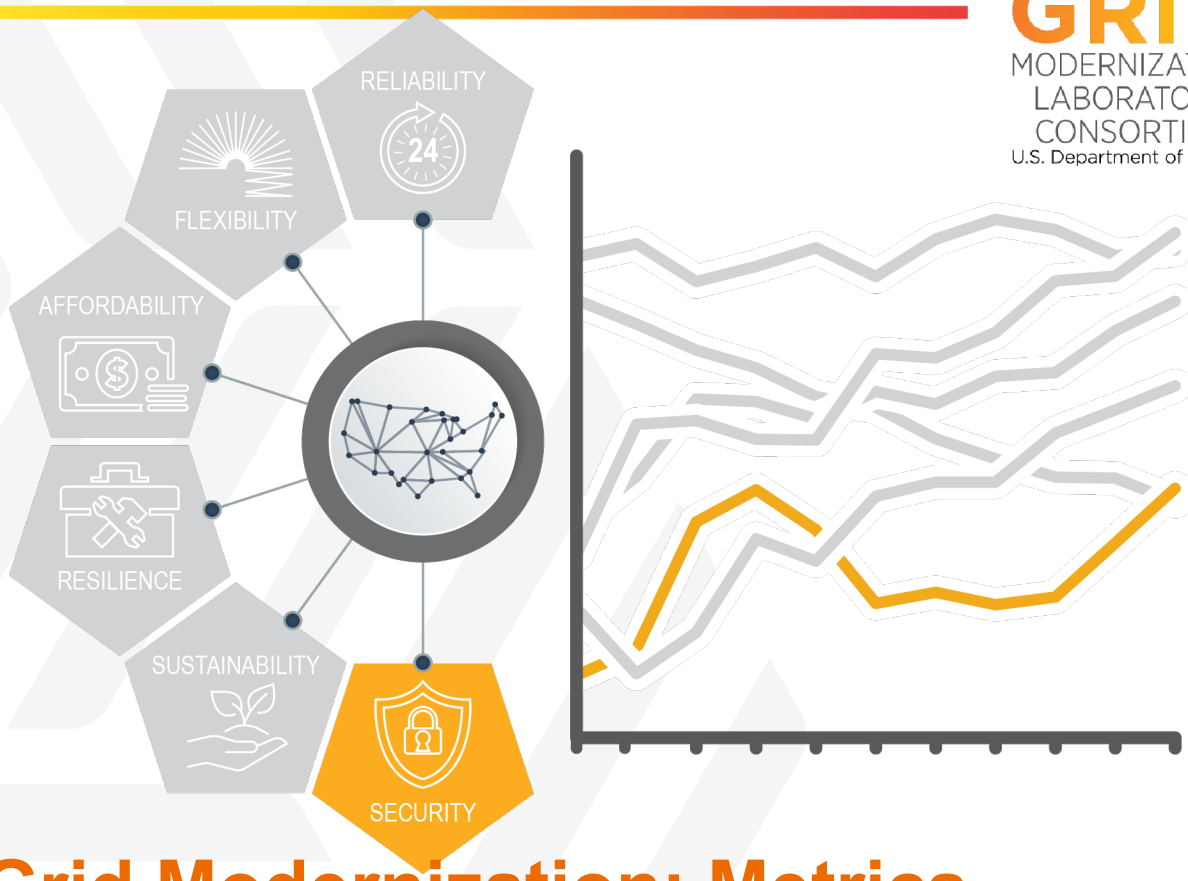

Grid Modernization: Metrics Analysis (GMLC1.1)– Physical Security

Reference Document, Volume 7

April 2020

Grid Modernization Laboratory Consortium

PNNL-28576

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

PNNL-28576

Grid Modernization: Metrics Analysis (GMLC1.1)

Reference Document
Volume 7

Primary Author:
Steven Folga[1]

Grid Modernization Laboratory Consortium Members:
Angeli Tompkins[1] Shabbir Shamsuddin[1]
Jessica Trail[1] Debra Fredrick[1]

PIs: Michael Kintner-Meyer[2] Joseph Eto[3]

April 2020

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

---

[1] Argonne National Laboratory
[2] Pacific Northwest National Laboratory
[3] Lawrence Berkeley National Laboratory

Summary

Lab Team: Steve Folga, Jessica Trail, Debra Fredrick, and Shabbir Shamsuddin, ANL

Security

Presidential Policy Directive 21 defines "security" as "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters."

This project focused on metrics for physical security.

The GMLC Metric Team adapted a Department of Homeland Security developed physical security metric, along with the underlying survey instrument and software system used to calculate and display the metric for application by electric utilities to assess their security posture. The system enables utilities to both assess their current security posture and evaluate the effectiveness of investments to change or modify aspects of their current posture.

S.1. Motivation

Security planning in the electricity sector does not yet possess a long-accepted canon of techniques for measurement and does not yet have established metrics. In other industries, the security community uses metrics, such as annualized loss expectancy (ALE), as a means for justifying budgets for security-related expenditures or actions.[1]

Application of the ALE approach in the electricity sector is difficult because the ALE approach depends on prior quantification of risks (i.e., annualized rates of occurrences); these risks are not yet well-understood, much less quantifiable with precision for the electric sector. For example, there are no actuary tables derived from decades of data collection that can tell us what adversaries will do, how often they will do it, and how much it will cost the electric sector to respond when they do it.

The absence of widely understood and accepted metrics for security is an emerging and national concern. The Congressional Research Service (CRS) recently concluded that the electricity grid's physical safeguards are "a work in progress" and states that there is currently no comprehensive accounting of changes in physical security throughout the sector.[2] It also concluded that security metrics (for both cyber and physical security) have consistently been a challenge due to evolving threats and vulnerabilities. In addition, the CRS emphasized that anecdotal information in the public domain suggests that these threats and vulnerabilities are significant and widespread.

[1] ALE is the monetary loss that can be expected for an asset due to a risk over a 1-year period and is calculated by multiplying the single loss expectancy by the annualized rate of occurrence.

[2] Congressional Research Service (CRS). 2018. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* available at https://fas.org/sgp/crs/homesec/R45135.pdf, accessed on November 15, 2018.

S.2. Outcome/Impact

The GMLC metrics team adapted a physical security metric, developed originally by the Department of Homeland Security, for specific application to and use by electric utilities.[3] The purpose of the Protective Measures Index (PMI) metric is to enable electric utilities, their regulators, and stakeholders to assess the physical security posture or readiness of the utility. The metric has nine constituents and is developed through a systematic process to assign values to the constituents. The PMI structure is shown in Figure S.1.

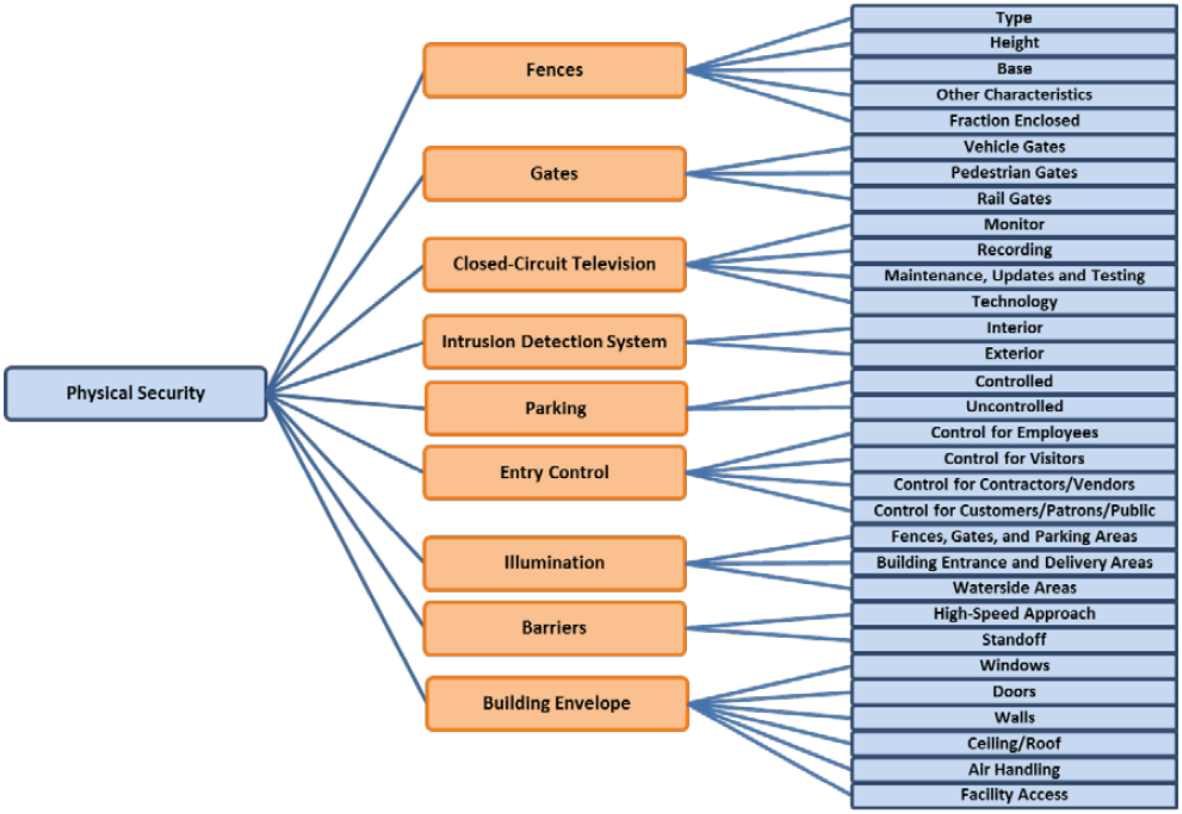

Figure S.1. Level 1 and 2 Subcomponents for Physical Security (Argonne 2013)

The team developed a customized survey instrument for assigning values to the constituents within the PMI and adapted an existing software tool for calculating and displaying the PMI. The survey instrument guides a utility analyst through a set of questions to assess the various underlying aspects of PMI and assign numerical or qualitative values. The outcome of the survey instrument is a ranking that scores relative values against a default value or peer groups. Figure S.2 provides an example of the survey output, as displayed by the software tool.

[3] Physical security is one of six major security-related components addressed by the Department of Homeland Security's Enhanced Critical Infrastructure Protection Initiative. The other five components address security force, security management, information sharing, and security activity history/background. [Argonne National Laboratory). 2013. *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*. Available at http://www.ipd.anl.gov/anlpubs/2013/11/77931.pdf]

The team envisioned use of the tool by electric utilities to self-assess their current security posture, identify current strengths and weaknesses, and evaluate how targeted investments could improve the overall PMI value or specific underlying constituents of the PMI.

Toward this end, the team sought an electric utility partner to demonstrate the approach. At the time this report was in preparation (Winter 2019), the team was in active discussions with a potential utility partner for the demonstration

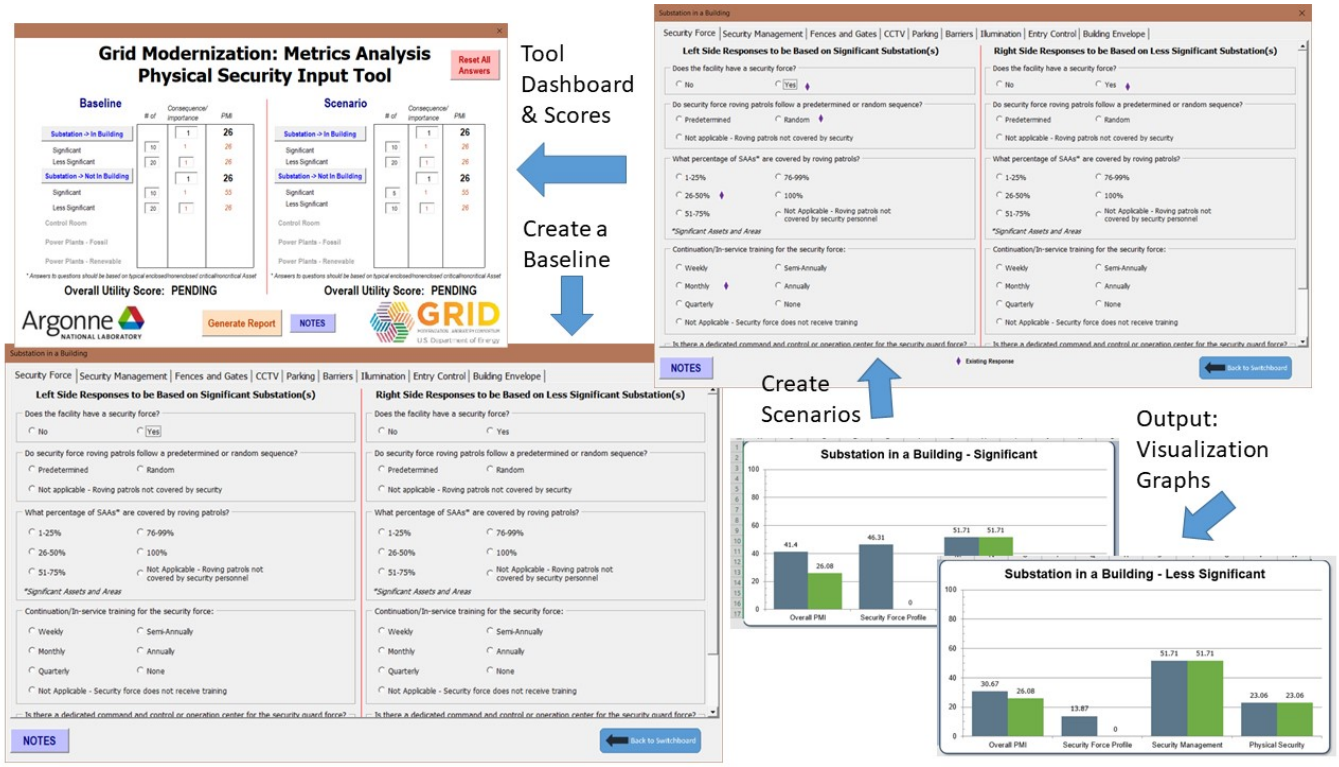

Figure S.2. Example PMI Dashboard for Consideration as Physical Security Metrics

Acknowledgments

The work conducted during the development of physical security metrics would not have been possible without the support of governmental and industry partners. The methodology presented in this report builds upon previous work funded by the U.S Department of Homeland Security (DHS); their support in providing data on the physical security attributes of the electric sector was invaluable. The authors are also particularly thankful for the feedback and comments from the Southern California Edison Company (SCE) and the Edison Electric Institute (EEI) during the development of the new physical security metrics.

Acronyms and Abbreviations

ALE	annualized loss expectancy
APPA	American Public Power Association
ARO	annualized rate of occurrence
BES	Bulk Electric System
BESSMWG	Bulk Electric System Security Metrics Working Group
C2M2	Cybersecurity Capability Maturity Model
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIRT	Critical Infrastructure Resilience Tool
C-IST	Cyber Infrastructure Survey Tool
ComEd	Commonwealth Edison
CPUC	California Public Utilities Commission
CRS	Congressional Research Service
CS&C	(DHS) Office of Cybersecurity & Communications
CSF	Cybersecurity Framework
CVSS	Common Vulnerability Scoring System
DBT	Design Basis Threat
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
ECIP	Enhanced Critical Infrastructure Protection
EEI	Edison Electric Institute
EIA	Energy Information Administration
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas, Inc.
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
GMLC	Grid Modernization Laboratory Consortium
GMLC1.1	Grid Modernization Laboratory Consortium Project Metrics Analysis
IOU	investor-owned utility
IST	Infrastructure Survey Tool
MYPP	Multi-Year Program Plan
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTTF	mean-time-to-fix
MW	megawatt(s)
NARUC	National Association of Regulatory Utility Commissioners

NASEO	National Association of State Energy Officials
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OMS	Outage Management System
PG&E	Pacific Gas and Electric Company
PMI	Protective Measures Index
PUC	Public Utilities Commission
QER	Quadrennial Energy Review
RAMP	Risk Assessment Mitigation Phase
RIST	Rapid Infrastructure Survey Tool
RTO	regional transmission organization
SCE	Southern California Edison Company
TS&D	Transmission, Storage, and Distribution

Contents

Figures

Tables

1.0 Introduction

1.1 Project Background and Motivation

The U.S. Department of Energy's (DOE's) 2015 Grid Modernization Initiative Multi-Year Program Plan (MYPP), states that as the U.S. electric grid transitions to a modernized electric infrastructure, policy makers, regulators, grid planners, and operators must seek balance among six overarching attributes (DOE 2015a): (1) reliability, (2) resilience, (3) flexibility, (4) sustainability, (5) affordability, and (6) security. Some attributes have matured and are already clearly defined with a set of metrics (e.g., reliability); others are emerging and are less sharply defined (e.g., resilience). To provide more clarity to the definition and use of the attributes, DOE is funding an effort that will evaluate the current set of metrics, develop new metrics where appropriate, or enhance existing metrics to provide a richer set of descriptors of how the U.S. electric infrastructure evolves over time.

DOE engaged nine National Laboratories to develop and test a set of enhanced and new metrics and associated methodologies through the Grid Modernization Laboratory Consortium (GMLC)'s Metrics Analysis project, generally referred to by its acronym GMLC1.1.

The project supports the mission of three DOE Offices (Office of Electricity Delivery and Energy Reliability, Office of Energy Efficiency and Renewable Energy, and Office of Energy Policy and Systems Analysis) by revealing and quantifying the current states and the evolution over time of the nation's electric infrastructure.

This project started in April 2016 and ended in March 2019.

1.2 Metric Categories Definitions

The MYPP uses the term "attribute" to describe the characteristics of the power grid. In this report, we use the terms "metric areas" or "metric categories." Metrics are physical or economic considerations that can be measured or counted. Several metrics can be grouped into a metric category.

The six metric categories explored in this project are described in Table 1.1. The purpose of this table is to list commonly-used definitions and indicate which aspects of the large breadth within a metric category this project addresses.

Table 1.1. Metrics Descriptions and Focus Areas

Metric Categories	Definitions	Focus Areas under GMLC 1.1
Reliability	Maintain the delivery of electric services to customers in the face of routine uncertainty in operating conditions. For utility distribution systems, measuring reliability focuses on interruption of the delivery of electricity in sufficient quantities and of sufficient quality to meet electricity users' needs for (or applications of) electricity. For the bulk power system, measuring reliability focuses separately on the operational	We are developing new metrics of distribution reliability, which account for the economic cost of power interruptions to customers, with the American Public Power Association. We are developing new metrics of bulk power system reliability for use in the North American Electric Reliability Corporation's Annual State of Reliability Report

Metric Categories	Definitions	Focus Areas under GMLC 1.1
	(current or near-term conditions) and planning (longer-term) time horizons.	We are demonstrating the use of probabilistic transmission planning metrics with Electric Reliability Council of Texas, Inc. and Idaho Power.
Resiliency	Can prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, including the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (Obama 2013).	We apply a consequence-based approach that defines a process using resilience goals to a set of defined hazards. This approach provides the information needed to prioritize investments for resilience improvements.
Flexibility	Respond to future uncertainties that may stress the system in the short-term and require the system to adapt over the long term. Short-term flexibility to address operational and economic uncertainties that are likely to stress the system or affect costs. Long-term flexibility to adapt to economic variabilities and technological uncertainties that may alter the system.	We focus on flexibility of the bulk power system needed to accommodate the variability of net load, which is the load minus variable generation including high penetrations of variable resource renewables.
Sustainability	Provide electric services to customers minimizing negative impacts on humans and the natural environment.	We focus on environmental sustainability specifically in Year 1 assessing metrics for greenhouse gas emissions from electricity generation. In Years 2 and 3, we also explore water metrics.
Affordability	Provide electric services at a cost that does not exceed customers' willingness and ability to pay for those services. (Taft and Becker-Dippman 2014).	We document established investment cost-effectiveness metrics and focus our research on emerging customer cost-burden metrics.
Security	Prevent external threats and malicious attacks from occurring and affecting system operation. Maintain and operate the system with limited reliance on supplies (primarily raw materials) from potentially unstable or hostile countries. Reduce the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters (Obama 2013)	We develop metrics to help utilities' evaluate their physical security posture and inform decision-making and investment.

The metric categories are described in depth in the ensuing sections of this report.

1.3 Report Contents and Organization

The ensuing sections of this Reference Document present the GMLC 1.1 Foundational Metrics approach to security (Section 2.0); describe the approach, stakeholders, and partners (Section 3.0); describe established physical and cyber security metrics that could be applied for the electric sector; address the proposed approach for electricity physical security metrics; and provide initial feedback on the proposed approach (Section 4.0). Finally, a brief discussion of next steps to further momentum gained by the GMLC 1.1 Foundational Metrics project is provided in Section 5.0.

2.0 Objective

Presidential Policy Directive 21 defines “security” as reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters (White House 2013).

Security does not possess a well-understood canon of techniques for measurement like “freight cost per mile” or “value at risk.” The security community generally uses annualized loss expectancy (ALE) as a means of justifying its security budget, instead of security metrics. ALE is the monetary loss that can be expected for an asset due to a risk over a 1-year period and is calculated by multiplying the single loss expectancy (SLE) by the annualized rate of occurrence (ARO).

The ALE approach involves a number of issues and is difficult for the electric sector to use because of many unknown probabilities. There are no actuary tables derived from decades of data collection that can tell precisely what adversaries will do, how often they will do it, and how much it will cost the electric sector when they do it.

The issue of security metrics has seen considerable activity in recent times. There are numerous approaches to monitoring and measuring security, but no consensus on which security metrics should be used for measuring security effectiveness in the electric sector.

Physical security for the bulk power system is also defined by security standards and guidelines. North American Electric Reliability Corporation (NERC) guidelines provide suggested guidance, but are not to be used to monitor or enforce compliance. This approach allows each organization to decide the risk it can accept and the practices it deems appropriate to manage its risk. NERC guidelines are intended to enable companies to develop a physical security plan that matches the level of accepted risk for each of their facilities.

The 2015 Quadrennial Energy Review (QER; DOE 2015d) indicated that a national priority is ensuring the security of the energy transmission, storage, and distribution (TS&D) infrastructure relative to new technologies, threats, and vulnerabilities. The report indicated that incomplete or ambiguous threat information may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., to address overestimated threats), or deployment of security measures against the wrong threat. The 2015 QER recommended the development of comprehensive data, metrics, and an analytical framework for energy infrastructure asset security.

The Congressional Research Service (CRS) recently concluded the grid's physical safeguards are a “work in progress,” stating that there is currently no comprehensive accounting of changes in physical security throughout the sector (CRS 2018). It also concluded that security metrics (for both cyber and physical security) have consistently been a challenge due to evolving threats and vulnerabilities. Nonetheless, anecdotal information in the public domain suggests that such changes (in security posture) may be significant and widespread.

The 2015 QER and the 2018 CRS report identified the need for the development of physical security metrics for the electric sector.

3.0 Approach

Physical security metrics have been developed by the U.S. Department of Homeland Security (DHS), through their Enhanced Critical Infrastructure Protection (ECIP) Initiative. This approach uses a methodology for assessing infrastructure risk and resilience to a variety of natural and man-made hazards. The methodology has more than 1,500 variables covering six major security-related components: physical security, security force, security management, information sharing, and security activity history/background. The gathered information is compiled into a metric called the Protective Measures Index (PMI; Argonne 2013), which is used to assist DHS in analyzing sector (e.g., Energy) and subsector (e.g., electricity, oil, and natural gas) vulnerabilities to identify potential ways to reduce vulnerabilities and to assist in preparing sector risk estimates.

The proposed physical security metrics for the electric sector are based on the PMI developed for and used by DHS, which DHS has applied to more than 600 electric sector assets in the United States. It was also used to identify gaps in preparedness and rapid recovery measures for the first QER (DOE 2015b), based on 273 energy facility site visits and surveys conducted from 2011 to 2014.

The proposed approach would ignore assets such as transmission towers, which can be quickly and easily replaced, and other electrical assets assumed to be not as critical as long-lead-time equipment (e.g., transformers in substations, etc.). The proposed approach was reviewed with various electric sector stakeholders, and corrections were made to address stakeholder comments and concerns.

For the physical security metrics development process, the physical security questions in the DHS Infrastructure Survey Tool (IST) were revised—the DHS IST contains many questions that are typically answered by site personnel; however, some questions could be answered using publicly available data or default values.

Information about all electric utilities is not available from DHS ECIP data set, so data collected from public sources were collected and used, such as security guard information available from the U.S. Bureau of Labor Statistics; U.S. Bureau of Justice crime statistics on violent crime and property crime (burglary, larceny-theft, and motor vehicle theft) as a function of city, region, category, age, and other categories; and Federal Energy Regulatory Commission (FERC) Form 1 data on substation characteristics, such as type (transmission, distribution, combined), voltages, capacity, and number of spare transformers, and to identify whether a substation is attended or unattended.

The IST summaries on various electric sector components/assets were first reviewed and statistical analysis of IST data for electric sector was performed, to develop default values (e.g., IST summary information indicates that almost all electric assets have performed background checks). The IST questions were then customized to reflect electric sector characteristics and a statistical analysis of DHS data was performed for substations, control centers, and electric generating plants.

This information was incorporated into a demo dashboard tool containing a reduced set of questions for the critical electric sector components (substations, generating plants, control rooms) in the form of an Excel spreadsheet. The demo dashboard tool was populated with default values and information about the number of electric assets by utility. Figure 3.1 shows the Excel-based dashboard developed to determine the security posture (PMI) for an unenclosed substation.

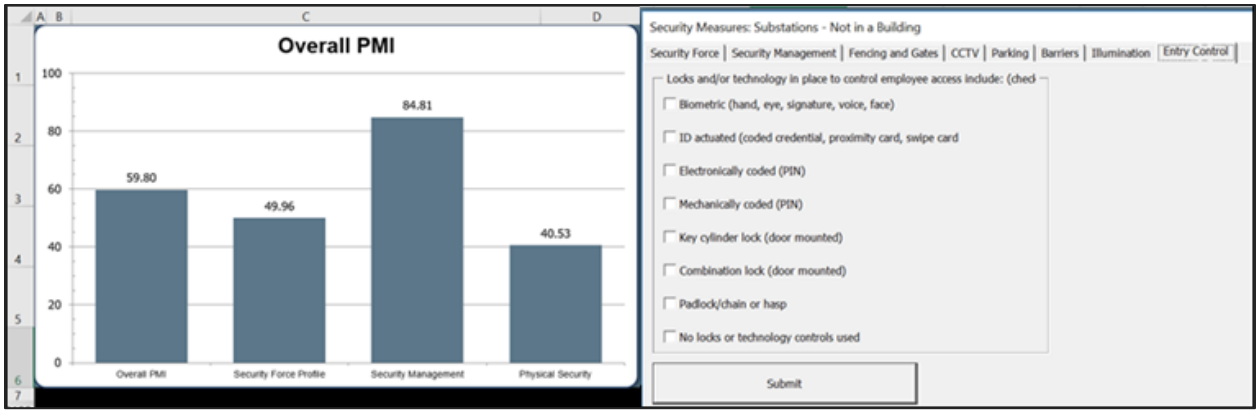

Figure 3.1. Example PMI Dashboard for Unenclosed Substations

The demo dashboard tool was sent to a number of stakeholders for their review and comments; further information on stakeholder involvement is provided in Section 4.7.2.

A key challenge in reporting grid-related metrics is that DOE is neither responsible for providing primary supporting data nor does it "own" much of the data from which grid metrics are expected to be derived. An ideal outcome would be for the organizations that bear this responsibility to adopt metric methodologies developed and successfully tested and accepted by a broad range of electric system stakeholders via GMLC 1.1.

Years 2 and 3 of the GMLC1.1 project will focus on validating metric methodologies by applying them to real-world situations with electric sector partners and establishing partnerships with key data providers, including federal and state agencies, and regional entities that could potentially help institutionalize the final products and results of GMLC 1.1. This approach is described in Figure 3.2. The physical security metrics development process was halted for nine months in Year 2 while awaiting a DOE decision to continue after the Year 1 review.

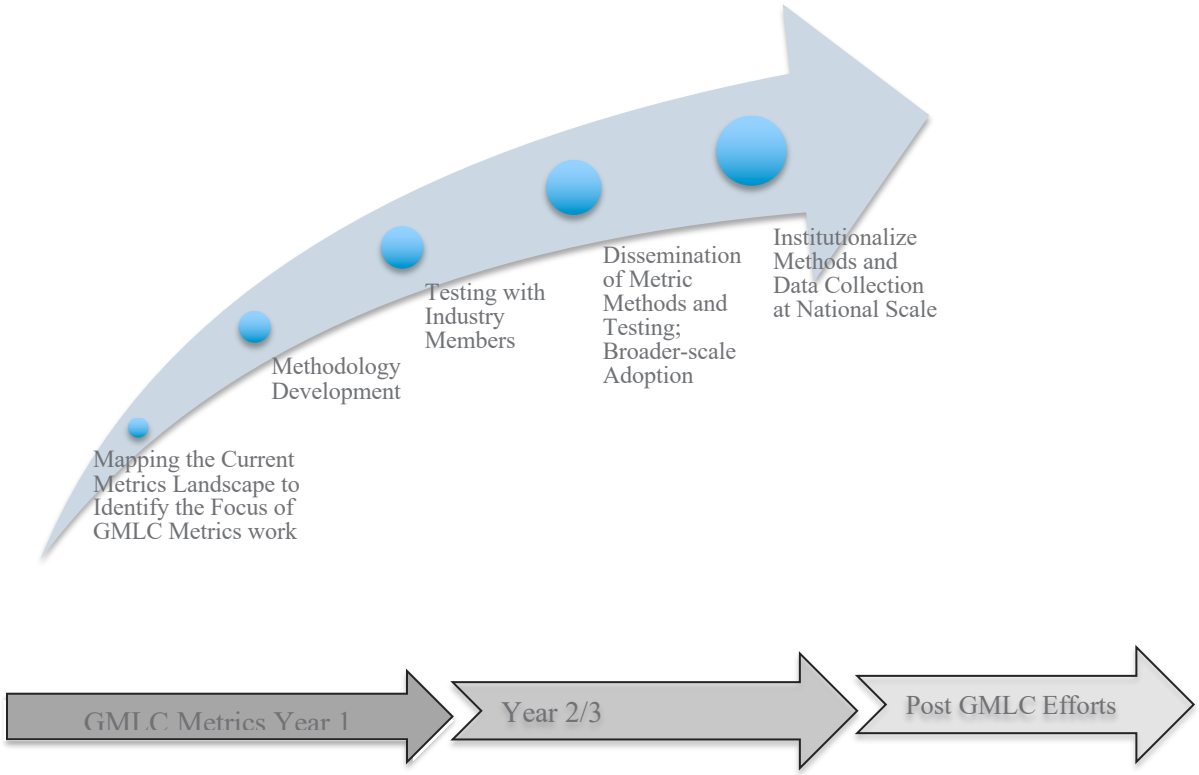

Figure 3.2. Time Line for GMLC1.1 Activities

Specific approaches to formalizing metrics varied across the six metrics category teams, depending on the maturity of metrics development and use in the area, the existence of publicly collected and disseminated sets of supporting data, and the presence of other organizations working in the space. The specific approaches included the following:

- Developing new methodologies and working with specific partners to pilot test the usefulness of these metrics with their data
- Collaborating with and leveraging related efforts of established national data providers or industry associations to explore and develop with them new ways of looking at their data
- Adapting methodologies originally developed for a specific stakeholder for broader application
- In emerging areas, working with a collection of system operators and utilities to carefully identify the existing measurement landscape and a longer-term research program to develop methodologies that could be effectively applied across jurisdictions.

Metrics are categorized by their ability to characterize the electricity system's properties historically (*lagging* metrics) or the system's ability to respond to challenges in the future (*leading* metrics). Lagging metrics are backward looking, or retrospective, where the impact of a collection of activities on a specific system can be assessed after their actual implementation. As such, they can be helpful in the aggregation of indicators of progress being made in grid modernization. Leading metrics are forward-looking or prospective, where the future impact of an activity can be estimated prior to its actual completion or implementation on a system. As such, they can be used to inform decisions about infrastructure investments or policy interventions.

3.1 Stakeholder and Partners

A critical aspect of the GMLC1.1 project is to ensure that the metrics being developed directly benefit the electricity sector. Throughout the process of developing and testing the metrics from this project, input and feedback was sought from stakeholders.

Key national organizations in the electric industry were identified as Working Partners at the inception of the project, and engaged to provide both strategic and technical input to the project as a whole. Three types of organizations were also identified for each of the six individual metric areas: (1) primary metric users, (2) subject matter experts, and (3) data or survey organizations. These stakeholders were engaged at various stages of the project, especially at, but not limited to, the beginning and scoping stages of the effort, and then to more formally review the content of this document at the end of Year 1.

The project team engaged with, received feedback from, and in some cases, formed a partnership with the following entities:

- Reliability: NERC, Institute of Electrical and Electronics Engineers (IEEE), American Public Power Association (APPA)
- Resilience: DOE/Office of Energy Policy and Systems Analysis (DOE EPSA), DHS, City of New Orleans, PJM Interconnection, Electric Power Research Institute (EPRI)
- Flexibility: FERC, Pacific Gas and Electric Company (PG&E), California Independent System Operator (CAISO), EPRI, Electric Reliability Council of Texas, Inc. (ERCOT)
- Sustainability: U.S. Environmental Protection Agency (EPA), Energy Information Administration (EIA), Arizona State University National Resources Research Institute, Sustainability Accounting Standards Board (SASB)
- Affordability: EPRI, Minnesota Public Utilities Commission (PUC), Colorado State Energy Office, Washington State Utilities and Transportation Commission, Nation Association of Regulatory Utility Commissioners (NARUC), Alaska Energy Authority
- Security: DHS, EPRI, National Association of State Energy Officials (NASEO), Edison Electric Institute (EEI), Southern California Edison Company (SCE).

In Years 2 and 3, metric category teams worked with some of the stakeholders listed above, as well as additional ones, to test the metric methodologies and demonstrate that they are technically feasible and provide value in a real-world setting. Working Partners and data organizations will be engaged at various stages.

3.2 Users of this Research

The current users of this research would be the electric utility sector, which would apply an Excel-based tool developed by this project to conduct security surveys and vulnerability assessments among their electric assets to estimate their security posture and consider potential options for improvement.

3.3 Outcome

An Excel-based spreadsheet tool was developed that accounted for the number of electric sector assets and was used to determine the PMI score as a function of asset category and degree of significance (higher versus lower):

- Electric substation (enclosed and unenclosed)
- Electric power plant (fossil and renewable)
- Electric control room (distribution and transmission).

The demo tool allows a user to specify the number of assets and their significance, provides default values for the importance of each asset category to overall electric utility operations that can be modified by the electric utility, and performs "what-if" cases to determine how changes in the protective measures used by the utility would change the overall PMI score. Figure 3.3 shows the tab in the demo tool in which the user provides the number of electric sector assets as a function of asset type and significance level; the tool predicts the asset-level PMI, which is then used to estimate the overall utility-level PMI.

Electric Asset	Significance	Valuation	Number of Assets	Predicted Asset Level PMI
Substation - outside	Higher	10	5	65
Substation - outside	Lower	2	800	55
Substation - within a building	Higher	10	5	75
Substation - within a building	Lower	2	10	65
Power Plant - fossil fueled	Higher	50	10	75
Power Plant - fossil fueled	Lower	10	15	70
Power Plant - renewable	Higher	20	10	45
Power Plant - renewable	Lower	4	15	40
Electric Control Room - distribution	Higher	1	1	80
Electric Control Room - distribution	Lower	1	1	70
Electric Control Room - transmission	Higher	1	0	80
Electric Control Room - transmission	Lower	1	0	70

Figure 3.3. Example Tab in Demo Tool containing Utility Data on Number of Assets

Figure 3.4 shows the "Substation in a building" tab in the demo tool; the right-hand side contains a series of security-related questions that the user would answer, and the resulting PMI calculated using the answers of these questions is shown on the left. The demo tool contains a feature that allows the user to compare possible security enhancements with the existing security posture and see how these changes affect the estimated overall utility PMI score (and how the changes can drive down risk).

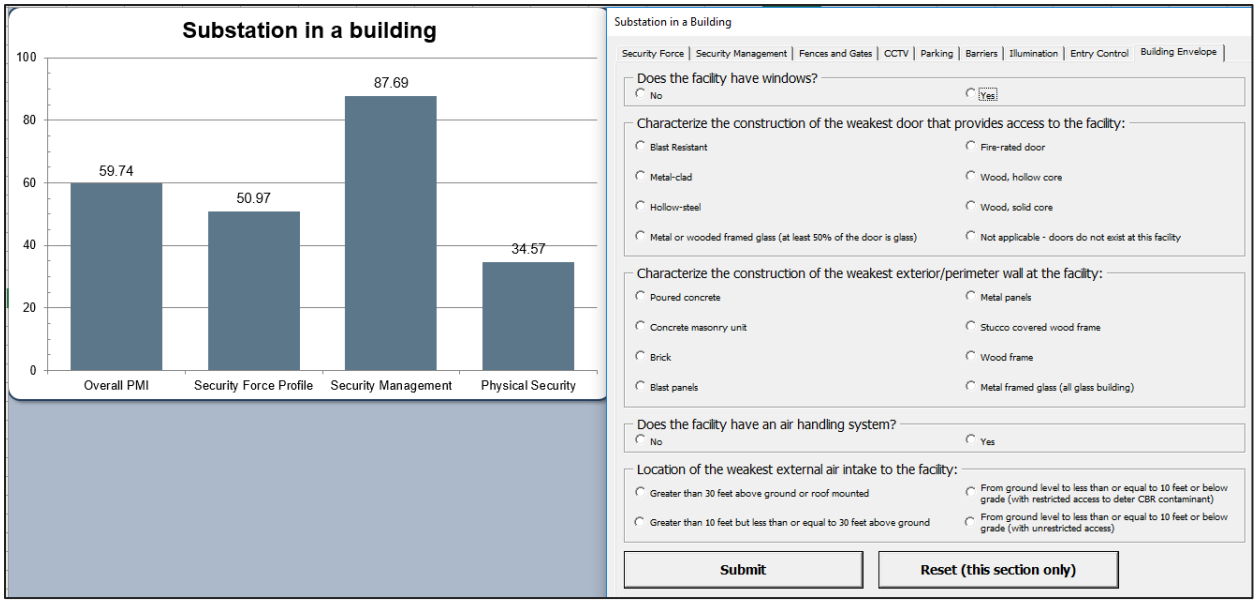

Figure 3.4. Example Tab in Demo Tool Showing Predicted PMI for Substations in Building Based on Electric Utility-Supplied Security Data

4.0 Physical Security

4.1 Definition

Security is defined as the ability to resist external disruptions to the energy supply infrastructure caused by intentional physical or cyber-attacks or by limited access to critical materials from potentially hostile countries. As applied to physical/cyber security, security prevents external threats and malicious attacks from occurring and affecting system operation. Specifically, with respect to the supply chain, security means maintaining and operating the system with limited reliance on supplies (primarily raw materials) from potentially unstable or hostile countries. These operational definitions are founded in principles outlined in Presidential Policy Directive 21 (Obama 2013), "Critical Infrastructure Security and Resilience," which defines "security" as "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters."

4.2 Established Metrics

Security metrics for the electric sector have recently seen considerable development (Brotby 2009; Bakshi et al. 2011; Biringer et al. 2013); however, there are numerous approaches but no consensus on which of the numerous security metrics should be used. One reason is that there is no well-understood canon of techniques for the measurement of security.

Instead of security metrics, the security community generally uses ALE as a means of justifying its security budget (Seger 2003; Zalewski et al. 2014; Jaquith 2007). ALE is the monetary loss that can be expected for an asset due to a risk over a 1-year period; it is calculated by multiplying the SLE by the ARO:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

There are issues with applying the ALE approach to the electric sector, especially in the case of planning for a deliberate attack by an intelligent adversary. The electric sector does not have actuary tables derived from decades of data collection that can tell precisely what adversaries will do, how often they will do it, and how much it will cost the electric sector when they do it. The number of unknowns that would have to be modeled to predict adversarial behaviors and the margin of error associated with modeling those unknowns would make the estimates far too uncertain for the ALE approach to be useful. In addition, the ALE approach is highly qualitative in terms of its inputs, and it does not provide metrics of progress that display the status of physical and/or cyber security in comparison with the final security goals of an electric utility.

4.3 State of the Art

Quantifying the benefits of managing cyber and physical security in the electric industry is challenging. The field of security metrics is relatively new compared to the engineering measures of a utility's traditional power systems. The following sections provide examples of recently developed security metrics (but are not meant to be all-inclusive).

4.3.1 NERC Bulk Electric System Security Metrics

In 2012, a new Bulk Electric System Security Metrics Working Group (BESSMWG) developed a framework for physical and cyber security metrics that measures and tracks historic performance (i.e., lagging) and provides leading indicators of future issues. The BESSMWG considered general categories of metrics related to security performance, including publicly available historical information about actual physical and cyber events, as well as leading indicators of information sharing and publicly available metrics of global cyber vulnerabilities relevant to the electric sector; no classified information was considered. The current NERC Bulk Electric System (BES) security metrics (NERC 2015) are as follows:

- Reportable cyber security incidents (that result in a loss of load)
- Reportable physical security events (that occur over time as a result of threats to a facility or BES control center or damage or destruction to a facility)
- Electricity Sector Information Sharing and Analysis Center (E-ISAC) membership (the number of E-ISAC member organizations)
- Industry-sourced information sharing (the number of E-ISAC Incident Bulletins, currently known as Watch List entries)
- Global cyber vulnerabilities (the number of global cyber vulnerabilities with a Common Vulnerability Scoring System [CVSS; NIST 2017] of 7 or higher).

4.3.1.1 Maturity Level

These security metrics have been in use since 2014.

4.3.1.2 Applications

The NERC BES security metrics have been applied to the U.S. bulk power system.

4.3.1.3 Data Source and Availability

The challenges in applying NERC's security metrics include limited historical data, limited ability to normalize available data, limited response to a changing threat landscape, and the need for sensitive information.

4.3.1.4 EPRI Cyber Security Metrics

Cyber security as a field is typically defined by security standards and guidelines. Cyber security metrics have been developed by EPRI for the bulk power system and are intended to provide example actionable metrics that utilities may leverage to create a cyber security metrics program (EPRI 2016a). In 2015, EPRI collaborated with members and external partners to create and vet a template for creating security metrics. In 2016, EPRI developed a set of potential metrics and data points that may be used in a security metrics program. These metrics were categorized at three different levels in a hierarchical structure—strategic, tactical, and operational. Figure 4.1 displays the connected nature of the metrics from strategic level, executive-level summary metrics, to tactical, management level summary metrics, down to operational day-to-day metrics calculated directly from data points gathered throughout the day.

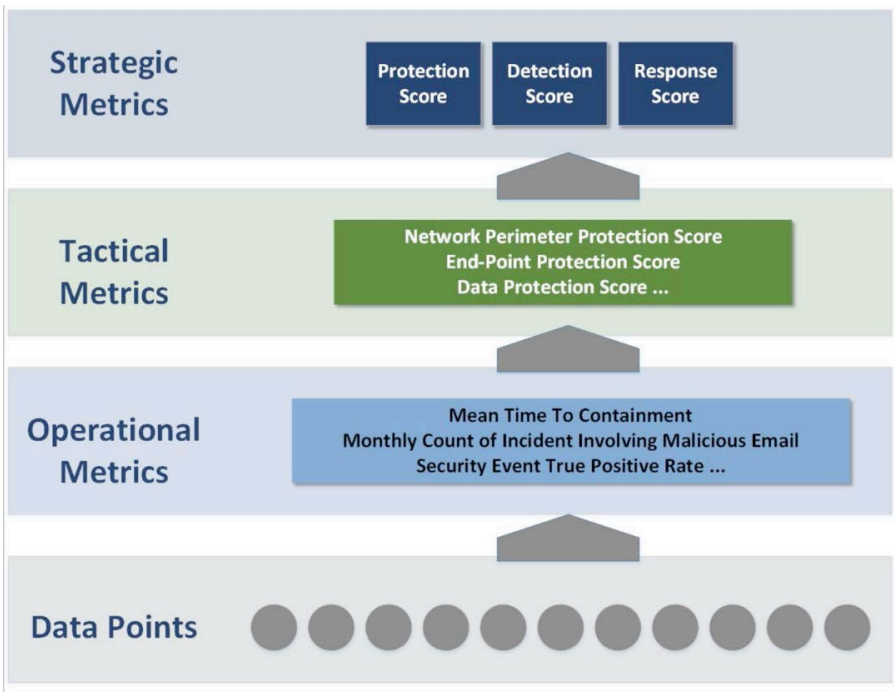

Figure 4.1. EPRI Hierarchy of Metrics (EPRI 2016a)

Strategic- and tactical-level metrics are represented by a normalized value between 0 and 10, where a higher value indicates better performance. The methodology for aggregating and normalizing the metrics is currently under development at EPRI. Operational-level metrics are derived directly from the data points, which consist of various operational statistics collected from different points in utility operations, and represent one specific aspect of security controls in a target system. Table 4.1 and Table 4.2 detail EPRI's strategic- and tactical-level cyber security metrics for measuring the effectiveness of the cyber security program for the electric sector. Information about naming nomenclature can be found in the associated EPRI report (EPRI 2016a).

Table 4.1. EPRI's Strategic Metrics and Associated Tactical Metrics

Metric ID	Strategic Metric	Tactical Metric ID	Tactical Metric Name
S-PS	Protection Score	T-NPPS	Network Perimeter Protection Score
		T-EPS	End-point Protection Score
		T-PAS	Physical Access Control Score
		T-HSS	Human Security Score
		T-NVS	Core Network Vulnerability Control Score
		T-NAS	Core Network Access Control Score
		T-DPS	Data Protection Score
		O-I-MTBI	Mean Time Between Security Incidents
		T-SMS-P	Security Management Score -Protection
S-DS	Detection Score	T-TAS	Threat Awareness Score
		T-TDS	Threat Detection Score
		T-SMS-D	Security Management Score - Detection
S-RS	Response Score	T-IRS	Incident Response Score
		T-SMS-R	Security Management Score - Response

Table 4.2. EPRI's Tactical Metrics and Associated Operational Metrics

Metric ID	Tactical Metric Name	Operational Metric ID	Operational Metric Name
T-NPS	Network Perimeter Protection Score	O-N-MAPS	Mean Access Point Protection Score
		O-N-MWAPS	Mean Wireless Access Point Protection Score
		O-N-MIPS	Mean Internet Traffic Protection Score
		O-I-MCME	Mean Count-M Malicious Email
		O-I-MCMU	Mean Count-M Malicious URL
		O-I-MCNP	Mean Count-M Network Penetration
T-EPS	End-point Protection Score	O-U-MSDPS	Mean Stationary End-Point Protection Score
		O-U-MMDPS	Mean Mobile End-Point Protection Score
		O-I-MCMW	Mean Count-M Malware
		O-I-MCMD	Mean Count-M Mobile End-Point
		O-I-MCSD	Mean Count-M Stationary End-Point
T-PAS	Physical Access Control Score	O-A-MPACS	Mean Physical Access Control Score
		O-I-MPAV	Mean Count-M Physical Access Violation
T-HSS	Human Security Score	O-H-MHSS	Mean Human Security Score
		O-I-MCSE	Mean Count-M Social Engineering
T-NVS	Core Network Vulnerability Control Score	O-A-MAC	Mean Asset Connectivity
		O-A-MAP	Mean Asset Proximity to Hostile Network
		O-A-MVRS	Mean Asset Vulnerability Risk Score
		O-A-MNVRS	Mean Network Vulnerability Risk Score
		O-I-MCNP	Mean Count-M Network Penetration
T-NAS	Core Network Access Control Score	O-A-MAC	Mean Asset Connectivity
		O-A-MAP	Mean Asset Proximity to Hostile Network
		O-A-MACS	Mean Asset Access Control Score
		O-A-MNACS	Mean Network Access Control Score
		O-I-MCNP	Mean Count-M Network Penetration
T-DPS	Data Protection Score	O-D-MDCS	Mean Data Confidentiality Score
		O-D-MDIS	Mean Data Integrity Score
		O-D-MDAS	Mean Data Availability Score
		O-I-MCDL	Mean Count-M Data Leak/Loss
T-SMS	Security Management Score	O-M-SBR	Security Budget Ratio
		O-M-SPR	Security Personnel Ratio
		O-M-CRTS	Cybersecurity Risk Tolerance Score
T-TAS	Threat Awareness Score	O-T-IES	Organization Threat Awareness Score
		O-T-MTIA	Mean Time from Intelligence to Action

Metric ID	Tactical Metric Name	Operational Metric ID	Operational Metric Name
		O-T-MTIP	Mean Time from Intelligence to Protection
		O-T-THES	Threat Hunting Effectiveness Score
T-TDS	Threat Detection Score	O-T-MITP	Mean Threat Intelligence True Positive Rate
		O-T-MCI	Mean Count-M Threat Intelligence
		O-E-METP	Mean Security Event True Positive Rate
		O-E-MC	Mean Count-D Security Events
		O-T-THTP	Mean Threat Hunting True Positive Rate
		O-T-MCH	Mean Count-M Threat Hunting Intelligence
		O-I-MCH	Mean Count-M High Severity Incidents
		O-I-MCM	Mean Count-M Medium Severity Incidents
		O-I-MCT	Mean Count-M Total Incidents
T-IRS	Incident Response Score	O-I-MTTD	Mean Time to Discovery
		O-I-MCMSI	Mean Count-M Missed Security Incidents
		O-E-SEMS	Security Event Management Score
		O-I-MTTC	Mean Time to Containment
		O-I-MTR	Mean Time to Recovery
		O-I-MTTA	Mean Time to First Action
		O-I-MCRM	Mean Cost of Response in Man-Hour (existing resource)
		O-I-MCRX	Mean Cost of Response in Dollar Amount (extra resource)

Unlike strategic or tactical metrics, operational metrics are not normalized into a numerical value between 0 and 10. Currently, 49 operational metrics are being considered by EPRI (please refer to the report for further information—EPRI 2016a).

4.3.1.5 Maturity Level

EPRI stated in its report that topics for future research may include the following:

- Data collection strategies including specific information technology and operational technology considerations related to extracting data from manual sources
- Identification of security tools required for data collection
- Mapping of each metric to NERC Critical Infrastructure Protection (CIP), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and the Cybersecurity Capability Maturity Model (C2M2)
- Development of a methodology for rolling up the lower level metrics to higher level metrics
- Normalization techniques for metric scores.

EPRI indicates that it intends to continue the discussion among members and external partners to aggregate metrics for industry benchmarking.

4.3.1.6 Applications

In addition to finalizing the methodology, EPRI intends to work with members to pilot the methodology. Through the pilot program, the utilities will identify the best approach to adopting security metrics in alignment with their own organizational goals and risk management strategies.

4.3.1.7 Data Source and Availability

Application of the EPRI cyber security metrics would require utility-specific data that could be considered sensitive and possibly business-proprietary. This would limit the use of this approach to utilities, and it may not be available on a regional or national scale.

4.3.2 DHS Cyber Infrastructure Survey Tool

The Cyber Infrastructure Survey Tool (C-IST) is used by the DHS Office of Cybersecurity & Communications (CS&C) to evaluate controls-based cyber protection and resilience measures within critical infrastructure sectors. The C-IST is a structured, interview-based assessment focusing on more than 80 cybersecurity controls grouped under five key surveyed topics. The key principles of the C-IST method focus on protective measures, threat scenarios, and a service-based view of cyber security in the context of the following five surveyed topics:

- Cybersecurity management
- Cybersecurity forces
- Cybersecurity controls
- Cyber incident response
- Cyber dependencies.

The cybersecurity controls surveyed within the C-IST broadly align with the NIST CSF.

4.3.2.1 Maturity Level

These security metrics have been in use since 2014.

4.3.2.2 Applications

The DHS C-IST is used by the DHS CS&C's Cyber Security Advisors.

4.3.2.3 Data Source and Availability

The data for the DHS C-IST are provided by the critical infrastructure asset owners and operators. This information is considered sensitive, non-public information by industry, and as such is designated as Protected Critical Infrastructure Information (PCII) and is subject to handling and dissemination restrictions. The PCII limitations on the use of this data set would be enforced when the information is associated with the facility or owner/operator. If the data are sanitized of identifying information, they can be more widely shared and potentially used in the development of cyber security metrics. The sanitization process might limit the use of this data set to only national- or regional-level aggregated metrics where individual sites or operators and their vulnerabilities are not identified.

4.3.3 DOE Electricity Subsector Cybersecurity Capability Maturity Model

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was developed by the DOE to improve electricity subsector cybersecurity capabilities and to understand the cybersecurity posture of the energy sector. The ES-C2M2 was derived from the C2M2, which DOE developed using industry-accepted cybersecurity practices to assist all types of organizations in evaluating their cybersecurity programs. The model provides maturity indicators that provide the organization information about their cybersecurity capabilities and risks during normal and crisis operations. In addition to the C2M2 core, the ES-C2M2 contains reference material and implementation guidance specific to the electric subsector (DOE 2016b).[1] The maturity indicators in the ES-C2M2 can be used to baseline and gauge the effectiveness of an electric organization's cybersecurity. The results allow an organization to quickly assess their current capabilities and outline plans for future states. As a one-day self-evaluation, the C2M2 provides a relatively easy entry into the world of security metrics. However, C2M2 does not measure the performance of each domain, a capability which is needed for security metrics.

4.3.3.1 Maturity Level

The ES-C2M2 tool has been available to the public since January 2012.

4.3.3.2 Applications

The DOE ES-C2M2 was developed in partnership with NERC, EEI, National Rural Electric Cooperative Association, APPA, and numerous utilities, including SCE, Bonneville Power Administration, PG&E, ERCOT, Dominion Resources, and American Electric Power.

4.3.3.3 Data Source and Availability

The data for the DOE ES-C2M2 are provided by the critical infrastructure asset owners and operators. According to the C2M2 Frequently Asked Questions sheet (DOE 2014), DOE does not retain any utility-provided information or results from the self-assessments.

4.3.4 California Public Utilities Commission Physical Security Metrics

The California Public Utilities Commission (CPUC) examined grid security at all levels of the electric supply system, including the distribution level, and has recommended a possible methodology for utility electric distribution system physical security planning (Brinkman et al. 2015). Existing CPUC rules establish various requirements regarding distribution system physical security, and California Senate Bill 699 mandates CPUC action to develop rules for physical security for the distribution system in a new proceeding or new phase of an existing proceeding (CA Legislative Assembly 2014). Examples of quantitative metrics considered by the CPUC for distribution physical security measures include tracking the following:

- Copper theft
- Successful or unsuccessful intrusion or attack
- False or nuisance alarms
- The condition of all monitoring equipment (e.g., number of malfunctions of security equipment)

[1] Note that there is also an Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) that comprises a maturity model, an evaluation tool, and DOE-facilitated self-evaluations specifically tailored for the oil and natural gas subsector.

- Performance of security personnel in training exercises and on tests
- Instances of vandalism or graffiti.

The CPUC stated that it was virtually impossible for regulators to establish a "one-size-fits-all" approach that would work for all utilities, and concluded that a performance-based approach with reliable metrics lends itself well to a system that has varied equipment in the electric sector.

4.3.4.1 Maturity Level

A June 2014 CPUC physical security workshop indicated that all California electric utilities use some sort of risk and vulnerability assessment to plan for physical security protections, as well as use similar physical threat mitigation techniques.

4.3.4.2 Applications

The CPUC examined grid security at all levels of the electric supply system in California during 2014, including the distribution level, and is currently re-evaluating its existing policies and oversight activities for electric system security.

4.3.4.3 Data Source and Availability

A portion of the data needed for these metrics is available from public literature, but data on the condition of monitoring equipment, problems with access control, and other conditions or issues would have to be provided by each electric utility. This type of information about the electric system would be confidential for security concerns. As such, it may be difficult to apply this approach on a regional and national level without heavy involvement of local electric utilities.

4.3.5 DHS Infrastructure Survey Tool

The IST is used to collect a series of physical security metrics developed by DHS, through their ECIP Initiative. This approach uses a methodology for assessing infrastructure risk and resilience to a variety of natural and man-made hazards. The IST has more than 1,500 data collection points covering five major security-related components: physical security, security force, security management, information sharing, and security activity history/background. The gathered information is compiled into a metric called the PMI (Argonne 2013), which is used to assist DHS in analyzing sector (e.g., Energy) and subsector (e.g., Electricity, Oil, and Natural Gas) vulnerabilities to identify potential ways to reduce vulnerabilities and to assist in preparing sector risk estimates. The PMI combines the information collected in five categories, which are also called PMI Level 1 components (Figure 4.2).

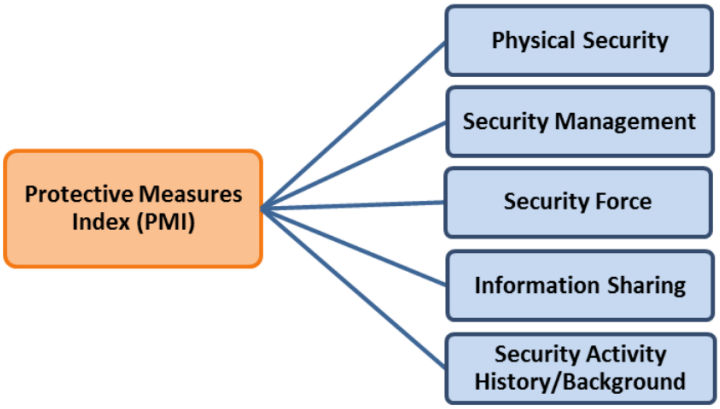

Figure 4.2. Level 1 Components of the Protective Measures Index

The PMI structures the information collected in five categories—physical security, security management, security force, information sharing, and security activity history/background[1]—to characterize the protective posture of a facility. The overall PMI consists of a weighted sum of the five major security-related components (W_i) and scaling constant (d_i), indicating its relative importance:

$$PMI = \sum d_i \times W_i$$

The PMI approach is based on following references, which contain information about the types of threats that are considered within the five physical security categories:

- FEMA 426 – Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 2003)
- FEMA 452 – Risk Management Series – Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 2005)
- ASIS– Protection of Assets Manuals (ASIS 2012)
- Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard (DHS 2015).

A design basis threat (DBT) is a profile of the type, composition, and capabilities of an adversary. The U.S. Nuclear Regulatory Commission (NRC) and its licensees use the DBT as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. The DHS PMI approach considers more than 30 DBTs that may be expected to encompass various threats that an individual electric asset may encounter, as shown in Table 4.3.

[1] The Physical Security component in the PMI approach refers to measures and features that protect a facility and its buildings, perimeter, and occupants from intrusion; Security Management refers to plans and procedures a facility has in place to deal with security issues; Security Force refers to a special group of employees or contractors that has security duties; Information Sharing refers to the exchange of hazard and threat information with local, state, and federal agencies; and Security Activity History/Background collects information related to previous vulnerability assessments and new protective measures that a facility may have implemented within the last year to improve its security posture.

Table 4.3. Partial List of DBT Events Considered in the PMI Approach

Threat	Application Mode	Duration	Extent of Effects; Static / Dynamic
Improvised Explosive Device (Bomb) - Stationary Vehicle - Moving Vehicle - Mail - Supply - Thrown - Placed - Suicide Bomber	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat until the attack site is determined to be clear.	Extent of damage is determined by the type and quantity of explosive. Effects generally direct-based than cascading consequences, incremental structural failure, etc.
Armed Attack - Ballistics (small arms) - Stand-off Weapons (rocket-propelled grenades, mortars, etc.)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.
Chemical Agent - Blister - Blood - Choking/Lung/ Pulmonary - Incapacitating - Nerve - Riot Control / Tear Gas - Vomiting	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.

4.3.5.1 Maturity Level

These security metrics have been applied by DHS since 2009 (Fisher and Norman 2010).

4.3.5.2 Applications

From the period between January 2011 and January 2016, the DHS has conducted more than 4,300 security surveys of critical infrastructure and key resources, which included more than 400 security surveys of electric subsector facilities.

4.3.5.3 Data Source and Availability

The data collected as part of a DHS IST are provided by the critical infrastructure asset owners and operators. The data are validated as PCII and are protected under the Critical Infrastructure Information Act of 2002 from the Freedom of Information Act; state, local, tribal, and territorial disclosure laws; use in regulatory actions; and use in civil litigation. Only authorized federal, state, and local security analysts are allowed to handle PCII data. (See the Final Rule at 6 CFR Part 29, published in the *Federal Register* on September 1, 2006, for more information about PCII.)

4.4 Emerging Metrics

Baseline metrics are calculated with existing electric facility security information collected via the IST. The baseline metrics listed in Section 4.2 would be augmented by emerging metrics or enhanced existing

metrics designed to fill the gaps identified through the security metrics reviews. Discussion with utilities, industry trade associations, DHS, and DOE decision-makers might be necessary to ensure the necessary and sufficient breadth of security activities and mitigation activities is captured by the developed metrics. The proposed framework for security metrics provides consistent and repeatable application and calculation across all utilities while maintaining flexibility to account for organization of facility security objectives given their specific threat landscape and security priorities. In general, security objectives focus on preventing, detecting, mitigating, and recovering from attacks on the system.

4.4.1 Revised Protective Measures Index

4.4.1.1 Potential or Proposed Approach

The DHS IST enables users to gather critical infrastructure data, including vulnerability, resilience, and consequence information, which provide a complete context for meeting users' mission-specific needs to identify vulnerabilities and develop mitigation strategies. As described in Section 4.3.5, the data collected with the IST are weighted and scored, enabling DHS to conduct comparisons of like sets of infrastructure. The DHS IST is the "most widely applied security survey method that can identify security gaps and trends, and enable detailed analyses of site and sector vulnerabilities" (DHS 2015b).

Figure 4.3 displays the process for creating a revised PMI. The current IST questions are answered by site personnel, but could conceivably be answered by public data sets. It is proposed that the individual IST questions about physical security, which are used in the PMI calculation, be examined to establish whether these IST questions require sensitive security information available only from site personnel or whether public data could supply the required information.

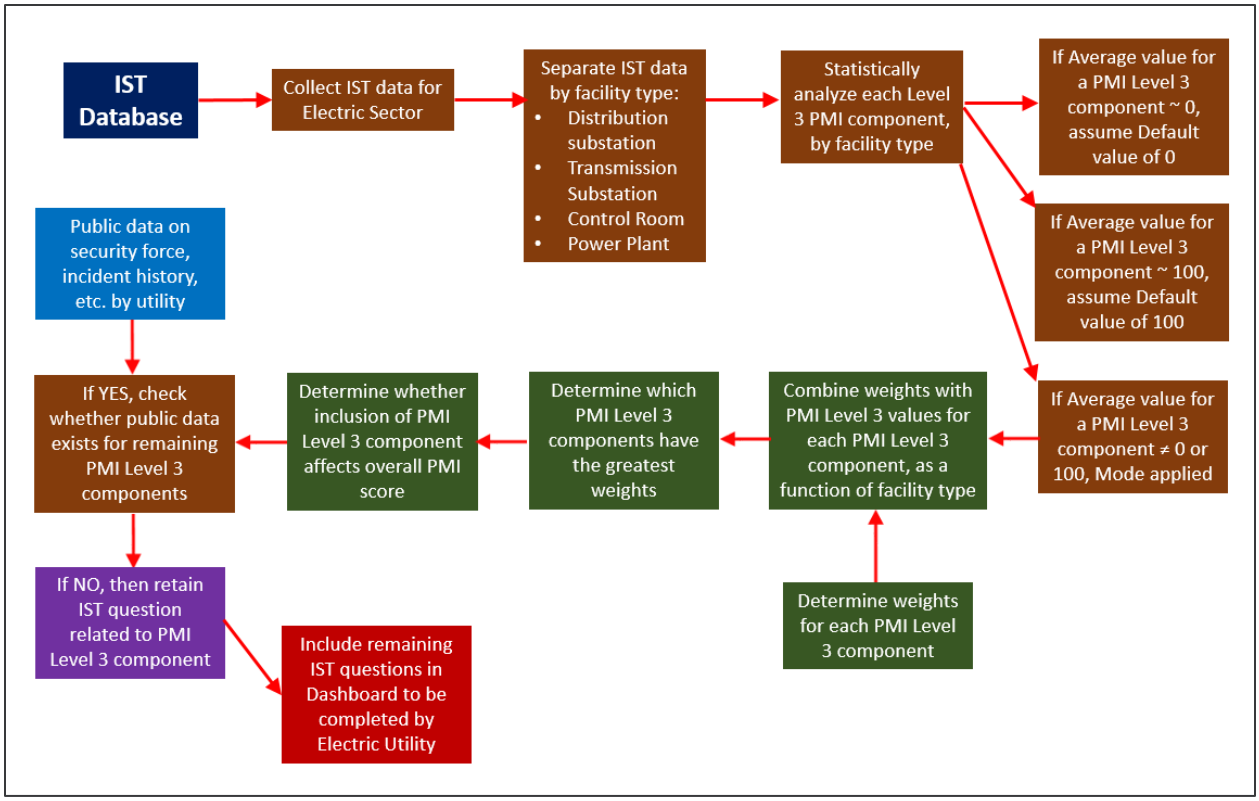

Figure 4.3. Overall Process Diagram for Revising the DHS PMI (Based on IST Questions) for the Electric Sector

The PMI organizes the information collected with the IST into four levels of information in order of increasing specificity; raw data are gathered at Level 4. These are then combined further through Levels 3, 2, and, finally, Level 1. Each of the Level 1 components is defined by the aggregation of Level 2 subcomponents that allow analysts to characterize aspects of a facility's existing security posture. The PMI is constituted by five Level 1 components, 25 Level 2 subcomponents, and 64 Level 3 subcomponents. For the PMI, the information collected characterizes the weakest protective measures (i.e., the weakest portion of fence if types and characteristics vary). Some of these values can be inferred from current industry practice (NERC and similar standards) for elements such as physical security, for which the Level 2 subcomponents are shown (Figure 4.4). In this figure, the Level 1 component is physical security and the nine Level 2 components are shown in the middle orange-colored boxes, including Fences to Building Envelope. The Level 3 components for the Level 1 physical security are shown on the right-hand side of Figure 4.4, and include Type (shown to the right of the "Fences" box) to Facility Access. The Level 3 subcomponents provide more granular information concerning the Level 2 subcomponents, which are aggregated into the Level 1 physical security component.

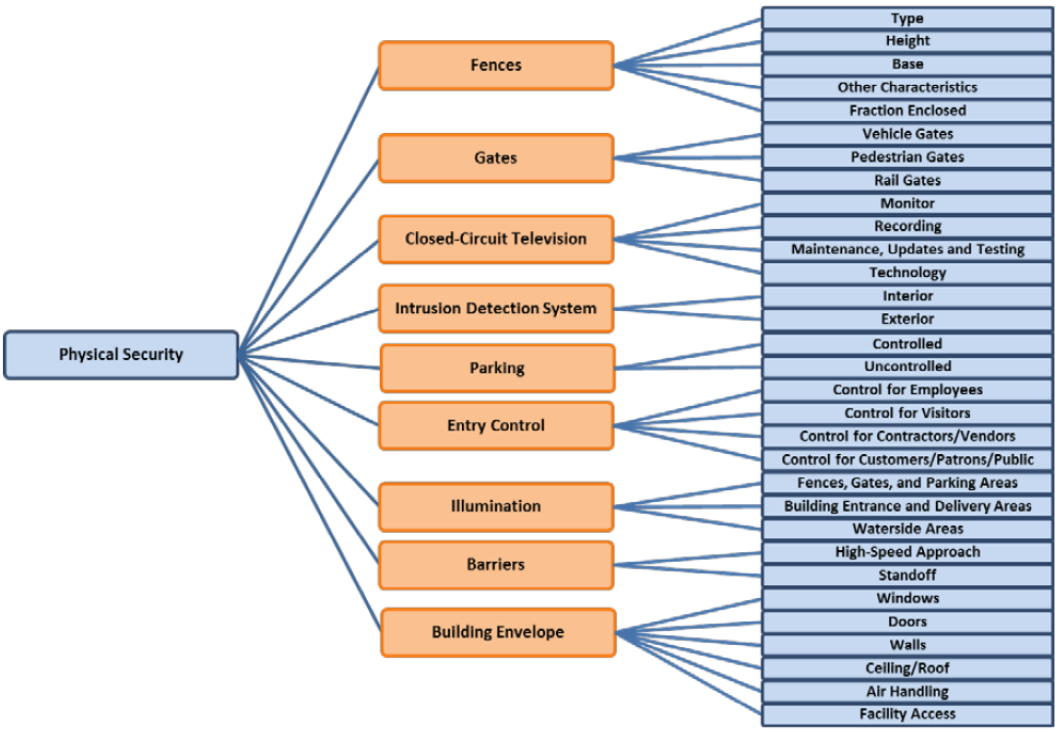

Figure 4.4. Level 2 and Level 3 Subcomponents for the Level 1 Physical Security Component (Argonne 2013)

The PMI requires information that may not be available from public data sources, such as Memoranda of Understanding/Memoranda of Agreement (MOUs/MOAs) with local law enforcement, and detailed characteristics of utility security forces. These gaps may be supplemented by analysis performed by Argonne National Laboratory (Argonne) to identify gaps in preparedness and rapid recovery measures for DOE's QER, which used data collected regarding 170 electric facilities from January 2011 through September 2014 (DOE 2015c). Another option being investigated is whether default values could be applied based on a statistical analysis of the PMI Level 3 components, which could be subsequently revised when site- or utility-specific data become available. This approach may be applicable for the Level 1 Security Force component and its Level 2 and Level 3 subcomponents, which are shown in Figure 4.5. Public information is available for the Level 2 subcomponent, Staffing, in Figure 4.5, while default values for Level 3 subcomponents, such as Programs and Frequency (associated with security force training), can be assumed based on current electric industry security guidance (e.g., NERC 2011).

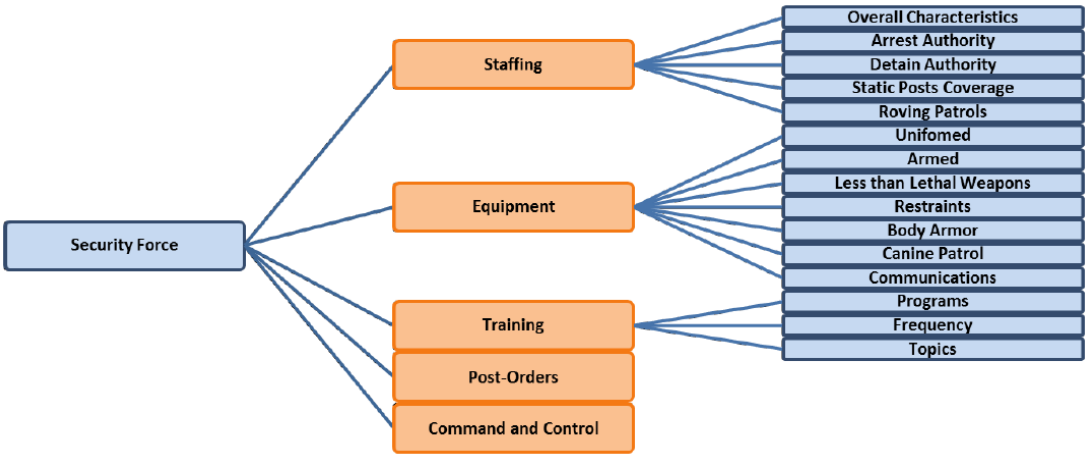

Figure 4.5. Level 2 and Level 3 Subcomponents for the Level 1 Component Security Force (Argonne 2013)

Information needed for the Level 1 Security Activity History/Background component may be available from data collected by various organizations concerning electric outages in the United States. The Level 2 subcomponents (the two orange-colored boxes) and the 10 Level 3 subcomponents (ranging from Prior Vulnerability Assessment Conducted to Initiation of Planning and Preparedness) are shown in Figure 4.6.

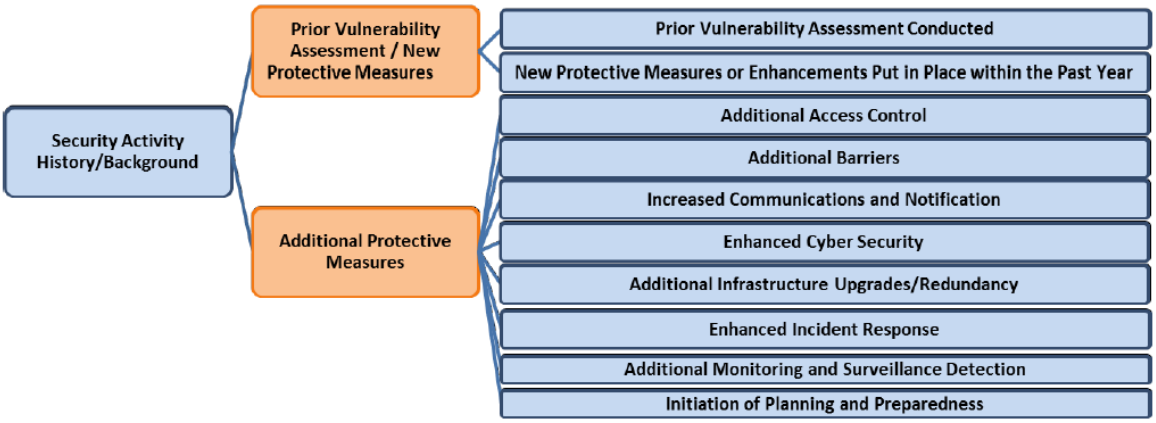

Figure 4.6. Level 2 and Level 3 Subcomponents for the Level 1 Security Activity History/Background Component (Argonne 2013)

Another sub-option shown in Figure 4.3 would be to reduce the number of questions in the analysis, based on the statistical analysis of the PMI Level 3 components, which may result in a model similar to the Rapid Infrastructure Survey Tool (RIST; NASEO 2014) (Figure 4.7). The Rapid Infrastructure Assessment captures a facility's physical and operational security and resilience data. The data are then analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities. This approach would have to be researched to determine its applicability for establishing the security posture of a given electric utility using publicly accessible data; an initial assessment indicates that the questions in the RIST would require utility input. Though the questions are similar to those in the IST, the methodology for the calculations is different, which creates uncertainty about the relationship between the indices provided via the RIST aligning with the indices provided b the IST.

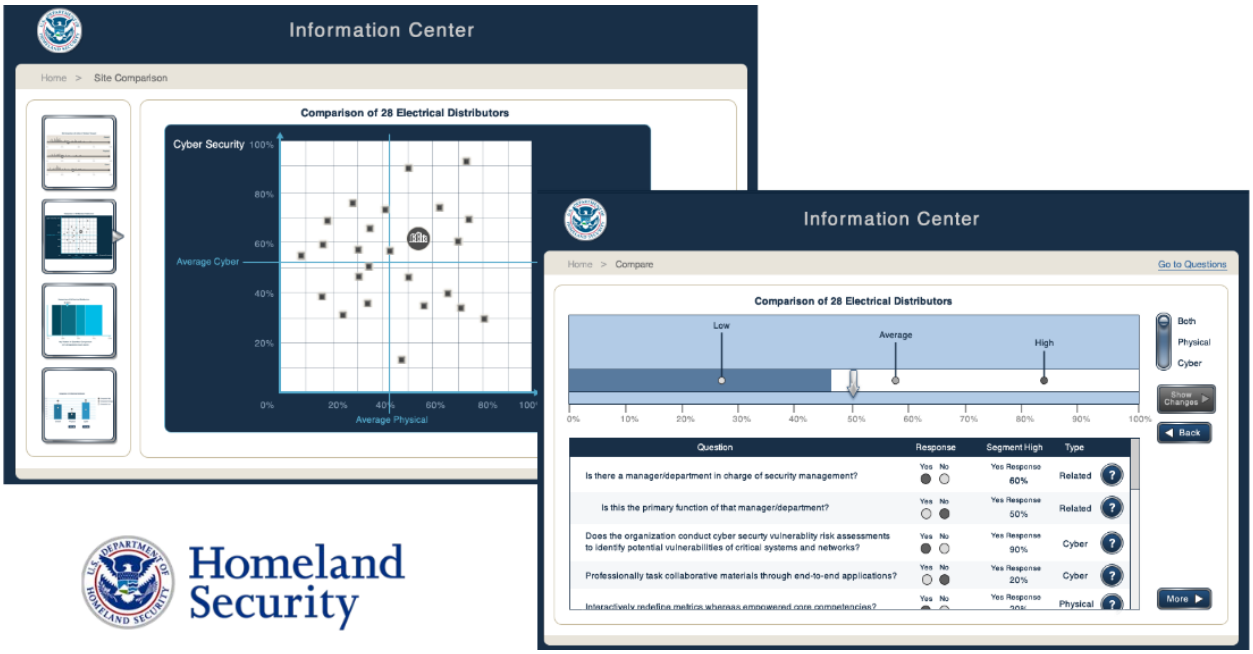

Figure 4.7. Sample Information from the Rapid Infrastructure Survey Tool (Norman 2015)

The above approach was presented to and discussed with a number of potential stakeholders during 2016, and the following points were made:

- Argonne received approval from DHS management to develop potential metrics for physical security based on the DHS PMI.
  - DHS agreed to support GMLC activity through development of default values (for sub-metrics) and identification of which sub-metrics are most significant in determining physical security of the electric sector.
  - Some PMI default values have been received from DHS, and statistical analysis of the DHS IST data set for the electric sector is under way.
- EPRI agreed to review the proposed approach and provide suggestions for improvement.
- EEI stated that it would be willing to present the proposed physical security metrics to its members for their approval and guidance if and when a demo tool (showing how the overall PMI is calculated for a given electric utility) has been developed.
- The NASEO stated that it would review the proposed approach to determine its acceptance by state PUCs and agencies, and establish which states/regions may be most willing to participate in a pilot program.
- The above organizations stated that they would be willing to be involved in the development of cyber security metrics for the electric sector during FY 2017.

4.4.2 National Infrastructure Protection Plan Security Metrics

4.4.2.1 Potential or Proposed Approach

For development of future security metrics, another option could be to follow the approach taken in the National Infrastructure Protection Plan (NIPP), which defined three sets of primary measures, as follows (DHS 2009):

- Descriptive measures, which will be used to understand electric resources and activities. These measures will be qualitative in value, and should be the easiest and least costly for which to collect data.
- Process (or output) measures, which show progress toward achieving security goals. The data for these measures would be quantitative or semi-quantitative in value.
- Outcome measures that track the progress toward a strategic goal by beneficial results rather than level of activity. These outcome measures, unlike descriptive and process measures, are generally determined by models, assumptions, or complex formulas.

Example metrics for the energy sector used in the NIPP are shown in Figure 4.8. This approach was rejected for physical security metrics development because it requires detailed utility input into decision metrics, such as how well does the utility "Assess Risks" or "Set Security Goals."

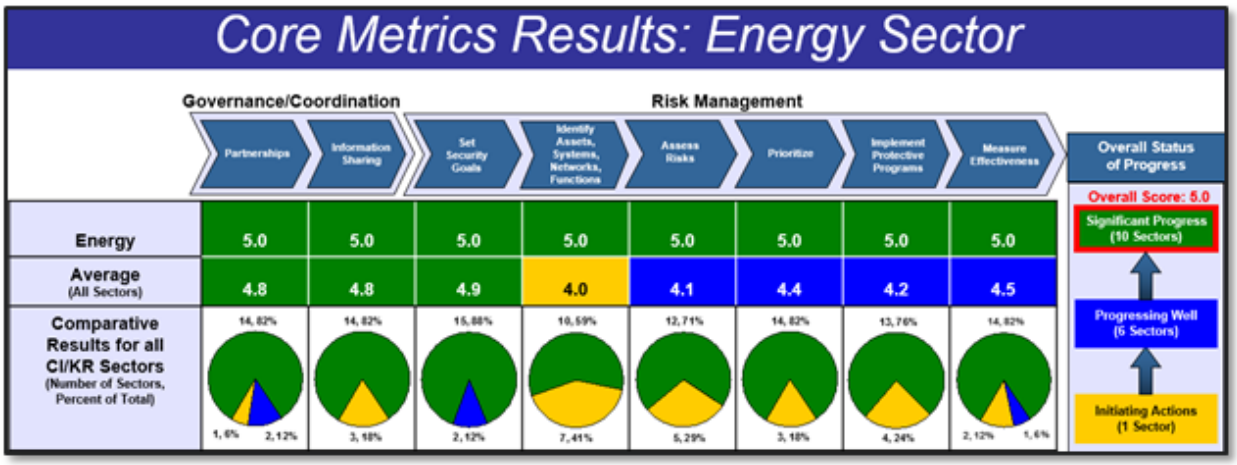

Figure 4.8. Core Metrics Results for the Energy Sector in the NIPP (DHS 2009)

4.5 Challenges

Some security data are available on a national level for the electric sector, but no single data set is derived from decades of data collection that can tell precisely what adversaries will do, how often they will do it, and how much it will cost the electric sector when they do it. Due to their sensitive nature, security data collected by the individual utilities are not publicly available.

Data that are publicly available for use in security metrics include the following:

- Historical data about electric outages due to vandalism, sabotage, and cyber incidents from Eaton's Blackout Tracker (Eaton 2016) and DOE Form OE-417 (DOE 2016a)
- U.S. Bureau of Justice crime statistics on property crime and burglary (DOJ 2016)

- U.S. Bureau of Labor Statistics data about the number of security guards at the state level, with potential for more location-granular data (DOL 2016)
- DHS ECIP data analysis for the 2015 DOE QER, which identified gaps in preparedness and rapid recovery measures for 273 surveyed energy facilities (DOE 2015b).

Discussions will be held with energy sector contacts to attempt to specify the source of the data needed for each proposed security metric, the frequency of data collection, and the spatial characteristics (national versus regional, state, utility, etc.). It will also be established who is responsible for raw data accuracy, data compilation into measurements, and calculation of each security metric.

The outcome of first-year activities would be the complete development of this approach to update the PMI using a revised version of the IST specific to the electric sector, including public data sets and default values for required inputs, which can be modified by electric utilities using site-specific information.

The vision for Years 2 and 3 would be the development of a spreadsheet, or potentially a Web-based dashboard tool, that could be publicly provided to the electric sector (Year 2) as well as the development of cyber security metrics and data (Years 2 and 3). Figure 4.9 shows an example dashboard showing physical security metrics.

Figure 4.9. Example PMI Dashboard for Consideration as Physical Security Metrics

4.6 Scope of Applicability

The primary users of this proposed approach for physical security metrics (the development of cyber security metrics will be addressed in the next phase of this project) would be the following:

- Utilities (for self-assessment)

- State PUCs (to assess the security posture of local utilities). Note that the development of state-level security metrics needs to be discussed further with the electric sector. There is generally a reluctance by electric utilities to share physical security information because of the inherent nature of the topic (i.e., making an electric utility more vulnerable to attack by giving out intelligence about its systems, weaknesses, monitoring methods, etc.). This may limit the potential application of the proposed approach to develop state-level security metrics scores.

4.6.1 Asset, Distribution, and Bulk Power Level

The PMI approach starts at the asset level and determines the PMI score for key assets, such as substations, control centers, and electric generation facilities.[1] The PMI approach was selected for physical security metrics development because a version of these metrics has been applied by DHS to more than 400 electric assets. The application of the PMI approach would address the lack of consistent information about the security posture of the electric sector.

The process described in Figure 4.3 will produce a revised PMI, specifically tailored toward electric sector infrastructure. Electric utilities that have not had DHS personnel conduct an IST survey could answer a select set of questions that would provide insight into their existing security posture. The revised set of questions will contain default values that would be determined using statistical analysis of the available IST data for electric sector components or publicly available data. The utility can then change those defaults and add additional information specific to their utility to get tailored PMI values for their assets, considering their threat environment.

As discussed in the previous section, the PMI is constituted by five Level 1 components, 25 Level 2 subcomponents, and 64 Level 3 subcomponents. Figure 4.10 provides a typical IST dashboard showing the calculated overall PMI and its five sub-metrics. The proposed approach is to develop a similar PMI dashboard for electric sector components that would focus on the five Level 1 components using IST answers to develop default values and/or public data sets.

[1] The NERC CIP-002 standard describes how utilities define critical assets, as well as critical "cyber" assets. Essentially, all bulk transmission assets are deemed critical, and utilities may designate additional assets as critical based on other factors. The first requirement under the CIP 014 standard is for utilities to identify transmission stations, substations, and control centers that—if rendered inoperable or severely damaged—could result in widespread instability, uncontrolled separation, or cascading failures within an interconnection.

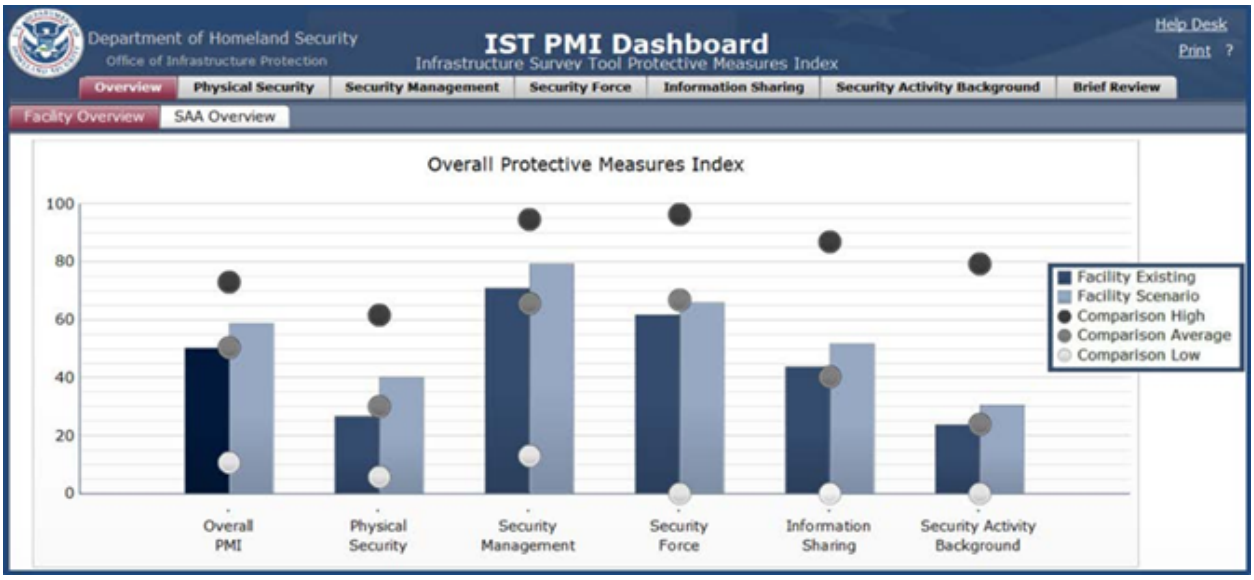

Figure 4.10. IST Dashboard showing Calculated PMI

For the PMI, the information collected characterizes the weakest protective measures (i.e., the weakest portion of fence if types and characteristics vary). Some of these values can be inferred from current industry practice (NERC and similar standards). IST summary information for typical electric sector responses, as provided by DHS, indicates that almost all electric substations have performed background checks, and contain fencing and gates, as shown in Figure 4.11 and Figure 4.12.

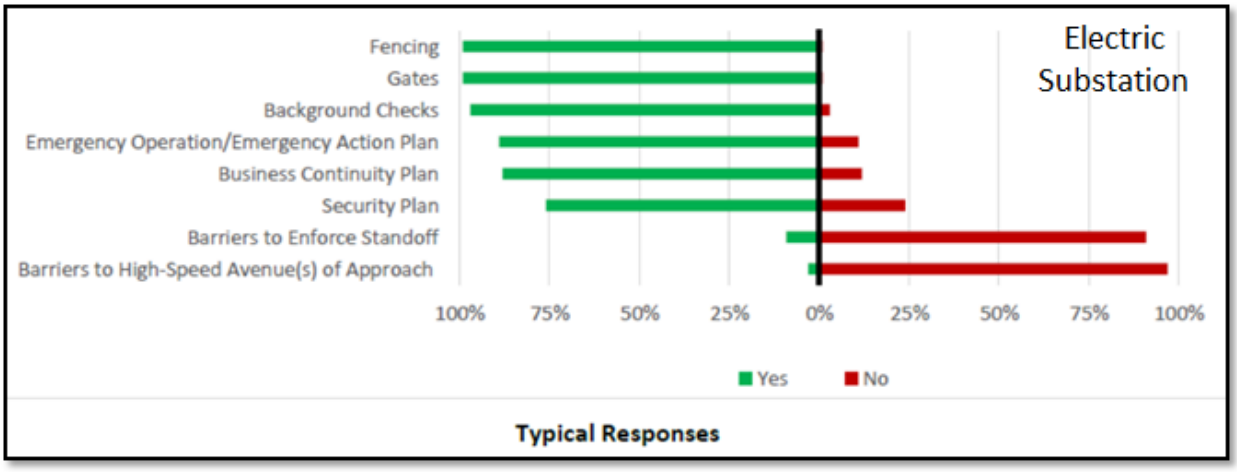

Figure 4.11. Typical Responses to IST Questions for Electric Substations

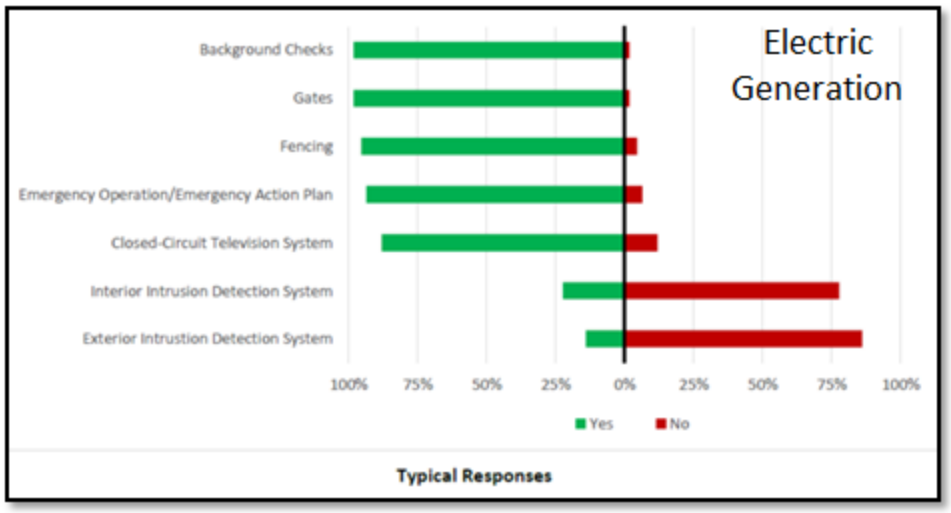

Figure 4.12. Typical Responses to IST Questions for Electric Generation Plants

The PMI requires information that may not be available from public data sources, such as MOUs/MOAs with local law enforcement and the characteristics of security forces. These gaps in publicly available data would be supplemented by analysis previously performed by Argonne to identify gaps in preparedness and rapid recovery measures for the QER using data collected for 170 electric facilities from January 2011 through September 2014 (DOE 2015d). The electric facilities considered in the previous Argonne analysis included transmission and distribution substations as well as control rooms and power plants, which are identified in the NERC CIP 014 standard as key physical assets and may be part of a utility's critical facility list (Shumard and Schneider 2014).

It can be expected that the current physical security posture of a given electric utility may depend on the following:

- Historical crime statistics
- Urban vs. suburban vs. rural locations of critical electric assets
- Prior incidents of vandalism and sabotage
- Instances of copper wire and electric equipment theft.

It is well known that substation design differs depending on its location; enclosed substations in urban areas typically are located within buildings (Figure 4.13), while open-air substations in rural areas are built without any secondary enclosure (Figure 4.14). The existence of any secondary enclosures, such as buildings, is a major physical security benefit that would be reflected in the PMI score for enclosed substations.

Figure 4.13. An Enclosed Substation (Note: Indoor Design Blends in with its Surroundings)

Figure 4.14. An Open-Air Substation (Note: Absence of Secondary Containment)

The proposed approach will investigate whether PMI scores for electric utilities correlate with historical crime statistics, prior incidents of vandalism and sabotage, and other physical security-related issues. The analysis will be limited to the electric sector facilities for which DHS IST data are readily available (more than 400 electric assets).

4.6.2 Utility Level

Overall PMI for a given electric utility would be the weighted sum of the PMIs for expensive hard-to-replace assets, such as substations, power plants, and control rooms, consistent with the approach in the NERC CIP 014, *Standard for Physical Security*. The approach would ignore assets such as transmission towers, which can be quickly and easily replaced and are assumed to be not as critical as long-lead–time equipment such as transformers in substations.

The overall PMI for an electric utility would account for the PMI scores of its critical assets, which are assumed to include the utility control center(s), distribution and transmission substations, and electric generation plants:

$$(PMI)_{utility} = \sum (n_j * IF_j * PMI_j) / \sum (n_j * IF_i)$$

where

(PMI)utility = the composite PMI score for the electric utility;
ni = the number of assets of category "i";
IFi = the importance factor of asset category "i" [an uniform IF of 1 would mean all assets are equally important];
PMIi = the PMI score for asset category "i".

The importance factor is a proxy for the consequence of the disruption or failure of a given electric asset and could be derived from the valuation or business interruption cost or the value of lost load typically attributed to that asset type. Research is currently under way to determine appropriate default values for these importance factors; one possible candidate is provided by the Federal Emergency Management Agency (FEMA) HAZUS approach for natural disaster modeling (FEMA 2018), as shown in Table 4.4. A user of this physical security metrics approach would have the option to revise the default values to those that more appropriately reflect the potential consequences of the loss or disruption of a given electric asset type for their electric utility.

Table 4.4. FEMA HAZUS Valuation of Various Electric Assets

Electric Asset	Size	FEMA Valuation	Normalized Value
Low Voltage Substation	34.5 to 150 kV	10,000	2
Medium Voltage Substation	150 to 350 kV	20,000	4
High Voltage Substation	> 350 kV	50,000	10
Small Power Plant	< 100 MW	100,000	20
Medium Power Plant	100 to 500 MW	500,000	100
Large Power Plant	> 500 MW	500,000	100
Control Room	---	5,000	1

Discussions with electric sector security personnel revealed that electric utilities protect their critical facilities with a greater degree of security, compared to electric assets whose disruption or failure have less significant consequences. The determination of the overall security posture of an electric utility would need to account for this dichotomy in security posture among electric assets. Table 4.5 shows an example calculation of the overall PMI for a generic utility composed of electric substations, generating plants, and control rooms; given a range of asset-level PMI values (ranging from 40 to 80), the utility-level PMI is estimated to have a value of 59.

Table 4.5. Example Calculation of the Protective Measures Index for a Generic Electric Utility

Electric Asset	Significance	Valuation	Number of Assets	Asset-Level PMI
Substation - outside	Higher	10	5	65
---	Lower	2	800	55
Substation - within structures	Higher	10	5	75
---	Lower	2	10	65
Power Plant - fossil fueled	Higher	50	10	75
---	Lower	10	15	70

Electric Asset	Significance	Valuation	Number of Assets	Asset-Level PMI
Power Plant - renewable	Higher	20	10	45
---	Lower	4	15	40
Electric Control Room	Higher	1	1	80
---	Lower	1	1	70
TOTAL	**---**	**---**	**---**	**59**

NOTE: the above values are examples only

Information about the number and characteristics of each utility's control center(s), distribution and transmission substations, and electric generation plants would be collected from the following sources:

- Electric utility control center data based on the location of the electric utility headquarters
- Electric substation data from Platts Electric Substation geospatial data layer (FEMA 2018)
- Electric generation plant data from the EIA-860, Annual Electric Generator Report, EIA-860M, Monthly Update to the Annual Electric Generator Report, and EIA-923, Power Plant Operations Report (EIA 2019a).

4.6.3 State Level

One potential approach to determining the overall PMI for a state would involve the PMI scores for the electric utilities located within the state, normalized by the number of electric utility customers:

$$(PMI)_{state} = \sum \{ (PMI)_{utility} * n_{customers} \} / \sum (n_{customers})$$

where $(PMI)_{state}$ is the composite PMI score for the electric utility sector in the state and $n_{customers}$ is the number of electric customers by utility in the state, as provided by EIA Forms EIA-861- Schedules 4A & 4D and EIA-861S (EIA 2019b).

Other approaches exist for determining the overall PMI for a state based on the PMI for each electric utility, such as normalizing using the following:

- The total capacity of each electric utility, as provided in Form EIA-826 (EIA 2017c)
- The total number of electric assets for each electric utility, as provided by EIA
- The total revenue of each electric utility, as provided by EIA Forms EIA-861- Schedules 4A & 4D and EIA-861S (EIA 2019c)
- The number of critical sites, such as healthcare facilities (hospitals and senior care centers), first responder (police and fire) stations, mass transit facilities, data centers, and wastewater treatment plants (FEMA 2013).

The most appropriate way to combine individual PMI scores for each electric utility into a composite PMI score for the electric sector in a state would be determined through consultation with electric sector subject matter experts. Preferences for the specific values for these weights would be determined via a formal elicitation process, and would account for factors such as variations in facility vulnerability between electric utilities. A sensitivity analysis would be performed to determine whether the weights are reasonable.

4.6.4 Regional Level

The proposed approach to determining the overall PMI at the regional level would involve the PMI scores for the electric utilities located within the region, similar to the approach proposed at the state level.

4.6.5 National Level

The proposed approach to determining the overall PMI at the national level would involve the PMI scores for the electric utilities located within the nation, similar to the approach proposed at the state level.

4.6.6 Other Level

The approach at this level is yet to be determined. The DHS PMI approach for physical security has been modified for use by Public Safety Canada and incorporated into the Canadian Critical Infrastructure Resilience Tool (CIRT), which is an onsite, survey-based tool that measures the resilience and protective measures of a facility, similar to the DHS PMI dashboard. The PMI uses a subset of the CIRT's variables to produce an estimate of a facility's protective measures and is derived from five components: physical security, security management, security force profile, information sharing, and security activity background (PSC 2018), as shown in Figure 4.15 (PSC 2016).

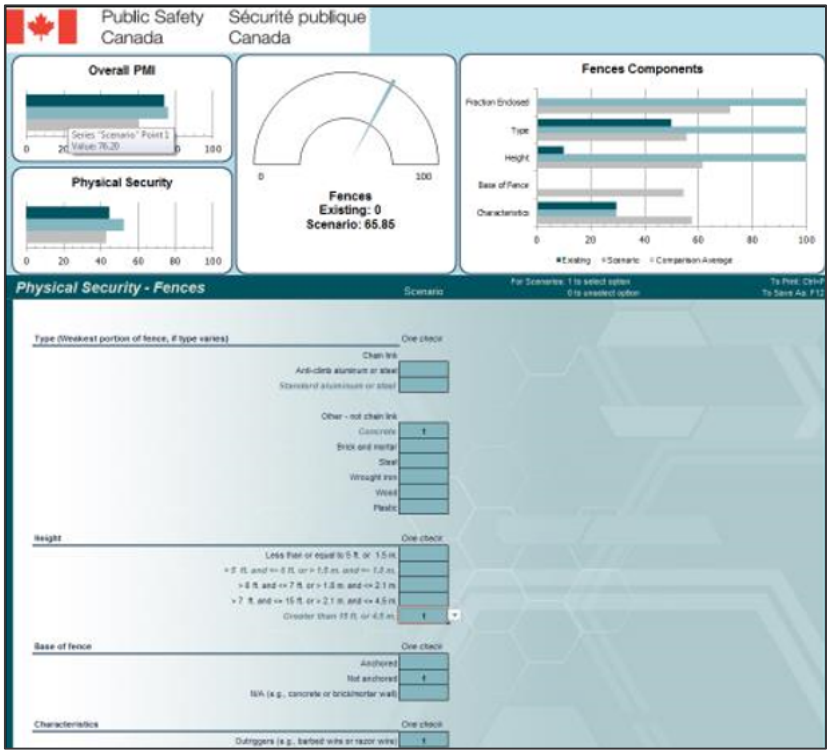

Figure 4.15. Canadian Critical Infrastructure Resilience Tool (CIRT)

The United States and Canada are currently working jointly on a Regional Resiliency Assessment Program (RRAP) project focusing on the shared electrical grid in the Northeast. By jointly assessing vulnerabilities, the countries can work together to address gaps and strengthen infrastructure in order to avoid large-scale failures in the future (DHS 2017). The demo physical security metrics tool developed

for use by U.S. electric utilities could be applied in Canada with a few modifications (such as including a French translation) to address vulnerability gaps in Canadian electric utilities.

4.7 Use Cases for Metrics

4.7.1 Smart Reconfiguration of Idaho Falls Power Distribution Network for Enhanced Quality of Service

The objective of the GMLC project titled "Smart Reconfiguration of Idaho Falls Power Distribution Network for Enhanced Quality of Service" is to identify existing technology and integration solutions/methods that could be applied to the Idaho Falls utility system, which relies on significant amounts of imported power to keep as much of the system operating as possible during system events at both the transmission and distribution levels. Improving physical security at Idaho Falls substations is something that is specifically called out (although with a focus on reducing the impact of any incidents via smart system design—e.g., islanding). There may be potential to use the PMI demo tool under development to estimate the composite PMI score for the Idaho Falls utility system; this would enable a broader understanding of the current physical security state and how proposed actions might improve it.

The physical security metrics team has contacted the GMLC project lead for the Idaho Falls GMLC activity to understand how the work being performed compares to what was originally scoped, including physical security, and whether there is interest in examining the physical security opportunity for the Idaho Falls utility system in greater depth. During the second and third years, no progress was made in the stakeholder relationship with Idaho Falls Power Company.

4.7.2 Commonwealth Edison

Exploratory discussions were held with security personnel at Commonwealth Edison (ComEd), which is the largest electric utility in Illinois and serves the Chicago and Northern Illinois area. ComEd provides electric service to more than 3.8 million customers across Northern Illinois; its service territory contains urban, suburban, and rural customers. It also contains transmission (69 to 765 kV), subtransmission (34.5 kV), and distribution (4.16 to 13.8 kV) substations.

This proposed use-case would provide a spreadsheet, or potentially a Web-based dashboard tool, that would contain electric facility data specific to ComEd and estimate the individual Level 1 and 2 components for review and comments. Discussions between Argonne and ComEd security personnel were held in early 2017 with the intention of determining the appropriate normalization method and importance factors specific to substations, control centers, and generating plants. DOE decided in April 2017 to halt all further development of physical security metrics and not to engage further with ComEd. When DOE decided to restart the physical security metrics project in mid-December 2017, ComEd personnel indicated that they were not interested in re-engagement.

4.7.3 Edison Electric Institute

EEI was contacted in early 2018 for its assistance in supporting the development of physical security metrics for the electric sector. EEI is the association that represents all U.S. investor-owned electric companies. Its members provide electricity for 220 million Americans, and operate in 50 states and the District of Columbia.

EEI provided valuable input in the determination of which electric assets could be considered critical to electric operations and suggestions about data availability. EEI also stated that they would be willing to present the proposed physical security metrics to their members for approval and guidance if and when a demo tool (showing how the overall PMI is calculated for a given electric utility) has been developed. This activity would determine the appropriate normalization method and importance factors specific to substations, control centers, and generating plants. The final outcome would be utility validation of the PMI approach for the electric sector, including assumptions, data, and default values.

4.7.4 Southern California Edison Company

Discussions with SCE security representatives started in August 2018. SCE, the largest subsidiary of Edison International, is the primary electricity supply company for much of Southern California. It provides 14 million people with electricity across a service territory of approximately 50,000 square miles. Its service territory is served by a total of 1,627 substations (SCE undated).

SCE stated during the discussions that the CPUC recently instituted a Risk Assessment Mitigation Phase (RAMP) plan that California regulated utilities have to complete (CPUC 2018). The RAMP is a trial case and it requires California regulated utilities to try to calculate the risk "buy-down" associated with various proposed physical security upgrades. As an example, if an investor-owned utility (IOU) in California gives more funds to one site than another, the "risk bin deficiency" would have to be calculated to support how physical security funds are being spent wisely.

One of the primary goals for the RAMP filings is to be able to compare risks against each other and determine how to prioritize projects in order to get the most risk reduction for money spent. Utilities such as SCE are attempting to determine the risk reduction associated with replacing existing substations with those located in buildings (as an example), and a tool is needed to estimate the security posture of substations in buildings, versus outside, as a means of estimating the potential risk reduction.

SCE stated that a tool is needed to estimate physical security metrics for this RAMP process, and "SCE is very happy to apply a DHS-approved approach that has been modified by a national lab," because they believed it would find easier approval by the CPUC.

The specific characteristics of the physical security metrics tool that would be most useful to SCE are as follows:

- The tool would have to consider multiple threat streams (not just one DBT) and it would have to allow variation/change in protective measures to see how these changes impact the predicted PMI score.
- The tool would have to estimate a physical security metric for the entire utility based on the physical security characteristics of its electric facilities. The demo tool approach would be used to perform this calculation, but would allow an electric utility, such as SCE, to modify the default weighting factors of "critical" versus "non-critical" facilities to those appropriate to SCE.
- The tool would have to distinguish between assets "critical to SCE operations" versus the others. It was stated that SCE has a handful of "critical" substations with many protective measures, and about 900 other substations with similar, lower-scale physical security attributes. The demo physical security tool was modified to accommodate the assessment of "critical" versus the remainder of electric assets.

The demo physical security metrics tool was modified during its development to make it more useful and usable by SCE.

4.8 Value of Metrics

Based on engagements with stakeholders, the following specific values were reported:

- The DHS IP Assessments Team from the DHS Office of Infrastructure Protection (IP) stated that DOE's "grid security metrics efforts" are "examples of opportunities for DHS IP assessments to contribute to DOE efforts."
- In an initial discussion describing the methodology, NARUC staff indicated that such a comparative scale could be useful in providing utility commissions with an understanding of the relative physical security posture of the utilities within their jurisdictions, and the relative impact of potential investments designed to improve physical security, without requiring the utilities to share potentially sensitive data. A follow-up engagement with NARUC's critical infrastructure resources staff subcommittee is being planned.

4.9 Feedback from Stakeholders Regarding Year 1 Outcomes

This section summarizes the feedback the research team received from domain experts regarding the outcome of the Year 1 sustainability metrics definitions, the relevance to the community's needs, and the overall value of monitoring progress as the grid evolves.

The following reflections stem from a briefing to domain experts who offered to review the team's Year 1 results. The reviewers represented DHS, EEI, EPRI, and NASEO. The following is a synopsis of the key points made during the 1.5-hour briefing:

- Technical considerations:
  - The aggregation of multiple indicators representing detailed information about the security posture may not be meaningful because an aggregated indicator masks the higher detailed information. Presenting both the sub-indicators that make up the PMI as well as the PMI was suggested.
  - One reviewer suggested providing as much transparency as possible about the underlying assumptions of security measures that were considered in the formulation of the approach and tool development.
- Value of work – Reviewers generally saw that the approach could provide value to an electric utility and regulators and state energy offices in the following respects:
  - The metrics approach was viewed as useful for utilities to better understand the relative strength of their physical security posture as well as how they compare to that of their peers.
  - The metric approach could be useful for identifying strategies to improve specific physical security practices within their organization.
  - Information derived from the developed approach could be useful for informing rate recovery decisions with or without consideration of the peer comparisons.
  - General concern was expressed about the appropriateness of using the method for peer comparison or even presenting geographically aggregated protected measures index values. This concern in part stemmed from prior experience where some reviewers have seen metrics for other projects be used to create unfair judgments among and between entities that could lead to inappropriate policies.

– The reviewers also recognized challenges associated with protecting the electric utility completed data.

5.0 Next Steps

Possible next steps after the third year of this GMLC project include the following:

- Demo the Excel-based approach for physical security metrics with EEI by providing results for an actual (not fictitious) electric utility (i.e., specifying the number of control centers, substations, and generating plants based on public data). This would require an electric utility to allow the demo tool to be applied to their current physical security situation.
- Estimate default values of the importance factor in the physical security metrics approach, which accounts for the relative significance of a given electric component (control center versus substation versus generating plant) to the overall operations of an electric utility. Currently, default values are taken from the FEMA HAZUS tool. However, one possible activity would be to examine the DHS IST database and statistically determine more appropriate values based on electric sector surveys. This analysis would determine whether different utility types (municipals, cooperatives, IOUs) view their electric sector assets differently (which would result in importance factors that vary based on utility type).
- Convert the Excel-based approach developed by this GMLC1.1 project into a Web-based tool similar to the DHS Infrastructure Survey Dashboard (DHS undated) (see Figure 4.10); this would be an interactive dashboard providing an overview of an electric utility's security posture, identifying potential areas of concern, and allowing users to explore the impacts of potential improvements to their physical security status.
- Further engagement with the electric sector (potentially through APPA, National Rural Electric Cooperative Association [NRECA], and the California IOUs) to determine whether other electric asset types (e.g., private microwave networks, transmission towers, etc.) could be included in the physical security metrics approach (the current approach neglected these asset types because they are generally not surveyed by DHS).
- Perform outreach to state PUCs and public service commissions to update the electric utility-specific approach developed for physical security metrics to apply state-wide, leveraging physical security metrics data for electric utilities within a state as a means of predicting the overall physical security posture of the electric sector in that state.
- Include unit cost data for physical security upgrades to allow users of the Web-based dashboard to explore the cost impacts of potential improvements to their physical security status.

If additional funding for long-term security metrics development is unavailable from DOE, it may be possible that the next steps could be supported by DHS; discussions would be needed with the appropriate DHS personnel to confirm this possibility.

6.0 References

Argonne (Argonne National Laboratory). 2013. *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*. Available at http://www.ipd.anl.gov/anlpubs/2013/11/77931.pdf, accessed June 27, 2016.

ASIS 2012. "Protection of Assets: Physical Security." Available at https://www.asisonline.org/publications/protection-of-assets-physical-security/, accessed March 7, 2019.

Bakshi A, Ahmad K, & Kimar N. 2011. "Security Metrics: Needs and Myths," *International Transactions in Mathematical Sciences and computers*, January-June 2011, Volume 4, No. 1, pp. 31–40 (available at https://www.researchgate.net/publication/262685082_Security_Metrics_Needs_and_Myths).

Biringer B, Vugrin E, & Warren D. 2013. Critical Infrastructure System Security and Resilience. Boca Raton: CRC Press.

Brinkman B, Chen C, O'Donnel A, & C Parkes. 2015. *Regulation of Physical Security for the Electric Distribution System*. Recommendation document to California Public Utility Commission, February, 2015. Available at https://pdfs.semanticscholar.org/e11b/21010c0fa8e68d0958496bc3564c50524c63.pdf, accessed March 21, 2017.

Brotby WK. 2009. "Security Metrics Overview." Available at http://www.infosectoday.com/Articles/Security_Metrics_Overview.htm, accessed March 17, 2017.

CA Legislative Assembly, SB-699 – Public Utilities: Electrical Corporations, 2013-2014. Available at http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB699, accessed March 21, 2017.

Congressional Research Service (CRS). 2018. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* available at https://fas.org/sgp/crs/homesec/R45135.pdf, accessed on November 15, 2018.

CPUC (California Public Utilities Commission). 2018. "Utility Risk Assessment and Safety Advisory," available at http://www.cpuc.ca.gov/riskassessment/, accessed on November 15, 2018.

Critical Infrastructure Information Act of 2002. 6 U.S.C. 131 – 134, subtitle B of Title II of the Homeland Security Act (P.L. 107-296, 116 Stat. 2135, sections 211 - 215)

CRS (Congressional Research Service). 2018. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* available at https://fas.org/sgp/crs/homesec/R45135.pdf, accessed on November 15, 2018.

DHS (Department of Homeland Security). 2009. *National Infrastructure Protection Plan, Partnering to enhance protection and resiliency*. Available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed June 27, 2016.

DHS (Department of Homeland Security). 2015a. *Facility Security Plan: An Interagency Security Committee Guide* (February 2015/1st Edition). Available at https://www.dhs.gov/publication/isc-facility-security-plan-guide, accessed March 7, 2019.

DHS (Department of Homeland Security). 2015b. "Critical Infrastructure Vulnerability Assessments." Available at https://www.dhs.gov/critical-infrastructure-vulnerability-assessments, accessed June 27, 2016.

DHS (U.S. Department of Homeland Security). 2017. "Beyond the Border U.S. Fact Sheet." Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwiHnIy0zNbeAhUqw4MKHSasCJcQFjADegQICRAC&url=https%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2Fpublications%2F2017%25201%252019%2520BTB%2520Fact%2520Sheet.pdf&usg=AOvVaw33x2MlCmQmO57GnCgtw2Hq, accessed November 15, 2018.

DHS (Department of Homeland Security). Undated. "Infrastructure Survey Tool." Available at https://www.dhs.gov/cisa/infrastructure-survey-tool, accessed March 7, 2019.

DOE (U.S. Department of Energy). 2014. "Cybersecurity Capability Maturity Model (C2M2) Frequently Asked Questions." Available at https://energy.gov/sites/prod/files/2014/02/f7/C2M2-FAQs.pdf, accessed March 21, 2017.

DOE (U.S. Department of Energy). 2015a. *Grid Modernization Multi-Year Program Plan*, November, 2015. Accessed online at: https://energy.gov/downloads/grid-modernization-multi-year-program-plan-mypp.

DOE (U.S. Department of Energy). 2015b. *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*. Available at http://energy.gov/sites/prod/files/2015/07/f24/QER%20Full%20Report_TS%26D%20April%202015_0.pdf, accessed June 27, 2016.

DOE (U.S. Department of Energy). 2015c. *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, "Vulnerabilities of Energy TS&D and Shared Infrastructures to Physical Attack," available at https://energy.gov/sites/prod/files/2015/07/f24/QER%20Full%20Report_TS%26D%20April%202015_0.pdf, accessed January 26, 2017.

DOE (U.S. Department of Energy). 2015d. *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. Available at https://www.energy.gov/policy/downloads/quadrennial-energy-review-first-installment, accessed on November 16, 2018.

DOE (U.S. Department of Energy). 2015e. *Quadrennial Technical Review*. Accessed January 23, 2017 at https://energy.gov/under-secretary-science-and-energy/quadrennial-technology-review-2015

DOE (U.S. Department of Energy). 2015f. *The Quadrennial Energy Review (QER)*. Available at https://www.energy.gov/policy/initiatives/quadrennial-energy-review-qer, accessed on November 15, 2018.

DOE (U.S. Department of Energy). 2016b. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)." Available at http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity, accessed June 27, 2016.

DOJ (U.S. Department of Justice). 2016. "Uniform Crime Reporting Statistics." Available at http://www.ucrdatatool.gov/, accessed June 27, 2016.

DOL (U.S. Department of Labor). 2016. "Occupational Employment and Wages, May 2015, 33-9032 Security Guards." Available at http://www.bls.gov/oes/current/oes339032.htm, accessed June 27, 2016.

Eaton (Eaton Corporation plc). 2016. "Blackout and Power Outage Tracker." Available at http://powerquality.eaton.com/blackouttracker/default.asp?wtredirect=www.eaton.com/blackouttracker, accessed June 27, 2016.

EIA (Energy Information Administration). 2017a. "2015 Utility Bundled Retail Sales- Total," available at http://www.eia.gov/electricity/sales_revenue_price/xls/table10.xlsx, accessed January 25, 2017.

EIA (Energy Information Administration). 2017b. "Layer Information for Interactive State Maps – Power Plants," available at http://www.eia.gov/maps/map_data/PowerPlants_US_EIA.zip, accessed January 25, 2017.

EIA (Energy Information Administration), 2019a. "Layer Information for Interactive State Maps – Power Plants," available at http://www.eia.gov/maps/map_data/PowerPlants_US_EIA.zip, accessed January 25, 2019.

EIA (Energy Information Administration), 2019b. "2015 Utility Bundled Retail Sales- Total," available at http://www.eia.gov/electricity/sales_revenue_price/xls/table10.xlsx, accessed January 25, 2019.

EIA (Energy Information Administration). 2019c. "Form EIA-826 detailed data," available at http://www.eia.gov/electricity/data/eia826/, accessed January 25, 2019.

EIA 2019d. "2015 Utility Bundled Retail Sales- Total," available at http://www.eia.gov/electricity/sales_revenue_price/xls/table10.xlsx, accessed January 25, 2019.

EPRI (Electric Power Research Institute). 2016a. "Creating Security Metrics for the Electric Sector, Version 2," available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002007886, accessed March 17, 2017.

FEMA (Federal Emergency Management Agency). 2003. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. Accessed online at: https://www.fema.gov/media-library/assets/documents/2150.

FEMA (Federal Emergency Management Agency). 2005. *A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*. Accessed online at: https://www.fema.gov/media-library/assets/documents/4608.

FEMA (Federal Emergency Management Agency). 2013. *Performance of Critical Facilities and Key Assets*, available at https://www.fema.gov/media-library-data/1385587199555-ebd60a9506168b4fd5a79ee519520c1e/Sandy_MAT_Ch5_508post.pdf, accessed on March 18, 2017.

FEMA (Federal Emergency Management Agency). 2018. "Hazus Technical and User's Manuals," available at https://www.fema.gov/media-library/assets/documents/24609, accessed on November 15, 2018.

Fisher R & Norman M. 2010. Developing measurement indices to enhance protection and resilience of critical infrastructures and key resources. *Journal of Business Continuity* 191–206.

Freedom of Information Act or 1967. 5 U.S.C. ch. 5, subch. II § 552

Interagency Security Committee. 2010. Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard.

Jaquith A. 2007. Security Metrics: Replacing Fear, Uncertainty and Doubt, Pearson Education, Inc., Upper Saddle River, NJ.

NASEO (National Association of State Energy Officials). 2014. *Infrastructure Protection Gateway, Rapid Survey Tool*. Aavailable at http://www.naseo.org/Data/Sites/1/events/riskworkshop/rapid-survey-tool_12-17-2014.pdf, accessed June 27, 2016.

NERC (North American Electric Reliability Corporation). 2011. *Security Guideline for the Electricity Sector: Physical Security*. Available at http://www.nerc.com/docs/cip/sgwg/Physical%20Security%20Guideline%202011-10-21%20Formatted.pdf, accessed April 25, 2017.

NERC (North American Electric Reliability Corporation). 2015. *Bulk Electric System Security Metrics Working Draft*. Available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf, accessed June 27, 2016.

NIST (National Institute of Standards and Technology). 2017. "NVD CVSS Support." Available at https://nvd.nist.gov/vuln-metrics/cvss. Accessed on March 29, 2017

Norman MA. 2015. *Infrastructure Information Collection Division*. Available at http://www.nrc.gov/docs/ML1532/ML15329A121.pdf, accessed June 27, 2016.

Obama B. 2013. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, Washington, D.C. (https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

PSC (Public Safety Canada). 2018. "Regional Resilience Assessment Program: Frequently Asked Questions," available at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/rrap-faq-en.aspx, accessed November 15, 2018.

PSC (Public Safety Canada). 2016. Regional Resilience Assessment Program and Critical Infrastructure Assessments Tools, available at http://www.cwwa.ca/pdf_files/2016Maciek%20Hawrylak.pdf, accessed November 14, 2018.

SCE (Southern California Edison Company). undated. Local Capacity Area Substation List July 2011, available at https://www.sce.com/wps/wcm/connect/f74056f1-d533-4810-9050-ec4bdf9bf287/SCE_LocalCapacityAreaSubstationList.pdf?MOD=AJPERES, accessed at November 15, 2018.

Seger KA. 2003. *Utility Security, The New Paradigm*. PennWell Corporation, Tulsa, Oklahoma.

Shumard R & S. Schneider. 2014. "Utility Security: Understanding NERC CIP 014 Requirements and Their Impact," *Electric Energy Online*, available at http://www.electricenergyonline.com/show_article.php?mag=100&article=813, accessed March 18, 2017.

Taft J & Becker-Dippmann A. 2014. *Grid Architecture.* PNNL-24044, Pacific Northwest national Laboratory, Richland, Washington. Accessed online at: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24044.pdf.

White House. 2013. "Presidential Policy Directive – Critical Infrastructure Security and Resilience." Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed on November 15, 2018.

Zalewski J, Drager S, McKeever W, & Kornecki A.J., 2014. "Measuring Security: A Challenge for the Generation." Available at https://pdfs.semanticscholar.org/b06c/9d1f7bab97d7ac7c22c2d4d392cdea33b5fa.pdf.

Appendix A

Metrics Inventory

Appendix A

Metrics Inventory

A.1 Security

A.1.1 Data

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classification** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available?** (Yes/No)	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
1	Electricity	Security	All	Physical Security	Accounts for presence of physical security measures such as fences, gates, etc.	Documents utility's current Critical Infrastructure and Key Resources (CIKR) protection posture and overall security awareness	0 to 100%	Numerical	Process	Account-ability	Utility	State regulator	Lagging	YES	YES (public & DHS)	Distribution system footprint	Annual	Argonne National Laboratory, 2009. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, available at http://www.ipd.anl.gov/anlpubs/2009/10/65406.pdf	
2	Electricity	Security	All	Security Force	Staffing, equipment, weaponry, training, patrols, after hour security, etc.	Documents utility's current CIKR protection posture and overall security awareness	0 to 100%	Numerical	Process	Account-ability	Utility	State regulator	Lagging	YES	YES (public & DHS)	Distribution system footprint	Annual	Argonne National Laboratory, 2009. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, available at http://www.ipd.anl.gov/anlpubs/2009/10/65406.pdf	
3	Electricity	Security	All	Security Management	Business continuity plan, security plan, threat levels, background checks, etc.	Documents utility's current CIKR protection posture and overall security awareness	0 to 100%	Numerical	Process	Account-ability	Utility	State regulator	Leading	YES	YES (public & DHS)	Distribution system footprint	Annual	*Argonne National Laboratory, 2009. Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, available at http://www.ipd.anl.gov/anlpubs/2009/10/65406.pdf	
4	Electricity	Security	All	Information Sharing	Threat sources and information sharing mechanisms	Documents utility's current CIKR protection posture and overall security awareness	0 to 100%	Numerical	Process	Account-ability	Utility	State regulator	Leading	YES	YES (public & DHS)	Distribution system footprint	Annual	Argonne National Laboratory, 2009. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, available at http://www.ipd.anl.gov/anlpubs/2009/10/65406.pdf	
5	Electricity	Security	All	Security Activity History/ Background	New protective measures, random security measures, etc.	Documents utility's current CIKR protection posture and overall security awareness	0 to 100%	Numerical	Process	Account-ability	Utility	State regulator	Lagging	YES	YES (public & DHS)	Distribution system footprint	Annual	Argonne National Laboratory, 2009. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, available at http://www.ipd.anl.gov/anlpubs/2009/10/65406.pdf	
6	Electricity	Security	All	BES Security Metric 1: Reportable Cyber Security Incidents	The number of reportable cyber security incidents that result in a loss of load, summed on a quarterly basis; this is a lagging metric	Describes how prepared the electric sector is to a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	NERC		Lagging	NO	YES (from NERC)	National	Quarterly	NERC, 2015. *Bulk Electric System Security Metrics Working Draft*, available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf	This metric is applied at the national level and there is insufficient public data for its application at the utility or state level.

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available?** (Yes/No)	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
7	Electricity	Security	All	BES Security Metric 2: Reportable Physical Security Events	The number of physical security reportable events that occur over time as a result of threats to a facility or BES control center or damage or destruction to a facility, summed on a quarterly basis; this is a lagging metric	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	NERC		Lagging	NO	YES (from NERC)	National	Quarterly	NERC, 2015. *Bulk Electric System Security Metrics Working Draft*, available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf	This metric is applied at the national level and there is insufficient public data for its application at the utility or state level.
8	Electricity	Security	All	BES Security Metric 3: ES-ISAC Membership	The number of ES-ISAC member organizations, summed on a quarterly basis; this is a leading metric	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Decision-making	NERC		Leading	NO	YES (from NERC)	National	Quarterly	NERC, 2015. *Bulk Electric System Security Metrics Working Draft*, available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf	This metric could be applied at the utility level.
9	Electricity	Security	All	BES Security Metric 4: Industry-Sourced Information Sharing	The number of ES-ISAC Incident Bulletins (currently known as Watchlist entries), summed on a quarterly basis; this is a leading metric	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Decision-making	NERC		Leading	NO	YES (from NERC)	National	Quarterly	NERC, 2015. *Bulk Electric System Security Metrics Working Draft*, available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf	This metric is applied at the national level and there is insufficient public data for its application at the utility or state level.
10	Electricity	Security	All	BES Security Metric 5: Global Cyber Vulnerabilities	The number of global cyber vulnerabilities with a CVSS (Common Vulnerability Scoring System, NIST 2015) of 7 or higher; this is a lagging metric	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	NERC		Lagging	NO	YES (from NERC)	National	Quarterly	NERC, 2015. *Bulk Electric System Security Metrics Working Draft*, available at http://www.nerc.com/comm/CIPC/Bulk%20Electric%20System%20Security%20Metrics%20Working%20G1/BES_Security_Metrics_CIPC_March_2015.pdf	This metric is applied at the national level and there is insufficient public data for its application at the utility or state level.
11	Electricity	Security	Distribution	Number of instances of copper theft	Tracks the impact of copper theft and vandalism	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metrics depends on proprietary utility data that are difficult to collect.
12	Electricity	Security	Distribution	Number of successful or unsuccessful intrusion or attack	This metric captures the total number of attacks against a given utility's facilities	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metrics depends on proprietary utility data that are difficult to collect.
13	Electricity	Security	Distribution	Number of false or nuisance alarms	Collection of the number of non-attack-related incidents for a given utility	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
14	Electricity	Security	Distribution	Condition of all monitoring equipment	The number of times that the security system is unable to respond and detect a physical security incident	Describes how prepared the electric sector is for a physical attack.	Qualitative	Qualitative	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available? (Yes/No)**	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
15	Electricity	Security	Distribution	Performance of security personnel in training exercises and on tests	Describes how prepared the electric sector is for a physical attack	Describes how prepared the electric sector is for a physical attack.	Qualitative	Qualitative	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
16	Electricity	Security	Distribution	Number of problems found with condition of deterrence and monitoring measures	Describes how prepared the electric sector is for a physical attack	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
17	Electricity	Security	Distribution	Number of instances of vandalism or graffiti	Tracks the impact of copper theft and vandalism	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
18	Electricity	Security	Distribution	Number of problems with access control	Identifies the number of times that an intruder tries to access electric sector facilities for a given utility	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
19	Electricity	Security	Distribution	Number of malfunctions of security equipment or camera coverage	The number of times that the security system is unable to respond and detect a physical security incident	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary utility data	Utility	Monthly	CPUC, 2015. *Regulation of Physical Security for the Electric Distribution System*, available at http://www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf	This metric depends on proprietary utility data that are difficult to collect
20	Electricity	Security	All	Incidents requiring manual cleanup	Number of incidents requiring manual cleanup	Describes how prepared the electric sector is for a cyber attack.		Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
21	Electricity	Security	All	Mean-Time-to-Fix (MTTF)	Mean-Time-to-Fix (MTTF)	Describes how prepared the electric sector is for a cyber attack.	≥0 (dimensionless)	Numerical	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
22	Electricity	Security	All	Cyber Security Workforce Management	Cyber Security Workforce Management	Describes how prepared the electric sector is for a cyber attack.	N/A	Qualitative	Process	Decision-making	Utility	State regulator	Leading	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
23	Electricity	Security	All	Mean Cost to Mitigate Vulnerabilities	Mean Cost to Mitigate Vulnerabilities	Describes how prepared the electric sector is for a cyber attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available?** (Yes/No)	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
24	Electricity	Security	All	Percent of Changes with Security Review	Percent of Changes with Security Review	Describes how prepared the electric sector is for a cyber attack.	≥0 (dimensionless)	Numerical	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
25	Electricity	Security	All	Number of outgoing viruses caught at gateway	Number of outgoing viruses caught at gateway	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
26	Electricity	Security	All	Mean Time to Incident Discovery	Mean Time to Incident Discovery	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
27	Electricity	Security	All	Number of cyber security skills mastered per employee	Number of cyber security skills mastered per employee	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
28	Electricity	Security	All	Mean Time between Security Incidents	Mean Time between Security Incidents	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
29	Electricity	Security	All	Cost of Incidents	Cost of Incidents	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
30	Electricity	Security	All	Percentage of Systems without Known Severe Vulnerabilities	Percentage of Systems without Known Severe Vulnerabilities	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
31	Electricity	Security	All	Mean Time to Patch	Mean Time to Patch	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
32	Electricity	Security	All	Percentage of Changes with Security Exceptions	Percentage of Changes with Security Exceptions	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available?** (Yes/No)	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
33	Electricity	Security	All	Percentage of Applications Subject to Risk Assessment	Percentage of Applications Subject to Risk Assessment	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Account-ability	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
34	Electricity	Security	All	Information Security Budget Allocation	Information Security Budget Allocation	Under investigation by EPRI	≥0 (dimensionless)	Numerical	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
35	Electricity	Security	All	Compliance or Coverage of Information Security Practice	Compliance or Coverage of Information Security Practice	Under investigation by EPRI	NA	Qualitative	Process	Decision-making	Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Monthly	EPRI, 2015. *Creating Security Metrics for the Electric Sector*, available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005947	This metric depends on proprietary utility data that are difficult to collect
36	Electricity	Security	All	Number of protective programs implemented in a given year	Number of protective programs implemented in a given year	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Federal (DHS), Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
37	Electricity	Security	All	Level of investment of protective programs	Level of investment of protective programs	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Federal (DHS), Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
38	Electricity	Security	All	Number of detection systems installed at facilities	Number of detection systems installed at facilities	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Federal (DHS), Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
39	Electricity	Security	All	Proportion of facility's workforce that has completed security training	Proportion of facility's workforce that has completed security training	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Process	Account-ability	Federal (DHS), Utility	State regulator	Lagging	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
40	Electricity	Security	All	Level of response to a data call for asset information	Level of response to a data call for asset information	Describes how prepared the electric sector is for a physical attack.	N/A	Qualitative	Process	Decision-making	Federal (DHS), Utility	State regulator	Leading	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
41	Electricity	Security	All	Reduction of risk from one year to another	Reduction of risk from one year to another	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Outcome	Decision-making	Federal (DHS), Utility	State regulator	Leading	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available?** (Yes/No)	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
42	Electricity	Security	All	Overall risk mitigation achieved nationally	Overall risk mitigation achieved nationally	Describes how prepared the electric sector is for a physical attack.	≥0 (dimensionless)	Numerical	Outcome	Decision-making	Federal (DHS), Utility	State regulator	Leading	NO	Proprietary company data	Company-level	Annual	DHS, 2006. *National Infrastructure Protection Plan*, available at https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf	This metric depends on proprietary utility data that are difficult to collect
43	Electricity	Security	All	Risk Management	Considers actions to (1) establish cybersecurity risk management strategy, (2) manage cybersecurity risk, (3) management activities	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Lagging	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
44	Electricity	Security	All	Asset, Change, and Configuration Management	Considers actions to (1) manage asset inventory, (2) manage asset configuration, (3) manage changes to assets, (4) management activities	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Lagging	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
45	Electricity	Security	All	Identity and Access Management	Addresses (1) establish and maintain identities, (2) control access, (3) management activities	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
46	Electricity	Security	All	Threat and Vulnerability Management	Addresses activities to (1) identify and respond to threats, (2) reduce cybersecurity vulnerabilities, (3) management activities	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
47	Electricity	Security	All	Situational Awareness	Considers actions to (1) perform logging, (2) perform monitoring, (3) establish and maintain a common operating picture	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
48	Electricity	Security	All	Information Sharing and Communi-cations	Addresses actions to (1) share cybersecurity information, (2) management activities	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
49	Electricity	Security	All	Event and Incident Response, Continuity of Operations	Considers activities to (1) detect cybersecurity events, (2) escalate cybersecurity events and declare incidents, (3) respond to incidents and escalated cybersecurity events, (4) plan for continuity	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
50	Electricity	Security	All	Supply Chain and External Dependencies Management	Addresses activities to (1) identify dependencies, (2) manage dependency risk	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect

	Categorization			Summary				Attributes							Historical Supporting Data - Lagging Metrics			Citations and Issues	
Metric #	**Sector**	**Category** *(from list)*	**Electric System Infrastructure Component** *(from list)*	**Metrics Name**	**Description**	**Motivation**	**Units**	**Metric Type** *(from List)*	**Metric Classifi-cation** *(from List)*	**Metric Use** *(from List)*	**Primary User** *(from List)*	**Secondary User** *(from List - if applicable)*	**Metrics Tense** *(Lagging/ Leading)*	**Applicable to Valuation Project** *(Yes/No)*	**Data Available? (Yes/No)**	**Geospatial Resolution** *(from list)*	**Temporal Frequency of Data Reporting** *(from list)*	**Citation/Data Source Reference #**	**Potential Issues** **Comments**
51	Electricity	Security	All	Workforce Management	Considers actions to (1) assign cybersecurity responsibilities, (2) control the workforce life cycle, (3) develop cybersecurity workforce, (4) increase cybersecurity awareness	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect
52	Electricity	Security	All	Cybersecurity Program Management	Evaluates actions to (1) establish cybersecurity program strategy, (2) sponsor cybersecurity program, (3) establish and maintain cybersecurity architecture, (4) perform secure software development	Describes how prepared the electric sector is for a cyber attack.	MIL1 to MIL3	Qualitative	Process	Account-ability	Utility		Leading	NO	Proprietary company data	Company-level	Annual	DOE, 2014. *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), available at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf	This metric depends on proprietary utility data that are difficult to collect

http://gridmodernization.labworks.org/