyber Security Risk Assessment & Risk Mitigation Plan Review for the Kentucky Public Service Commission* [10].

2.10 Siloed Information

Part of the interview process was to ask the same cybersecurity questions of different departments within a utility. The responses showed that at some of the small utilities departments disagreed about what was being done in cybersecurity. This indicates that small utilities may have an issue with internal communications, resulting in data and information remaining in silos across the organization.

Figure 6 provides an example of siloed information—or lack of inter-departmental communications—from one of the utilities interviewed for this project. In this case, the green and brown columns represent the count of implemented (green) or unimplemented (brown) security controls among several dimensions of the CMOM model. In this case, there are differences between two departments at the same utility (anonymized as "DEPT A" and "DEPT B") regarding their implementation and adherence to the CMOM metrics. Both departments agree that the strongest domain is IAM (Identity and Access Management)—note the mostly green bars. Nevertheless, the difference in IAM data given by DEPT A and DEPT B represents communication challenges among departments and the siloing of information. In a more integrated environment, a common understanding of knowledge and perception of policies and procedures would exist.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

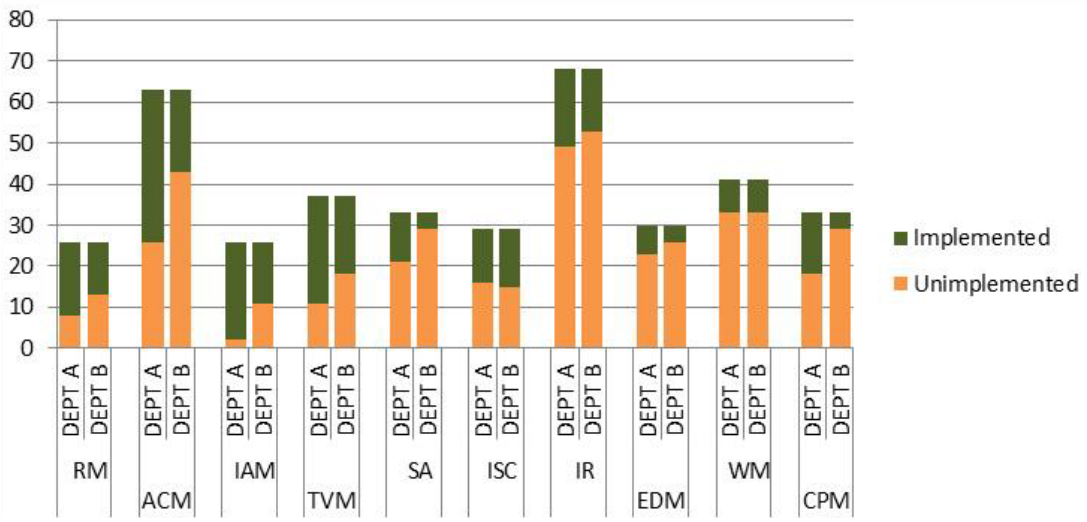

Figure 6. Illustration of siloed information and communication challenges.

In this case, two departments at the same utility (anonymized as "DEPT A" and "DEPT B") have a different perspectives on their cybersecurity implementation practices.

2.11 Undocumented Processes

Many of the utilities interviewed would have had much higher scores had they documented the processes that they perform to support reliability, resilience, and cybersecurity. The work of documentation is generally considered to be an important milestone on the road to maturity in any domain. Among the utilities interviewed, there is a lack of perceived value in documentation, and demands on staff time do not make this practical.

Documentation is a form of communication that allows employees to share knowledge among individuals and departments as it evolves over time. The value of documentation may not necessarily occur to small utilities. The following are benefits of moving processes from employee's heads to the page:

- Retain knowledge. Small-utility employees may have their own excellent processes for getting things done, but what happens if they should leave the company suddenly and unexpectedly?
- Make improvements. The assessment results pointed generally to "inadequate resources" across the breadth of cybersecurity domains. By documenting business processes, small utilities can have a basis for analyzing performance and making improvements.
- Manage the business. To communicate technical and performance requirements, documentation is especially important for those functions that small utilities contract out.

2.12 Summary

Having examined the challenges listed above and referring back to Figure 4, it is clear that three small-utility challenges are essential for strategic goal-setting and prioritization: governance, risk management, and ACM. Governance refers to (among other things) the proper role and function

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

of the board of directors or other governing body. As discussed above, small utilities can fall into the trap of making decisions on a project-level basis rather than executing strategic goals and priorities with a full understanding of risk management.

However, risk management in an asset-intensive industry requires information on the assets of the organization—in other words, an inventory. This is the domain of ACM. Figure 7 shows the dependencies among the three.

Figure 7. Dependencies for the development of strategic goals and priorities

This point was well illustrated during one of the utility interviews for this project. The utility interviewed was in the process of installing a new IT firewall. This firewall—which, among other functions, protected sensitive customer information—had not been replaced in *10 years*. Of course, during that time, threats and defensive technologies have advanced considerably, making a 10-year-old firewall seriously out of date, even if the utility has kept up with software updates.

Had the utility been doing better ACM, it would have identified updating this critical security component as a high risk-management priority. This would have been input to the board's decision-making process (governance), and, presumably, the board would have made it a priority to secure customer information. Timely firewall replacement would have been a project executed to support this priority.

Without ACM, risk management, and governance, small utilities will find it difficult to get off the starting block in terms of improving reliability, resilience, and cybersecurity. For this reason, this guide will next look at how to use existing guides to address these three challenges and how these guides can be scaled for small utilities.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

3 Applying Reliability, Resilience, and Cybersecurity,

3.1 Scaling Available Guidance

Many guides available to small utilities seek to address reliability, resilience, and cybersecurity. Many are also meticulously researched, well written, and rich in information. Appendix A lists some, including:

- For reliability, IEEE 1366: "Guide for Electric Power Distribution Reliability Indices"
- For resilience, ANSI/ASIS SPC.1-2009: "Organizational Resilience: Security, Preparedness, and Continuity Management Systems"
- For cybersecurity, DOE's "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)"

However, a common refrain from small utilities is that guidance documents are too large and overwhelming. The challenge is to scale these materials to the needs of small and under-resourced utilities. Two concepts can help address this: *tailoring* and *phasing*.

3.1.1 Tailoring

A small utility does not need to implement a guide or standard in toto to derive benefit from it. The utility can instead consider how to tailor the guide to its own risk-mitigation needs. In a sense, this can be treated similarly to the decision a utility makes about cyber risks when using ES-C2M2—which enables a utility to either mitigate, accept, tolerate, or transfer risks. This approach enables a utility to constrain the scope of its effort.

When tailoring on a document level, it may be helpful to identify which of the proffered controls should be *applied*, *adapted*, or *disregarded*.

For instance, one concept put forward in ES-C2M2 is that of role-based access—enabling access to resources based on predefined roles within the company. But consider a small utility that has an IT staff of one person. Does role-based access make sense if only one person is in that role?

A small utility could choose to disregard this control because there is no difference between the role and the individual. On the other hand, the process of defining roles (even for a group of one person) can be useful in defining job responsibilities, which can help with business continuity. If that one person leaves the organization suddenly, having defined his or her role can advance the process of locating a suitable replacement. So a small utility may elect to adapt this control, enforcing role-based access with an eye toward business continuity.

To accept and disregard is fairly self-explanatory; however, a utility should consider listing the rationales for disregarding any controls and revisiting that list periodically. As business drivers and technology evolve, there may be a need to either adapt or apply these controls.

3.1.2 Phasing

Phasing is the idea that the individual steps for improving reliability, resilience, and cybersecurity can be spread over time in order to accommodate the constrained resources of a

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

small utility. Staff members are encouraged to group steps found in guidance documents into discrete phases that result in progress toward the strategic improvement goals and a sense of institutional momentum. Getting there all at once may be impractical, but spreading the effort over a specific time period in a structured way can make the work manageable. Phasing allows strategic efforts to find a place in budgets of any size.

The idea of phasing is influenced by *continuous improvement*, a concept that is highlighted in NRECA's *Guide to Developing a Cyber Security and Risk Mitigation Plan* [11]. That document recommends conducting a self-evaluation (described in the NRECA guide) and then doing so again at specified periods (for instance, annually) to measure progress in cybersecurity. But some utilities report that the effort required to perform the self-evaluation once is burdensome and difficult to justify when placed against competing demands for staff time and attention. These utilities might use *phasing* to reach a maturity level where such an ongoing effort is recognized as valuable.

3.2 Practical Examples

The following section of this document identifies three challenges that small utilities face regarding strategic goal-setting and prioritization: governance, risk management, and ACM. These three challenges are used as examples to show how existing guidance documents can be scaled down and applied. For each challenge, a guidance document from Appendix A was chosen and applied to a small-utility perspective using *tailoring* and *phasing*.

The example challenges will be presented in the format shown in the table below.

Table 1. Format for example challenges

Example Guidance	A relevant document from Appendix A
Tailoring	Discussion of how controls from the document could be applied, adapted, or disregarded
Phasing	Discussion of how efforts could be divided into discrete phases that fit the budget and staff resources available

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

3.2.1 Governance

The challenge around governance is to establish an organization-wide approach to reliability, resilience, and cybersecurity. The board needs to be informed by staff's technical expertise but not driven by a project-centric view of progress. The proper role of the board is to set strategic goals, which are then supported by projects that are executed by staff. (This idea is supported by William W. Wommack in "The Board's Most Important Function" [12].)

The following example shows how tailoring and phasing can be used to scale existing governance guidance to the needs of a small utility.

Table 2. Example approach to addressing governance challenges

Example Guidance	*Cyber-Risk Oversight* [13], published by the National Association of Corporate Directors. As the name implies, this document focuses on cyber risk and the role of oversight bodies including the board of directors in managing that risk. It lays out a number of core principles, including the following example (quoted here): *Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.* Author's note: This principle works as well with reliability or resilience; therefore, it can be used in all three areas.
Tailoring	Abiding by this principle would imply board-level engagement and access to cybersecurity expertise. Unlike a large utility, a small utility may not have such access on a regular basis, and it may not have any staff members (or a very limited number) working to address cybersecurity risk management; however, experts might be available on an ad hoc basis (for instance, via special invitation or webinar) through industry associations, regional cooperatives, or joint agreements. A small utility could therefore adapt this principle and pursue appropriate implementation to fit its own circumstances.
Phasing	The core principle quoted above is one of five listed in the National Association of Corporate Directors document. The other four could be addressed over time once the board has had adequate access to cybersecurity expertise. For instance, after discussions with experts via webinars, the board might have new insights that would allow it to act on the principles of "approach cybersecurity as an enterprise-wide risk-management issue" and "understand the legal implications of cyber risks."

3.2.2 Risk Management

As stated in the challenges section, interviews with small utilities show that they are already doing some form of risk management but not necessarily in a structured way. An effective way to introduce that structure is for a utility to create a *risk register*.

A risk register is a key part of a structured risk-management program. The document contains information about identified risks, analysis of risk severity, and evaluations of the possible solutions to be applied. Its key function is to provide management, the board, and key stakeholders with significant information on the main risks faced by the organization. The addition of a risk register could be an important step toward formalizing efforts in this area.

Tellingly, when the small utilities interviewed for this project were asked if they had risk registers, their answers were some variation of the question "What's a risk register?" Not only is

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

having a risk register an import tool for managing risk, but the process of creating a risk register forces thinking and discussions about risk on an organization-wide scale.

The following example shows how tailoring and phasing can be used to scale existing guidance on developing a risk register to the needs of a small utility.

Table 3. Example approach to addressing risk management challenges

Example Guidance	*The Basic Principles of Compiling a Risk Register for Smaller Companies* [14], published by the Association of Chartered Certified Accountants (ACCA). This document provides a step-by-step guide for a small organization to develop its first risk register. The ACCA document suggests that an initial risk register should be compiled by a senior staff member, possibly a financial director or company accountant. The document should then be used as the basis for a brainstorming session to identify gaps and discuss existing risk-mitigation controls. The next step is to formally quantify risk tolerance, likelihoods, and materiality. The risks are then rated and scored, before assigning organizational responsibility for monitoring individual risks over time.
Tailoring	ACCA created this document with small organizations in mind; however, the challenge is that the document is not specific to the utility space. Also, it envisions a process requiring the involvement of a sizable team. A small utility would want to ensure that it accomplishes all of the core objectives required within the ACCA document, including producing the initial list, brainstorming and vetting the list, quantifying risks, prioritizing the identified risks, and assigning long-term responsibilities; however, in a small-utility setting, many of these tasks may be completed by an individual or small team of individuals.
Phasing	The ACCA document provides guidance for developing an organization's first risk register, and it does so in a way that fits within the scope of any size organization. It does not set a time line for these steps—a utility can address them on its own timescale. For the risk register to be useful over the long term, it must be a living document—one that is discussed at the board level; used to provide input into decision-making regarding projects to improve reliability, resilience, and cybersecurity; and refreshed on a periodic basis. As the utility becomes more comfortable with the form and use of the risk register, it can serve as the basis for ongoing improvements in risk management.

3.2.3 Asset, Change, and Configuration Management (ACM)

In the interview discussions among the small utilities in this study, reliability questions related to "traditional" assets indicated a mature practice and application of asset management. Yet, as stated in the challenges section, the small utilities' assessment results showed that aspects of IT asset management figured high on the prioritized list of areas that needed to be addressed for cybersecurity.

The utilities interviewed are already managing their traditional assets well, which implies that the value and the high-level processes are already understood. Given the detailed recommendations ("controls") resulting from the cybersecurity assessment, knowing where and how to begin—with an IT inventory—may be an important first step in this area.

The following example shows how tailoring and phasing can be used to scale existing ACM guidance to the needs of a small utility.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Table 4. Example approach to addressing ACM challenges

Example Guidance	"IT Asset Management: A Best Practice Guide for IT Asset Management" [15], published by Hewlett-Packard (HP). This document contains very helpful information for IT asset management and provides contrasts for how IT asset management differs from traditional asset management. The main tasks within the HP management guide involve answering the questions "What do you have?" and "Where is it?"This inventory discovery process is broadly classified as physical and automated. Preliminary steps include inspections of available records and reconciling those records to the actual equipment and staff on hand. The inventory discovery process should develop and then retain all relevant asset information. Tracking the physical, financial, and contractual information about assets are key elements of an IT asset-management inventory.
Tailoring	HP developed this document for chief information officers struggling to answer basic questions around their asset inventory (e.g., What do you have? Where is it? How well is it working? How much is it costing?). The initial steps for IT asset management as described in the HP reference are to conduct a physical inventory and to incorporate procurement and staff records. This step is of critical importance for performing asset management, yet a small utility may be challenged by the lack of available records to support an inventory. In such cases, a small utility could emphasize the physical inventory of its systems while leveraging the exercise as an opportunity to review records policies.
Phasing	For an IT inventory to be useful over the long term, it must be a living document. As the HP white paper suggests, an IT inventory relates to multiple business systems, including procurement, staff records, and accounting. Although a small utility may begin with a physical inventory and one or more of the network discovery techniques, long-term improvement may be gained by identifying bits of inventory-like activities taking place in other departments. Communicating the value of this information to the other staff members and developing ways to consolidate it can serve as the basis for ongoing improvements in IT inventory.

As stated above, small utilities can turn to many existing documents for guidance on cybersecurity, resilience, and reliability; however, there are no one-size-fits-all solutions, and these examples indicate how utilities could leverage existing materials to their needs through *tailoring* and *phasing* approaches. Despite this wealth of existing guidance, more could be done. The next section looks at a number of ways in which the federal government could contribute, many of which build on existing efforts.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

4 Federal Support for Improvement Efforts

The federal government has a long-recognized role in improving the reliability, resilience, and security of the electric grid; however, much of its work has focused on generation and transmission facilities. To take an example from the cybersecurity realm, NERC CIP requirements apply primarily to generation and transmission; however, Version 5 of the requirements, which went into effect in July 2016, includes more requirements for distribution facilities in its "low-impact" category. This approach to cybersecurity made sense at one time—generation and transmission facilities were the first to become automated, and thus they were the first to have cyber vulnerabilities. But the situation today looks very different. As distribution utilities become more automated, the potential for the disruption of service resulting from a distribution-based cyber attack becomes more serious.

Recall that in Figure 1, the bulk of the U.S. landmass is covered by electrical co-ops. In small municipal utilities and tribal utilities, it becomes clear that securing small utilities means securing the power source for hundreds of manufacturing facilities, dozens of military bases, and most of U.S. agriculture. For that reason, reliability, resilience, and cybersecurity at small utilities is vital to national well-being. The federal government naturally has a role in this.

A number of opportunities exist where the federal government could become more active in these areas. Below are some examples.

4.1 Further Develop the NIST Cybersecurity Framework

In February 2016, the President's *Cybersecurity National Action Plan* directed the NIST to work with stakeholders to inform further development of its *Cybersecurity Framework*, and this work is ongoing. It would be helpful if this process could include input from small, under-sourced utilities to broaden the application of the Framework and make it more useable for this subset of need.

4.2 Guide the ES-C2M2

Periodically, DOE develops and releases articles, podcast, and guidance on the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). It could be helpful to the small-utility sector if these supplemental materials were focused on its understanding and application of the ES-C2M2 model.

4.3 Assist with Vulnerability and Risk Assessments and Emergency Restoration Plans

The U.S. Department of Agriculture's Rural Utilities Service, a loan grantor for co-op and tribal utilities, has recognized the implications of digital threats to resilience. The Rural Utilities Service requires that a borrower complete a vulnerability and risk assessment of its entire business (physical and cybersecurity) to create and maintain an emergency restoration plan [16]. The Rural Utilities Service has issued procedural guidance [17] for borrowers that provides references and general methods related to procedures, as well as key provisions that should be incorporated in developing the emergency restoration plan and vulnerability and risk assessment. Unless small utilities have applied for loans from the Rural Utilities Service, it is unlikely that they are familiar with the high-level guidance in this document. Programmatic

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

technical assistance to potential loan applicants could include support for emergency restoration plans and vulnerability and risk assessment requirements. This technical assistance could be organized and packaged for delivery to regional associations that support small utilities.

4.4 Stand Up a Distribution-Specific ISAC

The North American Reliability Corporation operates the Electricity Information Sharing and Analysis Center in collaboration with DOE and the Electricity Subsector Coordinating Council. The Electricity Information Sharing and Analysis Center offers security services to owner and operator organizations of the bulk power system across North America. Our interviews revealed that some small utilities were familiar with the Multi-State Information Sharing and Analysis Center, which is operated by the nonprofit Center for Internet Security. Although the Multi-State Information Sharing and Analysis Center works with the Department of Homeland Security, the Center is principally focused on state, local, territorial, and tribal government entities. An opportunity may exist for the federal government to stand up an ISAC that is focused on distribution utilities, with a particular focus on companies not under NERC CIP regulation.

4.5 Nurture Grassroots Efforts

Traditionally, guidance documents are "top down"—in other words, they are produced by government, associations, research organizations, or some combination of those with input from a number of utilities. They are then passed to the bulk of the utilities for which they are intended.

Interviews with small utilities show that they perceive these documents to be overwhelming and impractical for organizations of their size—hence, suggestions in Section 3 for "scaling down." However, another approach might be to encourage and support the development of guidance documents by the people who will actually use them.

Kentucky Cooperatives Address Cybersecurity

The Kentucky Association of Electric Cooperatives (KAEC) has put together a unique project to support cybersecurity improvements among its members. The driver was a 2013 report issued by NARUC and funded by DOE that assessed the state of cybersecurity at six Kentucky electric cooperatives. Based on the report, the Kentucky Public Service Commission asked KAEC to take action to improve cybersecurity among its members.

The KAEC utilities sought to work together to remedy the cyber risks that were identified. In the words of one KAEC participant, "there is a lot of guidance out there." According to the group, many of the available guides and references are problematic because they assume a dedicated cybersecurity staff with a high knowledge level.

Seeking guidance better scaled to their members, the KAEC team of utilities decided first to identify a set of cybersecurity policies that could be implemented by even their smallest co-ops. They borrowed ideas from the SANS Technology Institute, NERC CIP, and ISO 27000. Many of the resulting policies are adaptations of policy templates publicly available through SANS. The resulting set of policy templates has been published as the *KAEC Cyber Security Policy Framework* on the website of NRECA.

The next phase of KAEC's efforts focuses on underpinning the policies with controls, developing an audit process, and adding new policies to the framework. The current approach is still all-volunteer, but it could benefit from federal support and encouragement.

At least one such "grassroots" effort is already underway at the Kentucky Association of Electric Cooperatives, where local electric co-ops have collaborated to produce their own cybersecurity framework (see sidebar). In some ways, KAEC's "grassroots" approach to cybersecurity is unprecedented. Utilities in other parts of the country have already made inquiries to KAEC about their program. It remains to be seen how far it could go with the right kind of nurturing.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Assisting grassroots efforts would be a new role for the federal government, but would also encourage more and deeper dialog with small and under-resourced utilities. The assistance might be as basic as capturing and disseminating the process used by a group of utilities that has undertaken such a project. What are the successes and challenges of groups of utilities that have tried a voluntary, collaborative approach? What risks are inherent to this approach and what are their mitigations? What policies are needed to encourage adoption of this collaborative model by utilities in other geographic areas? Although the technical products from such grassroots effort may be made publicly available, the participants' hard-earned experience is not so easy to transfer.

To some extent, looking at efforts in mutual assistance among utilities can shed light on how such grassroots efforts might be nurtured and supported. The next section focuses on mutual assistance as a possible way to advance reliability, resilience, and cybersecurity.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

5 Mutual Assistance

The electric industry, and particularly public power, has a long-held tradition of building resource-sharing relationships. Joint action agencies are formed between public utilities with shared interests in generation or transmission, to provide reliable and competitively priced energy or energy-related services. Early on, distribution cooperatives formed generation and transmission cooperatives to pool their purchasing power for wholesale electricity, and to assure an adequate supply of cost-effective, reliable power. This section explores another collaborative tradition: mutual assistance.

Mutual assistance has long been a pillar of the power industry's resiliency strategy to manage weather impacts that disrupt electric service to their customers. What began as electric power companies informally sharing crews and equipment with their neighboring utilities has evolved into Regional Mutual Assistance Groups. Following Superstorm Sandy in 2012, it became clear that a national framework was needed to most effectively deploy mutual assistance resources during significant regional or national events [18].

The need for structured mutual assistance was also illustrated in 2011, after a tornado outbreak cut through the Southeast. Small distribution utilities across Alabama and Tennessee depended on mutual-assistance agreements to make available crews and equipment and to help restore their systems. Yet, with limited staff, even managing the assistance from others can be a challenge. For that reason, the recovery plan for a small municipal utility in Tennessee now includes roles and resources specifically to direct assistance crews, as opposed to actively helping with recovery. These roles include meter readers, installers, and even retirees—trusted people that know the system.

In some cybersecurity domains, a structure for mutual assistance is evolving. In the areas of information gathering and threat assessment, a great deal of collaboration is already the norm for the power sector, with institutions like the Electricity Information Sharing and Analysis Center convening dialogue among power companies.

However, it is worth noting that robust debate still exists about whether information-sharing efforts are adequate and what can be done to improve them—ranging from a push to increase the number of asset owners and operators with clearances, to broader declassification of threat information. It is possible that market barriers and other forces can impede or disincentivize the idea of mutual assistance and shared defense in the cyber arena.

In 2015, NARUC published a primer on Regional Mutual Assistance [19]. In that report, NARUC determined that "cyber mutual assistance remains essentially unexplored. In short, the utility industry may not have explored this kind of arrangement because it has never needed to."

Ironically, that perspective changed in November 2015 with NERC's industry-wide GridEx III. Conducted biennially, GridEx is a multi-day voluntary exercise that simulates a cyber and physical attack scenario on the bulk electricity system. The 2015 event was the largest geographically distributed grid-security exercise ever staged in the United States. The after-action report by NERC recognized a clear distinction between how the electric sector responds to major storms through mutual assistance and its in-house capability to analyze a cyber attack.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

William Fehrman, president and CEO of MidAmerican Energy Company, wrote that the GridEx III exercise "wreaked havoc on grid operators for weeks" [20]. In response, the Electricity Subsector Coordinating Council established the Cyber Mutual Assistance Task Force, to convene industry experts and develop a cyber mutual-assistance framework that will aid electric power companies in rebuilding and recovering necessary computer systems in the event of a regional or national cyber incident. The Electricity Subsector Coordinating Council serves as the principal liaison between the federal government and the electric-power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The Electricity Subsector Coordinating Council includes utility CEOs and trade association leaders representing all segments of the industry.

This mutual assistance program will build on the industry's traditions to develop resource-sharing relationships. Developing a mutual-assistance framework for cyber threats has its own set of unique challenges. In its primer [19], NARUC acknowledged that "experts … in the States felt that the issues involved with a cyberattack were not comparable to those from a natural disaster..." Indeed, the cyber domain does not honor physical or geographical boundaries, and the skills to respond, remediate, and recover from a widespread cyber incident are different from those applied in the field in traditional mutual assistance.

The question of "mutual assistance in the cyber age" may be worth further exploration to determine whether the same benefits apply when translated from preparedness for a physical hazard to preparedness for a cyber hazard (event), particularly at the smaller-utility level. Although it is important to recognize this effort being led by Edison Electric Institute (EEI), it is relevant to note that this work is limited to the bulk electric system. Small utilities could benefit from this, as well.

The primary mission of maintaining electricity service often requires collaboration. The legacy of generation and transmission co-ops, the formation of joint action agencies, and the traditions of mutual assistance are well-established means of ensuring electric service. But they have not been applied consistently across all three domains of reliability, resilience, and cybersecurity. Distribution utility boards, executives, and associations may wish to explore this topic and stay abreast of the Edison Electric Institute effort. Through asking questions, these thought leaders may catalyze conversations about opportunities. As with traditional mutual assistance, the goal should be to create agreements, drills, training, communications networks, and other instruments that enable shared cybersecurity expertise, restoration capabilities, and network defense in the power sector. Smaller utilities may find the scope of these activities (e.g., drills) to be considerably different from traditional storm recovery because many digital systems and business processes are hosted services (external dependencies).

As demonstrated by KAEC (see sidebar in previous section), mutual-assistance *culture, practices, frameworks,* and *models* may also provide the basis for relief with labor-pool and time-management challenges. Generally, the electric sector fights with other critical industries and the government for the same limited pool of highly skilled cyber experts. This challenge can be particularly difficult at smaller utilities with limited resources to attract and retain high-demand expertise.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

6 Conclusion

6.1 Process

In developing this guide, NREL focused on the needs of small utilities in reliability, resilience, and cybersecurity. A formal data-gathering process was used to collect information in these three areas. This process was supplemented by discussions with the interviewees and with other small utilities that did not go through the interviews but were interested in the work. Through these data-gathering efforts and conversations, NREL identified a list of 11 broad challenges.

These 11 were categorized according to whether they supported setting strategic goals and priorities, executing projects based on the goals and priorities, or measuring effectiveness of those projects. This was presented in Figure 4, and it repeated here in Figure 8.

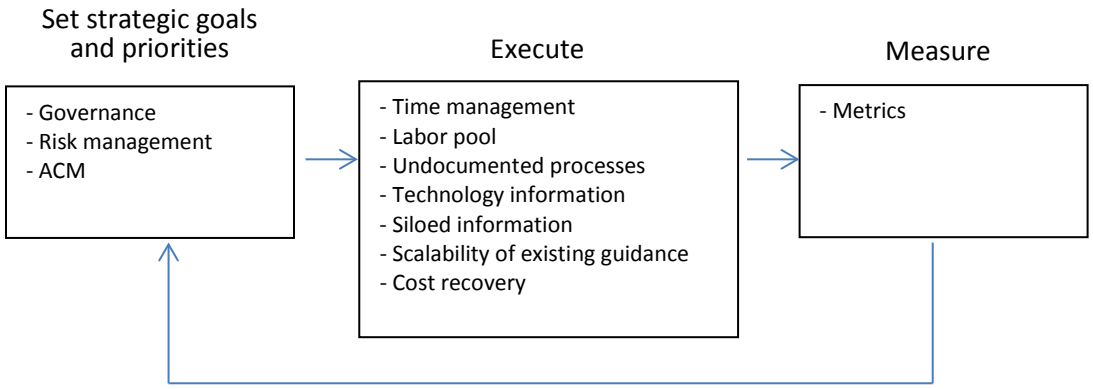

Figure 8. Challenges faced by the small utilities that were interviewed mapped to the organizational-level implementation model for improvement

The challenges that support setting strategic goals and priorities were used as examples for how existing guidance documents can be used, in scaled-down form, to address challenges at even the smallest utility. Two tools were used to scale down guidance documents: *tailoring* and *phasing*.

This guide then considered ways in which the federal government could support improvements to reliability, resilience, and cybersecurity by extending and enhancing its existing efforts. Finally, the guide explored the tradition of mutual assistance and how that tradition might be extended and enhanced in the areas of reliability, resilience, and cybersecurity.

6.2 Observations

Significant observations, based on the interviews, are as follows:

- Small utilities need to improve governance, risk management, and ACM efforts to properly set strategic goals and priorities. Risk management, which sits between ACM and governance, is key. For example, none of the utilities interviewed had developed a risk register.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

- Small utilities are largely unsatisfied with existing guides for reliability, resilience, and cybersecurity. Generally, these guides are unused due to their complexity. Small utilities expressed interest in guides that are scaled to their size and are more prescriptive.

- Small utilities tend not to document their processes for supporting reliability, resilience, and cybersecurity. This makes it difficult for them to retain institutional knowledge and make improvements to processes.

- Small utilities need to push past the sense of being overwhelmed by cybersecurity because this can create a kind of institutional paralysis. It is useful to understand and accept that although no organization can achieve 100% cybersecurity, every organization can avoid complacency and the idea that their current level of cybersecurity is an endpoint. By adjusting existing guidance to fit their needs (*tailoring*) and breaking large efforts into discrete phases (*phasing*), small utilities can find a place in their budgets and schedules to make meaningful improvements to cybersecurity.

- There are some efforts to extend the idea of mutual assistance into the cyber realm, but there are also many unanswered questions around how this could be made effective for small utilities. There seems to be consensus that mutual assistance in this area would take a different form than in more traditional areas (e.g., storm recovery).

6.3 Opportunities

The following opportunities exist for improving support to small utilities:

- Explore new ways for the federal government to nurture grassroots efforts to improve cybersecurity and foster mutual assistance in the cyber realm.

- Provide support for joint action and generation and transmission programs to assist public power entities and cooperatives, respectively, to improve their reliability, resilience, and cybersecurity activities.

- Develop smaller, more prescriptive guides specifically for small utilities.

- Organize regional workshops to "reality test" guidance documents and iteratively improve them.

- Consider a new, distribution-focused Information Sharing and Analysis Center.

- Provide templates and guidance for small utilities to create their own risk registers.

- Provide templates and guidance for small utilities to begin documenting their business processes that support reliability, resilience, and cybersecurity.

6.4 Final Thoughts

The dissatisfaction that small utilities expressed for existing guidance documents begs the question "How have so many documents failed to satisfy the needs of this group?"

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Often, when guidance documents are produced, there is some level of utility feedback in the process. This may take the form of input solicited during the creation of the guide, or there may be a comment period before the guide is finalized. Either of these approaches may be repeated when the guide is updated.

Missing from this is direct input from small utilities themselves. Small utilities may be represented in the process by their service organizations (for instance, small municipal utilities may be represented by the American Public Power Association), but this is not the same as hearing directly from the men and women who must put the guide into practice at a 14,000-electric-meter co-op or a 4,000-meter tribal utility. And often these organizations are too underfunded and understaffed to participate in the guidance-creation process. The final documents often end up better suited to large utilities because they had a voice in their creation.

What would guidance documents look like if small utilities had more input? During this project, small utilities repeatedly requested guidance that was more prescriptive than what is available. They wanted to know what to do first, second, third, and so on. They also requested guides that were more scaled to their needs than what are currently available. When asked for the optimal size for a guide on cybersecurity, one small utility said "three pages."

This may be below the limit of what is actually feasible in terms of scaling downward while still providing useful guidance. Nonetheless, this guide tries to point the way toward more appropriate materials to fulfill that request. But to be effective over time, any guidance document intended for small utilities (including this one) would need to solicit ongoing input directly from the men and women doing the work of reliability, resilience, and cybersecurity. Those who wish to help these utilities need to go to them because often they do not have the resources to participate in the established channels for input. Only by reaching out to ask, "Is this what you really need?" and adjusting guidance documents accordingly can government, research institutions, and nonprofits be sure that they are satisfying the needs of small and under-resourced utilities.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

References

[1] M. Shepherd, "These Are The Most Tornado-Prone Counties In America," *Forbes*. [Online]. Available: http://www.forbes.com/sites/marshallshepherd/2015/10/16/tornado-prone-counties-in-the-united-states/. [Accessed: 28-Dec-2016].

[2] "Co-op Facts & Figures," *NRECA*. [Online]. Available: http://www.nreca.coop/about-electric-cooperatives/co-op-facts-figures/. [Accessed: 23-Aug-2016].

[3] "Interactive Maps," *NRECA*. [Online]. Available: http://www.nreca.coop/about-electric-cooperatives/maps/. [Accessed: 05-Sep-2016].

[4] E. Lebanidze and D. Ramsbrock, "Guide to Developing a Cyber Security and Risk Mitigation Plan," National Rural Electric Cooperative Association, 2014.

[5] S. Gentry *et al.*, "KAEC Cyber Security Policy Framework," Kentucky Association of Electric Cooperatives, 2015.

[6] Paul Arveson, "The Deming Cycle," *Balanced Scorecard Institute*. [Online]. Available: https://balancedscorecard.org/Resources/Articles-White-Papers/The-Deming-Cycle. [Accessed: 24-Aug-2016].

[7] "NERC Frequently Asked Questions," North American Electric Reliability Corporation, Aug. 2013.

[8] S. Morgan, "Market expansion adds to cybersecurity talent shortage," *CSO Online*, 13-Jul-2016. [Online]. Available: http://www.csoonline.com/article/3094683/leadership-management/market-expansion-adds-to-cybersecurity-talent-shortage.html. [Accessed: 30-Dec-2016].

[9] "Building a Cyber Security Workforce for the Energy Sector," Energy Sector Security Consortium, Jun. 2016.

[10] Tim Fawcett and Randall R. Nason, "Cyber Security Risk Assessment & Risk Mitigation Plan Review for the Kentucky Public Service Commission.," National Association of Regulatory Utility Commissioners, DE-OE0000123, Dec. 2013.

[11] "A Guide to Developing a Cyber Security and Risk Mitigation Plan," National Rural Electric Cooperative Association, 2011.

[12] W. W. Wommack, "The Board's Most Important Function," *Harvard Business Review*, 01-Sep-1979. [Online]. Available: https://hbr.org/1979/09/the-boards-most-important-function. [Accessed: 26-Aug-2016].

[13] Larry Clinton, "NACD Cyber-Risk Oversight Executive Summary," National Association of Corporate Directors, 2014.

[14] Tony Morton, "The Basics Principles of Compiling a Risk Register for Smaller Companies," Association of Chartered Certified Accountants, 2010.

[15] "IT asset management: A best practice guide for IT asset management (Business white paper)," Hewlett-Packard Development Company, 2011 2009.

[16] "7 CFR 1730--Electric System Operations and Maintenance; Chapter XVII--RURAL UTILITIES SERVICE, USDA; Regulations of the Department of Agriculture; Code of Federal Regulations."

[17] "Bulletin 1730B-2," United States Department of Agriculture, Rural Utilities Service, Jan. 2005.

[18] "Mutual Assistance Enhancements Following Superstorm Sandy," EEI, Oct. 2013.

[19] Miles Keogh and Sharon Thomas, "Regional Mutual Assistance Groups: A Primer," National Association of Regulatory Utility Commissioners, DE-OE0000578.

[20] William J. Fehrman, "Mutual Assistance in the Cyber Age," *Electr. Perspect.*, Jun. 2016.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

List of Acronyms

ACCA	Association of Chartered Certified Accountants
ACM	Asset, change, and configuration management
ANSI	American National Standards Institute
ASIS	American Society for Industrial Security
CIP	Critical infrastructure protection
CMOM	Cybergovernance Maturity Oversight Model
DOE	U.S. Department of Energy
ES-C2M2	Electric Subsector Cybersecurity Capability Maturity Model
HP	Hewlett-Packard
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information technology
KAEC	Kentucky Association of Electric Cooperatives
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
NREL	National Renewable Energy Laboratory
SANS	SysAdmin, Audit, Network, Security
SPC	(ASIS) Security, Preparedness, and Continuity

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

Appendix A: Resources

Reliability

IEEE 1366 ("Guide for Electric Power Distribution Reliability Indices")

- The guide is used for trending reliability performance, setting the baseline for reliability performance as well as communicating performance to management, key customers, and regulators. The guide identifies useful distribution reliability indices and factors that affect their calculation.

IEEE 1250 ("Guide for Identifying and Improving Voltage Quality in Power Systems")

- The purpose of this guide is to assist power delivery system designers and operators in delivering power with voltage quality that is compatible with electrical end-use equipment. This guide includes discussions of ways to identify and improve voltage quality in power systems, as well as references to publications in this area. This guide includes factors that affect power system performance and mitigation measures that improve power system performance.

National Rural Electric Cooperative Association (NRECA) "Technical Assistance Guide/ Guides for Electric Cooperative Development and Rural Electrification"

- This guide contains a module that sets forth the principles and establishes the recommendations for the electrical design of a rural electrification project or system, including service reliability.

U.S. Energy Information Administration (The 861 reports include distribution reliability indices: SAIDI and SAIFI)

Resilience

ISO 22301:2012 ("Societal security—Business continuity management systems")

- The standard is a generic business continuity management standard that can be used by any organization, or any part of an organization, no matter the size or the purpose.

ANSI/ASIS SPC. 1-2009 ("Organizational Resilience: Security, Preparedness, and Continuity Management Systems")

- The standard provides a framework for businesses to assess the risks of disruptive events; develop a proactive strategy for prevention, response, and recovery; establish performance criteria; and evaluate opportunities for improvement.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

National Fire Protection Association 1600 ("Standard on Disaster/Emergency Management and Business Continuity Programs")

- The standard establishes a set of criteria for all hazards disaster/emergency management and business continuity. It has been adopted by the U.S. Department of Homeland Security as a voluntary consensus standard.

CERT Resilience Management Model, Version 1.2, Carnegie Mellon University, 2016

- The maturity model provides an approach to managing operational risk and resilience management.

National Institute of Standards and Technology (NIST) 800-184 (DRAFT) ("Guide for Cybersecurity Event Recovery")

- This guide contains information for improving cyber event recovery plans, processes, and procedures. It provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.

Cybersecurity

"NACD Cyber-Risk Oversight Executive Summary," National Association of Corporate Directors, 2014.

- This document explains how boards of directors can best participate in the process of improving cybersecurity.

"Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), DOE, 2014.

- ES-C2M2 enables electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity.

"NIST Framework," National Institute of Standards and Technology, 2013.

- This document provides a voluntary framework for reducing cyber risks to critical infrastructure. It aims to be flexible and repeatable while helping asset owners and operators manage cybersecurity risk.

"Guide to Developing a Cyber Security and Risk Mitigation Plan," NRECA, 2011.

- This document was developed specifically for the electric cooperative sector, and it provides a framework for improving cybersecurity focusing on measurable results and continuous improvement.

"National Cybersecurity Workforce Framework," U.S. Department of Homeland Security, 2014.

- The document categorizes and describes cybersecurity work. It establishes a common language to define cybersecurity work.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

NIST 800-34 (“Contingency Planning Guide for Federal Information Systems”)

- The guide provides instructions, recommendations, and considerations for information-system contingency planning. This guide defines a seven-step contingency-planning process that an organization may apply to develop and maintain a viable contingency-planning program for their information systems.

NIST 800-61 (“Computer Security Incident Handling Guide”)

- The guide provides direction for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

NIST 800-150 (DRAFT) (“Guide to Cyber Threat Information Sharing”)

- This publication provides guidelines for establishing and participating in cyber threat information-sharing relationships, establishing information sharing goals, and identifying cyber threat information sources.

NIST 800-92 (“Guide to Computer Security Log Management”)

- The document establishes guidelines and recommendations for securing and managing sensitive log data.

“Cyber Threat Metrics,” Sandia National Labs, SAND2012-2427, 2012.

- This report describes metrics and models for characterizing cyber threats consistently and unambiguously.

ISO/International Electrotechnical Commission 27001 (“Information Security Management”)

- The standard specifies a management system that is intended to bring information security under explicit management control.

NIST 800-128 (“Guide for Security-Focused Configuration Management of Information Systems”)

- The focus of this document is on implementing the information-system security aspects of configuration management.

NIST Interagency Report 7693 (“Specification for Asset Identification”)

- This specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.

NARUC “Cybersecurity for State Regulators”

- Small-utility boards might find this document useful as of way of looking at basic cybersecurity concepts through a regulatory lens.

Risk

“The Basic Principles of Compiling a Risk Register for Smaller Companies,” Association of Chartered Certified Accountants (ACCA), 2010.

- This document walks the reader through basic steps for establishing a risk register for a small organization.

ISO 31000:2009 (“Risk Management—Principles and Guidelines”)

- The standard provides principles, framework, and a process for managing risk that can be used by any organization regardless of its size, activity, or sector. Using the standard can help organizations improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

This report is available at no cost from the National Renewable Energy Laboratory at www.nrel.gov/publications.