Fall 2023

Cybersecurity Policy Rubric and Analysis for the State of Maine Electrical Transmission Grid

Benjamin Plummer M.S.

Cybersecurity Policy Rubric and Analysis for the State of Maine Electrical Transmission Grid

By

Benjamin Plummer

B.A. (University of Southern Maine) 2017

M.S. (University of Southern Maine) 2023

A THESIS

Presented to the Affiliated Faculty of

The College of Science, Technology, and Health

At the University of Southern Maine

In Partial Fulfillment of Requirements

For the Degree of Master of Cybersecurity

Portland & Gorham, Maine

October 16, 2022

Abstract

The State of Maine's (SOM) electrical grid is aging. While there are public and private efforts to bring it up to date, gaps in cybersecurity policies and laws exist (NERC, n.d.; see also MPUC, n.d.; CISA, n.d.). This policy and law research may also apply to other states and the protection of their critical infrastructure. The researcher examined the grid's controls, policies, and laws to determine the influence each exerts over the grid and where that influence presents vulnerabilities in security. The research focused on the controls, policies, and laws that play a role in protecting the grid. The researcher created and analyzed each procedure, approach, and regulation against a NIST five-function framework merged with the MITRE Adversarial Tactics, Aspects, and Common Knowledge (ATT&CK) model to observe and analyze what gaps or policies lack effectiveness or present risk (MITRE ATT&CK®. n.d.). The researcher utilized publicly available data and information from participating government agencies to discover and analyze current public policy regarding the cybersecurity of the State of Maine (SOM) Electrical Transmission Network. The study's results present numerous policies designed around the NIST recommendations. These policies are robust and work against most adversarial strategies. These policies are compared against the Center of Information Security's (CIS) Critical Control list to find any controls that the current policies and procedures have not covered. The researcher used the merged matrix to analyze each relevant policy from the SOM Office of Information Technology (OIT). The researcher designed the rubric to be improved and utilized to view policy from the perspective of the attacker in an efficient manner.

Table of Contents

CHAPTER 1 1
Introduction 1
Electrical Grid Overview 2
Research Questions 5
Conceptual Framework 5
Scope 5
Significance 6
CHAPTER 2 7
LITERATURE REVIEW 7
Laws, Policies, and Procedures 7
Conceptual framework 11
CHAPTER 3 15
METHODOLOGY 15
Stakeholders 15
Data 16
Analysis 20
Limitations 22
Pilot Study 23
CHAPTER 4 26
RESULTS 26
Analysis 26
Presentation of Results 26
CHAPTER 5 29
CONCLUSION 29
Introduction 29
Interpretation of findings 29
Implications 30
Recommendations for Action 30
Recommendations for further study 31
Conclusion 31
References 33

CHAPTER 1

Introduction

In today's highly connected world, with an increasingly sophisticated cyber threat, it is unrealistic to assume energy delivery systems are isolated or immune from compromise (Xue et al., 2022, 2.2). Cyber-attacks on the power grid affect more than just the lights. A large-scale blackout affects health, safety, productivity, trade, consumption, water supplies, transportation, communication, and tourism. “From the available records of large blackouts in North America between the years 1984 and 2006, we find (1) that the frequency of large blackouts in the United States has not decreased over time, that there is a statistically significant increase in blackout frequency during peak hours of the day” (Hines, et. el., 2009). Through the efforts of Government organizations and initiatives, such as the Department of Homeland Security’s (DHS) Cybersecurity Infrastructure Security Agency (CISA), The Maine Emergency Management Agency (MEMA), the Maine Office of Information Technology (OIC), and the Cyberspace Solarium Commission (CSC), we can safely address the policy and laws that cover these risks. This research aims to analyze the policies, controls, and regulations that these agencies utilize and enforce to ensure there are no gaps, contradictions, or ineffectiveness when compared with each other and state and federal laws. All of these are analyzed under the lens of the MITRE ATT&CK model to find these gaps and then compared against the CIS Critical Controls list to see what controls are not covered.

. The study utilizes information available to the public and any collaboration with the State of Maine and federal agencies to ensure that all relevant government policies, controls, and laws are evaluated and considered in the final project analysis.

Electrical Grid Overview

“The electricity grid is a complex machine in which electricity is generated at centralized power plants and decentralized units and is transported through a system of substations, transformers, transmission lines, and distribution lines that deliver the product to its end user, the consumer” (*U.S. Electricity Grid & Markets | US EPA*, 2023). The SOM Electrical Transmission grid is part of the larger SOM Electrical grid. The study focuses on the transmission grid as this is under the direct supervision of the SOM Government. The transmission grid transfers energy from the production sites to the distribution sites. Different companies and organizations operate each of these sites. Distributors are primarily commercial entities controlling the energy journey's final leg. The production sites include oil power plants, solar farms, wind farms, and nuclear power plants. Energy can also come from out of state or from Canada. The transmission grid monitors, maintains, and controls these connections and throughput. Much regulatory information is publicly available and accessible through government agency sites.

Electric Production

The U.S. electrical grid generated 20% from renewables, 20% from nuclear energy, 19% from coal, and 40% from natural gas in 2020. (EPA, 2023). Renewable sources range from wind, hydro, solar, biomass, and geothermal, which are generated mainly by wind and hydro. The electrical generation is trending towards natural gas and renewables and away from coal. This presents new challenges in cybersecurity while providing more diversity in generators. The generator diversity creates potential targets that could impact the electrical grid’s power generation.

Electrical Transmission

There are three significant portions of the United States’ electrical grid: the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas. “The

redundant design of the grid helps prevent service interruptions to retail customers due to transmission line or power plant failures" (EPA, 2023). These interconnections are broken down further into regional markets and with differing laws and regulations per state. The two market types are traditional regulation and competitive markets. In competitive markets, the suppliers compete for market share and profit. In traditionally regulated markets, energy projects are utility-owned and governed directly through government agencies and oversight. Maine is a competitive marketplace. As displayed in Figure 1, several companies, utilities, and organizations play a part in the Maine electrical grid. These are what make up the distribution of energy in the SOM.

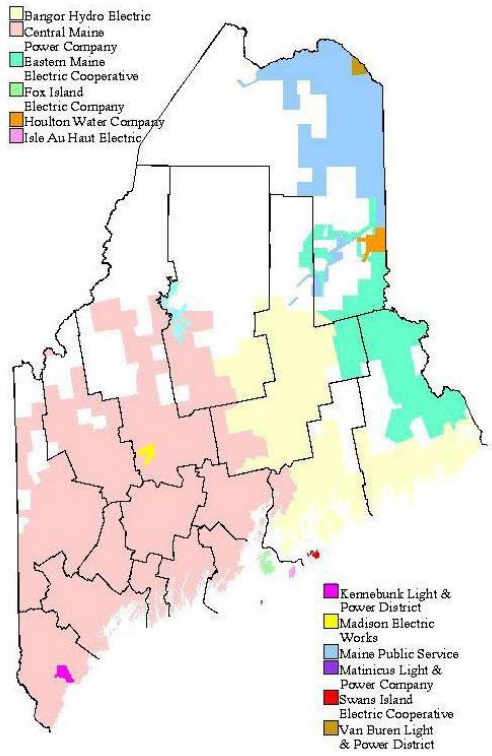
State of Maine Electrical Grid

This study specifically focused on the transmission grid and the governance put forth by the SOM regarding the cybersecurity of these lines and their operation. According to the Maine government website, three investor-owned companies and nine cooperative or municipal-owned utilities exist. These are the significant influences on energy distribution to the electrical grid with forms of controls and policies that ensure proper security. They are audited and overseen by the Maine Public Utilities Commission (MPUC) (MPUC, n.d.). Investor-owned utilities are for-profit organizations that provide competitive services like a standard business. There are nine cooperative or municipal-owned utilities in the state of Maine. Municipal utilities are controlled and governed by the government entities representing their district or area. Cooperative-owned utilities are owned by the customers they serve. Both options are non-profit organizations meant to provide power to their customers and reinvest all profits into the infrastructure. Government agencies like the MPUC and external auditors like the North American Electrical Reliability Corporation (NERC) oversee these entities to ensure they comply with the latest security

mandates and controls. They are responsible for setting their rules and policies regarding energy distribution, whereas the SOM sets policies and controls regarding energy transmission. In simple terms, the Utilities are responsible for where the electricity goes, while the SOM is responsible for how the electricity flows. Transmission is the bulk transfer of electricity throughout the grid. This study focuses on the laws, policies, and controls to protect electricity transmission. Figure 1 from the Central Maine Power Company at cmpco.com (Retrieved 10-30-2022) displays these respective areas and the entities that control them. Each area is a part of the transmission network managed and protected by the SOM.

Figure 1

The Maine Power Grid distribution map



Purpose

This study aimed to explore the State of Maine's policies and governance to evaluate and assess the electrical grid's vulnerabilities, contradictions, or gaps in cyber security. The study

developed a matrix to evaluate public policy through the lens of the attacker. This presents a new point of view and method of policy analysis.

Research Questions

The design explored the sufficiency of Maine's laws and policies to see if they protect the electrical grid against the objective evaluation tool. What are the federal laws that pertain to the cybersecurity electrical grid? What are the Maine laws and policies about the cybersecurity electrical grid? What frameworks pertain to developing a robust conceptual model for analyzing the cybersecurity of Maine's state policies? The researcher designed the study to answer these questions and assumptions by selecting and analyzing the SOM policies and procedures.

Conceptual Framework

The conceptual framework built upon the previous research by Polski & Ostrom (1999) on the IAD Framework and integrated concepts of MITRE ATT&CK (n.d.) and NIST regulatory functions to produce a new method of analyzing, sorting, and assessing risk related to policy and its efficacy in mitigating or combatting modern attack techniques.

Scope

The amount of policy and time assigned to the research limited the. The researcher utilized a strict filtering system to select policies for the study. These restrictions prevented the researcher from thoroughly analyzing every policy, law, and procedure that could impact the security of the SOM electrical grid. For the sake of this study, the researcher limited the conceptual framework to the NIST Five Functions (2023) and the 14 significant techniques of the MITRE ATT&CK (n.d.) framework.

Significance

The study provided significance by creating a new avenue to view, analyze, and assess public policy concerning cyber-attacks. Cyber-attacks on critical infrastructure can weaken economies and destroy societies. It is essential to understand and prepare for these attacks.

The electrical grid is a vast, interconnected legislation, business, and oversight network. Analyzing a small part of a massive supply chain only revealed some of the issues that might exist. To discover more, the researcher would need to conduct a more extensive study over a longer period of time with more data from a wider variety of agencies. The researcher conducted the following literature review, which explores and lists the data and information used in the study. The researcher sorted, filtered, and organized these policies to ensure efficient analysis.

CHAPTER 2

LITERATURE REVIEW

The modern power grid is evolving with the integration of smart grid technology. “Industry and government have made a significant investment to build a more innovative and more. Automated/connected power system” (Sun et al., 2021, p. 45). These interconnected networks provide more diverse and complicated risks that government agencies must consider when enforcing, creating, and evaluating current and future laws, policies, and controls.

Laws, Policies, and Procedures

Laws

“Laws can form the basis for regulations, guidance, and policy.” (DHHS, 2018) Laws explain what you can, cannot, or must do in the United States. Laws apply across society, business, and territory governed by the country or state. Federal and State laws cover various topics, regulations, and concerns of the citizens, businesses, and policymakers. Federal laws are passed by both branches of Congress and signed by the President. (DHHS, 2018) State laws are passed through the state’s congress and then signed by the governor.

Policies

“There are many other types of policy documents issued by the US Government, ranging from Presidential memoranda to agency guidance and policy statements. Each has its purpose and process for publication, but all must be consistent with existing law.” (DHHS, 2018) Executive orders, presidential directives, memoranda, guidance, and policy statements produce Federal policies. Government policies must align with laws and regulations made by governing bodies. State policies follow the same reasoning.

Procedures

Procedures are generated from public policies and laws by responsible government agencies. U.S. Federal government Departments and Agencies issue regulations to interpret and implement laws passed by Congress (DHHS, 2018). State policies and procedures are generated in the same way. Procedures and regulations are the actions required to enforce, incentivize, and enact the interpretation of laws and policies (Bauer, J.M. 2010).

Current Threats

"Cyber-attacks are increasing in number and sophistication, causing organizations to adapt management strategies for cyber security risks continuously" (Hart et al., 2020, page number). The literature below aims to identify, define, and understand what laws, policies, and controls exist to protect the energy grid's operations from the top down. In this study, the researcher examines existing regulations at the federal and state levels to analyze how designated government agencies enforce them and they enact controls to manage the state's electrical power grid's security.

Federal Laws

The United States government has one law tied explicitly to cybersecurity. The Federal Information Security Modernization Act of 2014 (FISMA 2014). This law amends the previous Federal Information Security Management Act of 2002 to "(1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) concerning agency information security policies and practices, and (2) set forth the authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems." (FISMA, 2014) FISMA 2014 addresses the management and authority of government agencies and initiatives that directly influence the cyber security of the United States. These

agencies and enterprises include the Federal Information Security Incident Center (FISIC), the Director of National Intelligence (DNI), the guidance developed by the National Institute of Standards and Technology (NIST), and the Information Security and Privacy Advisory Board. It directs these initiatives and dictates which position or agency is responsible (FISMA, 2014).

Federal Policies

The United States is the foremost nation regarding cybersecurity policies (Benoliel, D. 2014). Though the USA has a track record for establishing a cybersecurity policy, many factors still go into the enforcement and effectiveness of each policy including the six significant ways listed in Appendix G.

The Homeland Security Presidential Directives cover many issues regarding the continued operations of government agencies, infrastructure, programs, and identification of government employees and contractors but need more specific information regarding cyber policies related to the electrical grid. These policies are overarching and broad and do not directly apply to the purpose of this study.

The Federal Emergency Management Agency (FEMA) Federal Continuity Directive 1 (2017) is the official directive for the PPD-40 National Continuity Policy. It directs DHS and FEMA to coordinate the implementation, execution, and assessment of continuity activities. This document covers cyber security regarding the continued operation of essential activities, programs, and infrastructure.

Maine State Laws

The State of Maine's Laws regarding cybersecurity fall under Title 24-A Maine Insurance Law and Title 35-A public utilities (see Appendix H).

Only one of these laws pertains directly to the security policies of the grid. Title 35-A: Part 3: Chapter 31: Subchapter 2: Section 3143: Declaration of policy on smart grid infrastructure. This statute establishes a Resource Assessment Policy, Smart Grids Policy, Transition Plan, displaced employees, Compliance with safety, security, and reliability standards, Cost recovery, reporting, and consumer education. This is the only statute that directly influences the cybersecurity of the Electric grid in this study. Other laws about the public utilities of the state of Maine and their operations, accounting, legality, and regulations are in Title 35-A.

Maine State Policies

Maine state policy must be considered to assess the situation in Maine properly. According to the NCSL, “at least 40 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. Twenty-four states enacted at least 41 bills in 2022 so far” (2022). The most common enactments require government agencies to implement cybersecurity training, provide funding for cybersecurity programs and practices in state agencies, mandate security practices related to elections, and establish or support programs or incentives for cybersecurity workforce training (NCSL, 2022). The NCSL shares that many policies will focus on recent public concerns (election security) and cybersecurity funding and training.

The State of Maine has deployed several policies encompassing the electric grid and its security. Appendix A contains the policies considered in the study. Most State of Maine Policies include a policy conflict section stating, “If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail (SOM, AC-1, 2023).” The policies and procedures in Appendix A relate to the Office of Information Technologies (OIT) standards for securing all SOM IT assets. These policies are focused on the entirety of the SOM’s IT infrastructure, which includes any electrical grid IT assets. A short description of each policy with the security and privacy tag is provided in Appendix A.

Conceptual framework

Institutional Analysis and Development (IAD) Framework

“The Institutional Analysis and Development (IAD) Framework is best viewed as a systematic method for organizing policy analysis activities” (Polski & Ostrom, 1999, p. 5). It provides a ways to organize and analyze each policy to ensure non-biased filtering. The IAD Framework by Polski & Ostrom (1999) filters and categorizes each policy to ensure the study

focuses on the policies that bear the most significant impact on the cybersecurity of the SOM's electrical transmission grid. It does this through a 7-step process. Step one is to define the policy analysis objective and analytic approach. The objective is to define and identify policies that affect the cybersecurity of the electrical transmission grid through a series of questions about the policy under review. First, the first questions in the framework pinpoint the outcomes of the policies. It then identifies relevant patterns of interaction. For the purpose and scope of this study, only the first step is used to identify and filter the policies.

MITRE ATT&CK Analysis

All relevant governance will be considered for analysis through the MITRE ATT&CK model. The process will involve analyzing the public policy from the eyes of an attacker. The attack model covers 14 sections of attack aspects. Not all these attack aspects apply to public policy or the following legal proceedings. The study will only consider the 14 primary techniques as they pertain to the 5 NIST functions. The 14 sections of the MITRE ATT&CK model are Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and control, Exfiltration, and Impact. The policy and procedures are analyzed to identify which aspects the law, policy, or practice are designed to manage or counter. Then, the aspects will be considered regarding their ability or efficacy in dodging, avoiding, or neglecting any legal ramifications while maximizing the impact on the SOM electrical transmission grid.

NIST Breakdown

Each aspect of the MITRE ATT&CK framework is assigned to one of the five functions of the NIST framework. The functions are Identify, Protect, Detect, Respond, and Recover (NIST, 2023). Each function of the NIST Framework is identified by NIST (2023) (See Appendix C).

After the aspects of the MITRE ATT&CK Framework are assigned to the proper function, they are considered together for the final analysis. This serves as a focus for the analysis to ensure the study does not consider MITRE ATT&CK aspects that do not fall under these five essential cybersecurity functions.

Center for Internet Security (CIS) Comparison

The CIS has a set of Critical Security controls that it states are "mapped to and referenced by multiple legal, regulatory, and policy frameworks" (*CIS Controls Version 8*, 2022). The study compares the findings from the previous two frameworks and checks them against the CIS Critical Controls to ensure that each control is covered. All uncovered or partially covered controls are noted for the final report and referenced to the respective agencies to ensure they are notified of the gap. This step ensures that all relevant critical controls are considered or covered. There are many layers of policy and controls in the electrical grid of the SOM. From the top down are Federal, State, Vendors/Stakeholders, Local Municipalities, and lastly the consumers. This study focused on the laws, policies, and controls from the Federal and State influences to ensure that there are no inefficiencies, discrepancies, or gaps in governance that could create security vulnerabilities in the State of Maine's electrical transmission grid. This study took a different approach to public policy and threat assessment by developing a method of evaluation utilizing the MITRE ATT&CK framework to assess these policies through the lens of

the attacker. The study is designed for government agencies, concerned individuals, and responsible IT personnel to be aware of potential vulnerabilities in the current SOM Policy. The researcher used four established frameworks to build a rubric and rating system to filter and analyze each SOM Electrical Transmission Grid cybersecurity policy properly. The overall design explored the sufficiency of Maine's laws and policies on the grid's security through the perspective of public policy and response. The electrical grid is a massive, interconnected infrastructure machine, and the government is only directly responsible for the middle portion of the grid. This review has discovered the policies, laws, and procedures in the government's scope of control.

CHAPTER 3

METHODOLOGY

The research developed an objective means to evaluate Maine's Public policy for the SOM Electrical transmission grid. The Methodology used multiple frameworks and matrices to create a rubric for grading and analyzing state policies. The researcher designed the final rubric to rate, filter, and analyze each policy regarding the cybersecurity of the electrical grid. These three questions were the basis for the Methodology and the steps taken. First, the researcher filtered and analyzed each policy using the first step of the IAD framework. Next, the researcher merged the NIST Five Functions and the MITRE ATT&CK Framework's 14 techniques into a new conceptual model for evaluating laws and policies (MITRE ATT&K, n.d.). Lastly, the researcher compared the current policies and procedures against the CIS Critical Controls list and other government regulatory documentation, such as NIST and FISMA 2014, to ensure compliance and completeness.

Stakeholders

The study focused on relevant government agencies, specifically the SOM OIT, and their regulatory cybersecurity functions. The electrical grid stakeholders include but are not limited to energy producers, government agencies, energy distributors, and consumers (EPA, 2023). Each stakeholder played its part in the protection and operation of the grid. The scope focused on the Government agencies and the jurisdiction that they govern. The state of Maine is a part of the Eastern Interconnection, and power generators contribute from across this interconnection of networks. The Maine Governor's Energy Office (GEO) "is responsible for several activities such as providing policy leadership and technical assistance, developing energy programs, monitoring energy markets, and reporting on heating fuel and energy prices" (Energy | Maine.gov, n.d.).

The primary stakeholder for this study was the GEO. Its influence and connection in corroboration with Maine OIT created the policies and procedures analyzed in the study.

Data

The study analyzed policies, laws, and procedures from the SOM OIT and federal agencies. These policies were all publicly available on the corresponding government websites. The study focused on any policies, laws, or procedures that have the most impact or had the most significant influence over the cybersecurity of the electrical transmission grid. Many policies, procedures, and rules can play even the slightest effect on the electrical transmission grid. The study focused only on the most influential policies, procedures, and regulations. Reviewing each policy took time and effort, so to minimize the scope of the study, the researcher reduced the number of policies reviewed. These reductions provided a more robust analysis of each policy and its impact.

Federal

These sources of federal cybersecurity law and policy were considered for the study from the DHHS Introduction to Law and Policy (2023).

- White House Office of Management and Budget (OMB) Circulars
- OMB Memoranda
- Presidential Executive Orders (EO)
- Presidential Policy Directives (PPD)
- Homeland Security Presidential Directives (HSPD)
- Federal Emergency Management Agency (FEMA) Directives

These laws and policies are all publicly available on government websites. Some of these policies are not considered as they bear no immediate impact on the cybersecurity of the SOM Electrical Transmission Grid. The researcher filtered the listing to find all associated

cybersecurity policies and removed all policies that had no immediate impact on public infrastructure.

Maine

The researcher searched the SOM Law on the Maine.gov legislature site in the statute search by searching all statutes for the cybersecurity key term (see Figure 2 for example).

Figure 2

SOM Statute Filtered search.

The Statute considered most influential on this generated list was title 35-A, section 3143: Declaration of policy on smart grid infrastructure. The remaining policies were assessed and did not correlate with the electrical grid. Further laws were reviewed regarding the grid with the keyword search containing electric grid. This yielded a longer list of statutes, most of which did not pertain to the grid's cybersecurity. The SOM policy information collection was like that of the Federal government but with a different interface and website. The Maine.gov/oit/policies-standards listed every primary policy and allowed for sorting them according to Security and Privacy considerations. The policies tagged for Security and Privacy were considered first in the evaluation of SOM IT Policies. The figure below displays an example of SOM Policies and the tagging in reference.

Figure 3

SOM IT Policy filtered search example.

Title	Date Last Updated	Security and Privacy	Web & Network	Accessibility	Lifecycle Management
Access Control Policy (AC-1)	2023/07	•			
Access Control Procedures for Users (AC-2)	2023/09	•			
Audit Policy	2018/07	•			
Data Centers Access Control Procedure	2019/04	•			
Data Classification Policy	2023/02	•			
Data Exchange Policy	2021/03	•	•		
Drone (Unmanned Aerial Vehicle) Policy	2021/12	•			
FOAA Policy	2017/10	•			
Information Privacy Policy	2017/09	•			
Information Security Policy	2019/03	•			

The researcher analyzed each policy to determine if it bore any immediate impact on the cybersecurity of the electrical grid, then sorted and filtered further by running them through the

first step of the IAD Framework (Polski & Ostrom, 1999). The Framework was explicitly focused on cybersecurity and the Electrical grid to ensure that no unnecessary evaluations are carried out. Figure 4 displays an example of this framework and how it filters the tagged policies.

Figure 4

Example of step one IAD Framework filtering process

Policy	1.0 Document Purpose	What is happening in this policy?	Which outcomes are most important?	CIS Critical Control Aligned policy	How does this policy impact electrical Infrastructure?	Does this policy pertain to Cybersecurity?	NIST Function Alignment
Access Control Policy AC-1	The purpose of this document is to define the State of Maine policy and procedures for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).	This policy dictates the means to control access to IT systems and networks.	Controlling who, when, how, and what people, systems, and vendors can access.	CIS Control 6: Access Control Management	Access control dictates the means to access IT infrastructure supporting the Electrical grid.	Yes	Identify/Protect
Access control Procedures AC-2	These procedures identify how the State of Maine meets security requirements pertaining to account management, access enforcement, separation of duties, least privilege, remote access, wireless access, and access control (see Definitions) for mobile devices. This document corresponds to the Controls AC-2, 3, 5, 6, 17, 18 and 19 of the Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).	These procedures dictate the steps to control access to IT systems and networks.	Controlling who, when, how, and what people, systems, and vendors can access.	CIS Control 6: Access Control Management	Access control procedures dictates the steps and enforcement of access to IT infrastructure supporting the Electrical grid.	Yes	Protect
Audit Policy	This policy establishes expectations for OIT personnel regarding any I.T. audit the Executive Branch is subject to. The purpose of audit monitoring/tracking is to ensure that audit responses are provided to auditors with full information needed and audit findings are addressed in a timely manner.	The policy sets expectation for future and ongoing audits	Dictates how and who controls and manages audit proceedings	CIS Control 8: Audit Log Management	Audits are carried out on Electrical Infrastucture systems	Yes	Identify
Data Center Access Control Procedures	The purpose of this document is to clarify the process by which employees, contractors, vendors, and other individuals are authorized for access to OIT Data Centers, and the conditions for controlling that authorized access. Enterprise Operations and Monitoring (EOM) must maintain and operate the OIT Data Centers physical environment in a professional manner, equivalent to what one would expect of a commercial facility.	This policy dictates the access procedures to government data centers	Dictates how access is managed and what steps are taken to grant or authorize access to data centers.	CIS Control 6: Access Control Management	This pertains primarily to Data Centers.	Partially/ Covered in AC-1 & AC-2	Protect

The filtering process reduced the policies in scope by observing their purpose and removing any policies that did not directly influence cybersecurity or the electrical grid. After minimizing the number of laws in scope from 24 to 11, the researcher examined the policies. The OIT manages and enforces all the cybersecurity and Information Technology policies and controls. They have a headquarters in Augusta but many satellite offices for regions and cities throughout the state. The closer the study gets to the direct control over portions of the grid, the more in-depth and widespread the rules and policies become. The guidelines were filtered to focus on cyber security and then analyzed to assess if the policy directly influenced the Electrical Transmission grid and

the personnel that work on and with it. Policies were reconsidered as the grading and analysis steps in the study were performed.

Analysis

The study utilized four frameworks and a list of critical controls to construct a rubric to grade and analyze each of the laws, policies, and procedures. The Matrix uses portions of the IAD to filter and sort relevant policies. Then, the Matrix integrates the MITRE ATT&CK model with the NIST five functions to view each policy about each NIST function through the lens of an attacker or exploiter. In the case of policy, it is looking for ways to work around them to avoid the consequences or cause the most damage to the system. The final step of the rubric is to compare the policy against the CIS Critical Controls list to see if it is considered or corresponds with one of the Critical Controls.

Compliance

During the grading process, the policies are assessed by federal and state laws to ensure they follow the rules they intend to enforce. Most policies will be related to the FISMA (2014) act and all corresponding regulations and procedures that are derived from this act. These include but are not limited to the Federal Information Security Incident Center (FISIC), the Director of National Intelligence (DNI), the guidance developed by the National Institute of Standards and Technology (NIST), and the Information Security and Privacy Advisory Board. The study primarily focused on the SOM Policies and procedures regarding IT Security of the Electrical grid. Still, in many policies, some clauses refer to the guidelines and regulations produced by these agencies and FISMA (2014). The study cannot analyze the policies and procedures without understanding these agencies, regulations, and laws.

Policy Rubric

The policy rubric merged the functions of NIST with the MITRE ATT&CK techniques to assess each policy. This created a lens to grade policy based on current recommendations from NIST with consideration of attack techniques from MITRE. The researcher created the merged rubric by individually going technique by technique and comparing the description of each to the description of each of the five functions from the NIST framework (see Appendix B). The MITRE ATT7CK sub-techniques are excluded from the vigorous analysis performed but are considered and reviewed for further consideration in future rubric development. The sub-technique initial analysis can be found in Appendix I where the count of each sub-technique is mapped to the NIST Functions. The researcher mapped the techniques to the five functions, revealing that four aligned with Detect, three aligned with Identify, five aligned with Protect, one with Recover, and one with Respond. This finding shows that the policies analyzed fall primarily into protect, detect, and identify, as these are the three primary functions of the rubric and contain the most information and content to compare against.

Application

The rubric is applied across all the policies in the scope of the study. Some procedures, such as AC-2, refer to AC-1 for nonrelevant aspects or sections. Due to the interconnected nature of these policies, it is impossible to observe each policy in a vacuum. To thoroughly assess each policy, some attributes must be referred to other approaches. AC-1 is a primary policy and will often be directed to by other policies. Due to this nature, the prior policies will be assessed more thoroughly to ensure that all the dependencies are covered in the following analysis. Utilizing the IAD Framework diminishes selection bias from the policies considered for the analysis.

Bias

Bias is mitigated by producing results based on the most justified answers. Some bias will remain in the researcher's interpretation of complicated or vague texts or understanding. Each policy will be examined piece by piece, and each piece will be associated with its respective risk. Upon association, the researcher assigned the risk value based on the number of aspects corresponding to that risk and which ones were mitigated or prevented due to that portion of the policy. Selection bias is mitigated with the use of the IAD Framework analysis. Trusted government agencies or previous academic research produce all descriptions and identifying functions. The researcher thoroughly considers and compares these given descriptions to ensure the most suitable mapping, analysis, and understanding.

Insights

The grade and the results are a product of understanding and research. Many components go into forming an effective policy. No policy can perfectly cover the risks present in the modern day, especially with the rapid development of technology and the many government regulations that slow innovation for agencies like the SOM OIT. These grades are subject to scrutiny. They utilize the perceived enforcement and procedures to test them theoretically against MITRE ATT&CK aspects. These aspects are vast and often updated to reflect new or emerging threats in the digital environment. When looking at the more technical or complicated factors, it is clear that these policies need to contain the depth of knowledge or actions to mitigate the risk that these aspects present fully. These policies are the backbone of the procedures and activities that must be taken to reduce this risk. No matter how many policies are in place or how well they are written, they all rely heavily on the agencies and their personnel's ability and enforcement.

Limitations

The researcher is limited by the amount of information each government agency provides and any publicly available records. This study is an overall review of the current state of the

security policy of the SOM electrical grid and what potential security gaps might exist in public policy. It is not an in-depth dive into the grid's security features or the existing vulnerabilities. It is an exploratory analysis of current issues that may be present in public policy. The research only intends to highlight potential risks to the SOM electrical grid. The policy grading weighs heavily on the understanding and knowledge of the researcher.

Pilot Study

The first policy analyzed is AC-1 Access Control Policy and Procedures. The process starts with the IAD filter. The filter and analysis presented by the first step of the IAD Framework define what Function the policy falls under, if it pertains to cybersecurity, and if it impacts the electrical grid. AC-1 impacted the electrical grid and pertained to cybersecurity. The IAD framework integrates the CIS Comparison to remove a step later in the analysis. The CIS Control that aligns with AC-1 is CIS Control 6: Access Control Management.

The second phase of the rubric checks the policy against the aspects in the MITRE ATT&CK framework as defined by the NIST Five Functions to find how well this policy mitigated MITRE techniques. The NIST Function filters techniques to minimize the redundancy of testing each technique against the policy. For Example, most aspects of reconnaissance fall under Identify, as they are actions or activities that identify vulnerabilities and can be mitigated by identifying them. Then, each policy is defined based on the Functions and assessed against the MITRE ATT&CK aspects that fall under that function. Each policy is summarized based on the totality of its sections and then analyzed against this framework. For the case of AC-1, it is suggested that a form of Two-Factor Authentication is implemented. AC-1 protects access controls such as IDs, Passwords, and logins.

This procedure is intended to mitigate risks under the Identify and Protect functions in the NIST framework. The researcher only considered MITRE ATT&CK aspects corresponding to

these NIST functions to make the process more efficient and streamlined. Other policies primarily cover these aspects, and AC-1 only influences how these policies are implemented, not how these aspects are mitigated. The primary focus is on Access Control. The highest-risk aspects identified are Privilege Escalation and Lateral Movement. These aspects bear the most significant risk for AC-1's procedures as many government initiatives require information sharing and external parties. These fall under the Detect and Identify categories of the rubric. AC-1 primarily focused on the Identify category but has relevant connections and considerations for Protect and Detect functions. The rubric compared AC-1 against these categories to analyze what percentage of each is covered by the policy. The rubric displays (Table 1) the grade of each category that the policy addressed. Each category is carefully considered through the description of NIST Functions and MITRE ATT&CK technique descriptions. When focusing on the SOM Electrical Transmission grid, it is essential to understand how contractors, employees, and privileged users access the systems and networks.

The final grade is granted by entering the numbers provided by the rubric into a percentile calculation. Table 1 in Appendix D shows how the numbers are assigned to AC-1 and how it quantifies the analysis results. The numbers are then added and divided by the total possible points. This yielded a final score of 80 for AC-1. The final grade is shown in Figure 5.

Figure 5

Example of Rubric Grade Final

Policy	NIST Function Alignment	Identify	Protect	Detect	Respond	Recover	Grade
Access Control Policy AC-1	Identify/Protect	4	4				80%

The grade of four is designated due to the significance that AC-1 has on the identified functionality of the NIST Functions. However, since the policy only partially covers the

identifying techniques that pertain to access controls, the score is reduced by one to four. The same can be said of the Protect Function. AC-1 analysis is considered concurrently with following analysis as it plays a major role in the cybersecurity procedures of many SOM policies.

CHAPTER 4

RESULTS

The researcher presented the results of each policy included in the study's scope. They are assessed based on their ability to prevent, mitigate, or identify potential threats to the SOM IT Security, specifically for the portion of the Maine electrical grid governed directly by the state. Presented below are the study results and any recommendations made by the researcher for further study and action.

Analysis

The researcher scored each relevant SOM OIT Policy according to the rubric and then compared it to agency regulations to ensure that each policy covered the risk and the code. The researcher compared each approach to the CIS Critical Controls to ensure that all critical controls were noticed. It is essential to note that the scope of the research was only policies that concerned the SOM Electrical Transmission Grid. The first step of the analysis filtered the policies through a rigid selection process to find the most impactful policies. The researcher analyzed data by comparing NIST's five functions and MITRE ATT&CK techniques and merging these two frameworks required comparing the descriptions of both frameworks. The comparison of policy sections with the merged rubric organized the analysis of the data.

Presentation of Results

The research produced two significant points of data: 1) A sequence of grades for policy around the cybersecurity of the SOM Electrical grid and 2) a means to measure NIST Functionalities as they pertain to the MITRE ATT&CK primary techniques. The framework filtered policies to ensure policies pertained to the purpose of the study. The first step of the IAD was to integrate the filter directly into the framework. This filter helped the researcher minimize 26 policies into 11 of the most relevant (see Appendix F). The researcher examined eleven

policies using the rubric developed in the study and considered each policy according to the criteria designated for its respective NIST Function on the scale (see Figure 6).

Figure 6

NIST/MITRE Function grade scale

Aligns with NIST Functions and mitigates a majority techniques - 5 points	Aligns with NIST Functions or Mitigates a majority Techniques - 4 points	Does not Align with NIST Functions or mitigate a majority of Techniques - 3 points	Does not Align with NIST Functions or mitigate Techniques - 2 points	Does not Align with NIST Functions and does not mitigate Techniques 1 points	N/A - 0 points

Policies are graded based on how well they followed the descriptions of the NIST Functions and how well they mitigated the MITRE ATT&CK techniques that aligned with those functions. Appendix B contains the list of functions assigned for each technique and the description for each technique. Appendix C contains the list of NIST Functions and the descriptions provided by NIST. Appendix E contains the final list of grades.

The overall state of policy for the SOM Electrical grid's cybersecurity was robust and provided excellent coverage of two major NIST Functions. Identifying and protecting were the primary NIST Functions that were the focus of the policy examined in the study. There was less coverage for the Detect function and much less for Respond and Recover. This study did not include all policies produced by the SOM OIT. Other policies could be considered and examined but were outside the scope of this study. Though there are discrepancies in the data utilizing filtering and scope, what the researcher discovered is a vital policy foundation for the protection of the grid. Policies that are diverse in their coverage will improve the overall status of these policies. Breaking down and being specific on policy coverage provided a more robust understanding of what the policies protect or dictate.

This study aimed to explore the State of Maine's policies and governance to evaluate and assess the electrical grid's vulnerabilities, contradictions, or gaps in cyber security. The study did this by considering federal agencies' regulations and frameworks to develop a conceptual model

that graded each policy related to NIST regulations and MITRE ATT&CK techniques. Government policy was not as robust as it could be, and specific guidelines may not consider the attack techniques that would go up against them and the systems they govern. The study showed that the current policies are robust in dictating protections but could use improvement as they consider the attack techniques linked to the NIST Functions. The analysis took 24 policies and filtered them down to 11 through a series of questions to assess their impact on the grid's cybersecurity. These final 11 were evaluated according to the model and presented with a final grade. Four policies graded 70 or lower showed that they could use attention towards the NIST Functions or the MITRE ATT&CK techniques that pertain to that function. Three policies scored 100% as they were well-defined and to the point with no extra purpose or reasoning.

The study discovered what policies and procedures play a role in the cybersecurity of the SOM electrical grid by developing a framework that filters and analyzes the policies. The researcher proceeded to analyze the efficacy of these policies as they pertain to the framework's merged rating of the MTIRE ATT&CK techniques NIST five functions. By utilizing and merging existing and trusted frameworks, the researcher learned and assessed different methods of analysis and understanding. These frameworks and filters are what built the understanding and analysis that took place.

CHAPTER 5

CONCLUSION

Introduction

The study found laws and policies that pertained to the SOM Electrical grid's cybersecurity. Policy filtering and analysis are utilized to prevent the scope of the study from escalating. Upon identifying these key policies, the researcher evaluated them according to the rubric developed from merging the NIST Functions and the MITRE ATT&CK framework. The grades produced by this rubric were interpreted and deciphered to determine that the SOM has a robust policy foundation but could improve specificity, simplicity, and overall coverage of the merged framework's factors. The researcher builds a merged framework of the IAD, NIST, and MITRE ATT&CK to analyze policy through the lens of the attacker. The Merged framework filters the policies and compares them against the NIST five functions while considering the related MITRE ATT&CK techniques.

Interpretation of findings

There are many laws about cybersecurity and even more about infrastructure. Several federal laws also pertain to the cybersecurity of the electrical grid. Though they may not specifically address the electrical grid alone, many infrastructure initiatives, agencies, and procedures around the grid's security exist. Most of these stem from FISMA 2014 and its directives. There are significantly fewer State of Maine laws regarding the cybersecurity of the electrical grid. SOM laws need to be revised due to the discrepancies in federal legislation that covers state laws. The laws, both national and SOM, mandate the generation of policy. The SOM policy about the electrical grid's cybersecurity is more robust and detailed than state laws. This is because the Federal laws, regulations, and oversight that these policies provide the foundation for more stringent policy. The SOM lacks laws specifically targeted towards cybersecurity. The

SOM OIT developed a robust policy base to build upon in future additions to their policies. The researcher discovered a need for more specificity for policies. Many policies contained pieces of other policies or referred to many other policies that could have held those sections instead. This created an interconnected web of guidelines where more straightforward, concise, and focused policies would suffice.

Implications

This researcher intends to further the discussion of methods and refined frameworks for policy grading and analysis. The researcher encourages any individual, government agency, or institution to continue improving the model, developing stricter research, and integrating better policy controls built upon the IAD Framework for their public policy analysis. The development of the merged framework pushes the narrative for all involved organizations towards understanding and focusing on the further development of attack analysis. The merged framework allows any organization, individual, or institution to continue developing.

Recommendations for Action

The SOM institutions should develop more policies designed to counteract attack techniques. The SOM should explicitly break down the details of each policy to create a more straightforward, more specific policy regarding cybersecurity. The policy should be designed with the grid and other major infrastructure in mind, as these are critical to the well-being and continued operations of the SOM. The SOM OIT should consider developing more policies to encompass the excess covered in their current policies. The SOM policies need to be organized and analyzed. The organization should maintain policy integrity while developing effective means to sort and understand what the policy pertains to and what it is meant to do.

Recommendations for further study

Further research on policy assessment should be conducted through the lens of the attacker. This research can include more policies, laws, or robust analysis. The rubric can be redesigned or reconfigured to work towards understanding any approaches from the attacker's perspective. The following steps researchers can take regarding this study are expanding the capabilities of the merged framework, introducing more quantitative measures, or utilizing it on more policies in other industries or concerns. This merged framework needs to be completed or perfected. There is an opportunity for further development and research on the efficacy and usability of this framework.

Conclusion

The researcher conducted a study to develop a means to analyze, filter, and grade public policy about cybersecurity and the electrical transmission grid. This rubric is capable of analyzing policy through the lens of attack techniques, the understanding of NIST five Functions, and the filtering of the IAD Framework. The researcher used the CIS Critical Controls as the control group for the study to have a basis to understanding basic critical controls and what is required from them. The researcher implemented the rubric to test it and analyze existing SOM IT Policies. This revealed what policies are in need of more work or understanding while displaying what policies are robust and well defined in regards to cybersecurity and the MITRE ATT&CK Techniques.

The researcher concluded from the study that the SOM laws and policies are sufficient to protect the grid. Though enough, they need to be more efficient and proficient; there is always room for improvement. In this instance, the SOM can produce more laws to fill any lack of legislation. It can create more straightforward, concise, focused policies and procedures to

improve infrastructure cybersecurity like the electrical grid. The study showed that there are more ways to approach cybersecurity policy than through the lens provided by government agencies and laws. Understanding how attacks can be executed and the resources or controls they will target is essential. Policies can be sufficient, but they must also be maintained, improved, or reconfigured to adjust to existing and new threats as they arise, not just the current regulations or laws in place.

References

Almutairi, A., Wheeler, J. P., Slutzky, D. L., & Lambert, J. H. (2019). Integrating Stakeholder Mapping and Risk Scenarios to Improve Resilience of Cyber-Physical-Social Networks. Risk Analysis, 39(9), 2093-2112.

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the US electric power grid. Risk analysis, 40(9), 1744-1761.

Bauer, J. M. (2010). Regulation, public policy, and investment in communications infrastructure. Telecommunications Policy, 34(1-2), 65–79.

Benoliel, D. (2014). Towards a cybersecurity policy model: Israel National Cyber Bureau case study. NCJL & Tech., 16, 435.

Case, D. U. (2016). Analysis of the cyber-attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29.

Central Maine Power Company. Retrieved from cmpco.com, Date Retrieved 10/16/2022.

Chen, X., Zhou, J., Shi, M., Chen, Y., & Wen, J. (2022). Distributed resilient control against denial-of-service attacks in DC microgrids with constant power load. Renewable and Sustainable Energy Reviews, 153, 111792.

Crim, H. (2019). Heat and Light in the City of the Future: A Feasibility Study of Renewable Energy in Lewiston, Maine.

CIS Controls Version 8. (2022, February 4). CIS. https://www.cisecurity.org/controls/v8

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Access Control Policy and Implementation Guides | CSRC | CSRC*. https://csrc.nist.gov/Projects/access-control-policy-and-implementation-guides

Cybersecurity Programs & Policy. GSA. (n.d.). https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/programs-policy

National Conference of State Legislatures, NCSL, (2022) Cybersecurity Legislation 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2022637922035.aspx

Department of Health & Human Services, *Introduction to U.S. Law and Policy*, (reviewed 2018) Retrieved 10/29/2023.

Electricity Laws and Rules | MPUC. (n.d.). Retrieved October 30, 2022, from https://www.maine.gov/mpuc/regulated-utilities/electricity/electric-laws-rules

The Federal Information Security Modernization Act, S.2521 — 113th Congress (2013-2014)

Ferland, J. (2020). Ten Years of Tidal Energy Experience with the Maine Ocean Energy Act. Ocean & Coastal LJ, pp. 25, 221. https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1390&context=oclj

Gong, S., & Lee, C. (2021). Cyber threat intelligence framework for incident response in an energy cloud platform. Electronics, 10(3), 239.

Hart, S, Margheri, A, Paci, F, Sassone, V, (2002). Risk: A Serious Game for Cyber Security Awareness and Education, Computers & Security, Volume 95, 101827, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101827.

Hines, P., Apt, J., & Talukdar, S. (2009). Large blackouts in North America: Historical trends and policy implications. *Energy Policy*, *37*(12), 5249-5259.

Iron Net, (2022). Cyber Attacks on the Power Grid. https://www.ironnet.com/blog/cyber-attacks-on-the-power-grid

Kabir-Querrec, M., Mocanu, S., Thiriet, J. M., & Savary, E. (2015, September). Power utility automation cybersecurity: IEC 61850 specification of an intrusion detection function. In ESREL 2015-25th European Safety and Reliability Conference. CRC Press.

Knapp, E. D., & Samani, R. (2013). Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. Newnes.

Kulkarni, V., Sahoo, S. K., Thanikanti, S. B., Velpula, S., & Rathod, D. I. (2021). Power systems automation, communication, and information technologies for smart grid: A technical aspects review. TELKOMNIKA (Telecommunication Computing Electronics and Control), 19(3), 1017-1029.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for an enhanced level of /cyber-security in organizations. Journal of Enterprise Information Management.

Laufer J.A., (2014). Catching Fire: An Analysis of Maine's Combined Heat and Power Energy /Incentive Policies, UMI:1558554.

Li, Y., Liu, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.

Maine Public Utilities Commission, retrieved from https://www.maine.gov/mpuc/regulated-utilities/electricity/cep, Date Retrieved 10/16/2022,

Maine Legislature, retrieved from https://legislature.maine.gov/legis/statutes/search.asp Retrieved on 9/19/2023.

Maine, A. V. (2018). Offshore Wind in Maine.

MITRE ATT&CK®. (n.d.). https://attack.mitre.org/ Retrieved on 12/2/2022.

National Academy of Sciences. (2017). Enhancing the resilience of the nation's electricity system. Retrieved from https://www.nap.edu/catalog/24836/ enhancing-the-resilience-of-the-nations-electricity-system.

North American Electrical Reliability Corporation (NERC) (n.d.). https://www.nerc.com/pa/Stand/Pages/default.aspx Retrieved 9/21/2023

Office of Information Technology. (2023). Access Control Policy and Procedures (AC-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf

Office of Information Technology. (2023). Access Control Procedures for Users (AC-2). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlProceduresForUsers.pdf

Office of Information Technology. (2023). Architecture Compliance Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ArchitectureCompliancePolicy.pdf

Office of Information Technology. (2018). Audit Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AuditPolicy.pdf

Office of Information Technology. (2017). Business Continuity and Disaster Recovery policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/BusinessContinuityDisasterRecoveryPolicy.pdf

Office of Information Technology. (2019). Change Management Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

Office of Information Technology. (2022). Configuration Management Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ConfigurationManagementPolicy.pdf

Office of Information Technology. (2019). Data Centers Access Control Procedures. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataCenterAccessControlProcedure.pdf

Office of Information Technology. (2021). Data Exchange Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

Office of Information Technology. (2023). Digital Accessibility Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DigitalAccessibilityPolicy.pdf

Office of Information Technology. (2023). Data Classification Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

Office of Information Technology. (2018). Forensic Investigation Workflow Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ForensicInvestigationWorkflowPolicy.pdf

Office of Information Technology. (2019). Information Security Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityPolicy.pdf

Office of Information Technology. (2019). Major Incident Procedure. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/MajorIncidentProcedure.pdf

Office of Information Technology. (2020). Mobile Device Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/MobileDevicePolicy.pdf

Office of Information Technology. (2023). Network Device Management Policy. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/NetworkDeviceManagementPolicy.pdf

Office of Information Technology. (2019). OIT Building Access Procedures. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/OITBuildingAccessProcedures.pdf

Office of Information Technology. (2022). Personnel Security Policy and Procedures. https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PersonnelSecurityPolicy.pdf

Office of Information Technology. (2023). Physical and Environmental Protection Policy (PE-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PhysicalandEnvironmentalProtection.pdf

Office of Information Technology. (2022). Program Management Policy and Procedures (PM-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ProgramManagementPolicy.pdf

Office of Information Technology. (2021). Risk Assessment Policy and Procedures (RA-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RiskAssessmentPolicyProcedure.pdf

Office of Information Technology. (2021). Security Awareness and Training Policy and Procedures (AT-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAwarenessTrainingPolicy.pdf

Office of Information Technology. (2021). Security Planning Policy (PL-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityPlanning.pdf

Office of Information Technology. (2021). System and Communication Protection Policy and Procedures (SC-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemCommunicationsProtectionPolicy.pdf

Office of Information Technology. (2022). System and Information Integrity Policy and Procedures (SI-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemInformationIntegrityPolicy.pdf

Office of Information Technology. (2023). System and Communication Protection Policy and Procedures for Encryption Mechanisms (SC-12,13,17). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SCEncryptionMechanismsProcedures.pdf

Office of Information Technology. (2020). System and Services Acquisition Policy and Procedures (SA-1). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf

Office of Information Technology. (2018). Vulnerability Scanning Procedures (RA-5). https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf

Plietzsch, A., Kogler, R., Auer, S., Merino, J., Gil-de-Muro, A., Liße, J., ... & Hellmann, F. (2022). PowerDynamics. Jl—An experimentally validated open-source package for dynamically analyzing power grids. SoftwareX, 17, 100861.

Prehoda, E. W., Schelly, C., & Pearce, J. M. (2017, October). U.S. strategic solar photovoltaic-powered microgrid deployment for enhanced national security. Renewable and Sustainable Energy Reviews, 78, 167–175. https://doi.org/10.1016/j.rser.2017.04.094

PJM Learning Center - Transmission & Distribution. (n.d.). https://learn.pjm.com/electricity-basics/transmission-distribution

Polski, M. M., & Ostrom, E. (1999). An institutional framework for policy analysis and design. 1999.

Public Utilities. Title 35-A. https://legislature.maine.gov/statutes/35-A/title35-Ach0sec0.html

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Sridhar, S., Hahn, A., & Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100(1), 210-224.

State of Maine Statutes, Title 24-A, Chapter 24-A: Protection of Beneficiaries of Structure Settlements, Retrieved on 11-3-2023. Retrieved from https://legislature.maine.gov/legis/statutes/24-A/title24-Ach24-Asec0.html

State of Maine Statutes, Title 35-A: Public Utilities, Retrieved on 11-3-2023, Retrieved from https://legislature.maine.gov/legis/statutes/35-A/title35-Ach0sec0.html

State of Maine Statutes (2023), Title 35-A: Public Utilities part 3: Electric Power Chapter 31: General Provisions, Subchapter 2: Energy Planning; Construction; Purchases, Section 3143. Declaration of Policy on Smart Grid Infrastructure. Retrieved from https://legislature.maine.gov/legis/statutes/35-A/title35-Asec3143.html

Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56. https://doi.org/10.1016/j.ijepes.2017.12.020.

Ten, C. W., Govindarasu, M., & Liu, C. C. (2007, October). Cybersecurity for electric power control and automation systems. In 2007 IEEE International Conference on Systems, Man, and Cybernetics (pp. 29-34). IEEE.

The Five Functions | NIST. (2023, March 16). NIST. https://www.nist.gov/cyberframework/online-learning/five-functions

Umunnakwe, A. Sahu A. and Davis K., "Multi-Component Risk Assessment Using Cyber-Physical Betweenness Centrality," 2021 IEEE Madrid PowerTech, 2021, pp. 1–6, doi: 10.1109/PowerTech46648.2021.9494796.

U.S. Electricity Grid & Markets | US EPA. (2023, April 18). US EPA. https://www.epa.gov/green-power-markets/us-electricity-grid-markets

U.S. Energy Information Administration. Annual energy outlook. (2021). Retrieved from https://www.eia.gov/outlooks/aeo/pdf/appa.pdf

U.S. Energy Information Administration - EIA - Independent Statistics and Analysis. (2022). Retrieved October 30, 2022, from https://www.eia.gov/state/analysis.php?sid=ME

Wang, A., Zhang, A., & Schoeller, N. (2020). SHIFTING WINDS: WIND FARM SITING PROCESSES IN NEW YORK, HAMPSHIRE, AND MAINE.

Xue, Y., Liu, G., Taft, J. D., & Shankar, M. A. (2022). Emerging trends and systemic issues influencing today's US electric grid.

Appendix A

Table 1

Access Control Policy AC-1	The purpose of this document is to define the State of Maine policy and procedures for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).
Access control Procedures AC-2	These procedures identify how the State of Maine meets security requirements about account management, access enforcement, separation of duties, least privilege, remote access, wireless access, and access control (see Definitions) for mobile devices. This document corresponds to the Controls AC-2, 3, 5, 6, 17, 18 and 19 of the Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).
Audit Policy	This policy establishes expectations for OIT personnel regarding any I.T. audit the Executive Branch is subject to. The purpose of audit monitoring/tracking is to ensure that audit responses are provided to auditors with full information needed and audit findings are addressed in a timely manner.
Data Center Access Control Procedures	The purpose of this document is to clarify the process by which employees, contractors, vendors, and other individuals are authorized to access OIT Data Centers and the conditions for controlling that authorized access. Enterprise Operations and Monitoring (EOM) must maintain and operate the OIT Data Centers physical environment in a professional manner, equivalent to what one would expect of a commercial facility.

Data Exchange Policy	The Office of Information Technology (OIT) adopts all necessary measures to ensure that data exchanges with Maine State information assets comply with all relevant Federal and State Laws, as well as the industry best practices of Privacy and Security.
Drone Policy	This policy sets forth guidelines for appropriate Unmanned Aerial Vehicle (UAV) (also known as "drone") use by State of Maine Executive Branch personnel.
OIT policy on Access to Data and Information on State Owned Computer Devices	The responsibility for responding to Freedom of Access Act1 requests for data or information that is hosted on state-owned computer devices falls to the State department and/or agency responsible for the collection and use of the data or information requested. The Office of Information Technology (OIT) will provide assistance to the department or agency with searching for, identifying all data stored within OIT, retrieving, and/or compiling such data or information when requested to do so. The purpose of this policy is to set forth the respective responsibilities of State departments and agencies, and the Office of Information Technology, in responding to Freedom of Access Act requests for data or information that is hosted on state-owned computer devices
Information Privacy Policy	Within the operations of the State of Maine all implementations of information and telecommunication technologies will protect the confidentiality of all non-public records that are collected from respondents through State of Maine information collection activities or from other sources and that is maintained on State systems. For the purposes of this policy the information termed "non-public records" is limited to those records excepted from definition as "Public Records" in Title 1 MSRA §4021. The purpose of this policy is to define the responsibilities of State personnel and the implementation requirements of State information and telecommunications systems to prevent the unauthorized disclosure of information.

Mobile Device Policy	The Office of Information Technology (OIT) takes all necessary measures to ensure the security, and acceptable performance, of the State network. This Policy defines the criteria for access to State Information Assets from mobile devices. Any mobile device that connects to State Information Assets must comply with this Policy, irrespective of whether such a device is personal or State-issued.
Network Device Management Policy	. The Office of Information Technology (OIT) takes all necessary measures to ensure the security, and acceptable performance, of the State network. This Policy defines the rules that apply to devices, which are not managed by OIT, seeking to attach to the Statewide Area Network.
Off-Hours Coverage Policy	This policy establishes customer expectations and identifies staff compensation for OIT Off-Hours coverage. The services furnished by OIT are important to the operation of Maine State government. In order to respond to issues, both planned and unplanned, OIT Employees are occasionally called to duty outside of their scheduled work week. This policy defines the default Off-Hours support that Agency customers can expect from OIT, as well as the compensation OIT Employees can expect for working outside their scheduled (typically 40-hour) work week.
OIT Building Access Procedures	It is the responsibility of the OIT Security Officer to provide a secure and stable physical environment. The purpose of this document is to clarify and delineate the process by which employees, contractors, vendors, and other individuals are authorized for access, and the conditions for controlling that authorized access.

Personnel Security Policy and Procedure (PS-1)	This policy establishes the Office of Information Technology's personnel security policy and procedures governing screening and access to the State's information technology systems and assets. It is a system of policies and procedures which seek to manage the risk of permanent, temporary, and contract staff trusted with access to State of Maine information systems and assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data. This policy corresponds to the Personnel Security (PS) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800- 53.
Physical and Environmental Protection Policy and Procedures (PE-1)	This policy establishes the State of Maine's information technology physical and environmental protection. This corresponds to the Physical and Environmental Protection (PE) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).
Program Management Policy and Procedures (PM-1)	The purpose of this policy is to provide oversight for organization-wide information security programs to help ensure the confidentiality, integrity, and availability of information processed, stored, and transmitted by State of Maine information systems. The Program Management family provides security controls at the organizational level rather than at the information system (see Definitions) level. This corresponds to the Program Management (PM) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).1
Risk Assessment Policy and Procedures (RA-1)	The purpose of this document is to outline the Office of Information Technology's (OIT's) policy and procedures for assessing and addressing security risks. This policy corresponds to the Risk Assessment Control Family of the National Institute of Standards and Technology (NIST), Special Publication 800-53 (Rev. 4).

Security Awareness and Training Policy (AT-1)	The purpose of this document is to outline the State of Maine's policy and procedures for security awareness and training. This corresponds to the Awareness and Training (AT) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).
Security Planning and Procedures (PL-1)	The purpose of this document is to outline the Office of Information Technology's (OIT's) policy and procedures for security planning. This document corresponds to the Security Planning Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).1
System and Communications Protection Policy and Procedures (SC-1, SC-7, and SC-8)	The purpose of this document is to outline the State of Maine's policy and procedures for the protection of Agency information systems and their communications. This corresponds to the System and Communications Protection (SC) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4)1.
System and Communications Protection Procedures for Encryption Mechanisms (SC12, 13, and17)	The System and Communications Protection Procedures for Encryption Mechanisms detail State of Maine (SOM) procedures to leverage multiple layers of security measures to protect the organization's assets. The security controls detailed in this document align with select SC controls detailed in National Institute of Standards and Technology (NIST) Special Publication 800-53.
System and Information Integrity Policy and Procedures	The purpose of this document is to define the State of Maine policy and procedures that are in place to ensure system and information integrity for State of Maine information assets (see Definitions). This part of the security program is focused on protecting the confidentiality (see Definitions), integrity (see Definitions), and availability (see Definitions) of State information assets. This document corresponds to the System and Information Integrity Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

System and Services Acquisition Policy and Procedures (SA-1)	The purpose of this document is to establish the Office of Information Technology's (OIT) policy and procedures for the effective implementation of security controls and control enhancements in the System and Services Acquisition family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4)1. This policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.
User Device and Commodity Application Policy	Maine State information and communication technology exists exclusively for official Maine State business. The purpose of this Policy is to ensure that Maine State information and communication technology is best positioned to facilitate official Maine State business, while complying with relevant Federal and State laws, as well as general industry best practices. This policy also contains directives regarding allowable applications, both resident on the device, as well as consumed remotely.
Vulnerability Scanning Procedure (RA-5)	The purpose of this document is to define the Office of Information Technology's (OIT's) procedures for assessing cybersecurity vulnerabilities through proactive scanning of information assets (see Definitions) and addressing vulnerabilities in a timely fashion. It falls under the umbrella Risk Assessment Policy. More specifically, this document corresponds to the Control RA-5, Vulnerability Scanning, including Control Enhancement (CE) numbers 1 through 3, and 5 of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

Appendix B

Table 2

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.	Identify
Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access or stealing code signing certificates to help with Defense Evasion.	Identify
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.	Protect
Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.	Protect
Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.	Detect

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include: SYSTEM/root level local administrator user account with admin-like access user accounts with access to specific system or perform specific function These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.	Detect
Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross listed here when those techniques include the added benefit of subverting defenses.	Protect
Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.	Identify
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.	Respond
Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.	Detect

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.	Protect
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim’s network structure and defenses.	Detect
Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they’ve collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission.	Protect
Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries’ goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.	Recover

Appendix C

Table 3

Identify	The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
Protect	The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
Detect	The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.
Respond	The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
Recover	The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Appendix D

Table 4

NIST/MITRE Rubric AC-1 Example

Function	Description	Aligns with NIST Functions and mitigates a majority techniques - 5 points	Aligns with NIST Functions or Mitigates a majority Techniques - 4 points	Does not Align with NIST Functions or mitigate a majority of Techniques - 3 points	Does not Align with NIST Functions or mitigate Techniques - 2 points	Does not Align with NIST Functions and does not mitigate Techniques 1 points	N/A - 0 points
Identify	The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.		AC-1 identifies and corresponds with many of the risk factors. It covers nearly all of the Identify Category.				
Protect	The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.		AC-1 aligns with this function but does not mitigate a majority of the techniques. It relies heavily on the experience and actions of OIT Personnel.				
Detect	The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.			AC-1 does not align with this function and a majority of Techniques are not mitigated.			
Respond	The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.						AC-1 does not have nor is responsible for responding to incidents
Recover	The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.						AC-1 does not have nor is responsible for recovering from incidents

Appendix E

Table 5

Policy	NIST Function Alignment	Identify	Protect	Detect	Respond	Recover	Grade
Access Control Policy AC-1	Identify/Protect	4	4				80%
Audit Policy	Identify	5					100%
OIT policy on Access to Data and Information on State Owned Computer Devices	Identify/Protect	3	4				70%
Personnel Security Policy and Procedure (PS-1)	Identify/Detect	5		4			90%
Risk Assessment Policy and Procedures (RA-1)	Identify/Respond	4			3		70%
Security Awareness and Training Policy (AT-1)	Detect/Respond			3	4		70%
Security Planning and Procedures (PL-1)	Respond				4		80%
System and Communications Protection Policy and Procedures (SC-1, SC-7, and SC-8)	Protect		5				100%
System and Communications Protection Procedures for Encryption Mechanisms (SC12, 13, and17)	Protect			4			80%
System and Information Integrity Policy and Procedures	Protect/Respond/ Recover		3		4	3	67%
Vulnerability Scanning Procedure (RA-5)	Identify	5					100%

Appendix F

Table 6

Policy	CIS Critical Control Aligned policy	How does this policy impact electrical Infrastructure?	Does this policy pertain to Cybersecurity?	In Scope
Access Control Policy AC-1	CIS Control 6: Access Control Management	Access control dictates the means to access IT infrastructure supporting the Electrical grid.	Yes	Yes
Audit Policy	CIS Control 8: Audit Log Management	Audits are carried out on Electrical Infrastructure systems	Yes	Yes
OIT policy on Access to Data and Information on State Owned Computer Devices	CIS Control 6: Access Control Management	All devices associated with this study are state owned. This has an impact on the grid.	Yes	Yes
Personnel Security Policy and Procedure (PS-1)	CIS Control 5: Account Management	This pertains to access to government information and networks; this includes the Grid and its networks. This is relevant to the study.	Yes	Yes
Risk Assessment Policy and Procedures (RA-1)	CIS Control 13: Network Monitoring and Defense	Any risk assessment of government infrastructure is going to impact grid security	Yes	Yes
Security Awareness and Training Policy (AT-1)	CIS Control 14: Security Awareness and Skills Training	All personnel involved in the grid will undergo this training. It directly impacts the operations of the grid.	Yes	Yes
Security Planning and Procedures (PL-1)	CIS Control 4: Secure Configuration of Enterprise	The policy impacts the grid through planned security procedures.	Yes	yes

	Assets and Software			
System and Communications Protection Policy and Procedures (SC-1, SC-7, and SC-8)	CIS Control 4: Secure Configuration of Enterprise Assets and Software	This pertains to the protection of system information. This directly impacts the security of the grid.	Yes	yes
System and Communications Protection Procedures for Encryption Mechanisms (SC12, 13, and17)	CIS Control 3: Data Protection	This pertains to the protection of system information. This directly impacts the security of the grid.	Yes	yes
System and Information Integrity Policy and Procedures	CIS Control 12: Network Infrastructure Management	This defines the procedures for data integrity, confidentiality, and availability. This has a partial impact on the security of the grid.	Yes	Yes
Vulnerability Scanning Procedure (RA-5)	CIS Control 7: Continuous Vulnerability Management	This process will scan the grid's assets and networks. It has a direct impact on the security of the grid.	Yes	Yes

Appendix G

- White House Office of Management and Budget (OMB) Circulars
    - OMB Circular A-130 [PDF]
- OMB Memoranda
    - M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management [PDF] (June 15, 2017)
    - M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information [PDF] (Jan 3, 2017)
    - M-17-02, Precision Medicine Initiative Privacy and Security [PDF] (Oct 21, 2016)
    - M-16-19, Data Center Optimization Initiative (DCOI) [PDF] (August 1, 2016)
    - M-16-15, Federal Cybersecurity Workforce Strategy [PDF] (July 12, 2016)
    - M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government [PDF] (October 30, 2015)
    - M-15-16, Multi-Agency Science and Technology Priorities for the FY 2017 Budget [PDF] (July 9, 2015)
    - M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland [PDF]
- Presidential Executive Orders (EO)
    - EO 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
    - EO 13691 - Promoting Private Sector Cybersecurity Information Sharing
    - EO 13681 - Improving the Security of Consumer Financial Transactions
    - EO 13636 - Improving Critical Infrastructure Cybersecurity

    - EO 13556 - Controlled Unclassified Information
- Presidential Policy Directives (PPD)
    - PPD 41 - United States Cyber Incident Coordination
    - PPD 21 - Critical Infrastructure Security and Resilience
- Homeland Security Presidential Directives (HSPD)
    - HSPD 20 - National Continuity Policy [PDF]
    - HSPD 12 - Policy for a Common Identification Standard for Federal Employees and Contractors
    - DHS Presidential Directives
- Federal Emergency Management Agency (FEMA) Directives
    - Federal Continuity Directive 1 - *Federal Executive Branch National Continuity Program and Requirements* [PDF]

The OMB Circular No. A-130 Covers Managing Information as a Strategic Resource. Its two appendices cover responsibilities for protecting and managing federal information resources and responsibilities for managing personally identifiable information (PII)

The OMB Memoranda Covers eight different policies that each cover a different aspect of cybersecurity.

M-18-02 Provides reporting guidelines and deadlines for agencies adhering to FISMA, 2014. This Memorandum consolidates requirements from previous OMB annual FISMA guidance.

M-17-12 This memorandum is not relevant to this study.

M-17-02 This memorandum is not relevant to this study.

M-16-19 This memorandum is not relevant to this study.

M-16-15 This memorandum is not relevant to this study.

M-16-04 This is initiating a cybersecurity sprint designed to identify, prioritize, and develop effective cybersecurity policies and practices. It provides a set of objectives and actions to establish cybersecurity best practices.

M-15-16 sets the priorities of government agencies regarding cybersecurity research and innovations. It emphasizes nine R&D priorities and STEM Education investments.

M-10-28 is the oldest active memorandum regarding cybersecurity and clarifies the responsibility of government agencies in implementing FISMA 2002.

Five Executive orders are still active regarding cybersecurity.

EO 13800 issued on May 11th, 2017, to improve the nation's cyber posture and capabilities. DHS, the American Technology Council (ATC), the OMB, and key government stakeholders' addressed cybersecurity and Critical Infrastructure priorities in this Executive Order.

EO 13691 issued on February 13th, 2015, and covers eight sections supporting private sector information sharing, especially regarding policies, standards, critical infrastructure programs, and definitions.

EO 13681 issued on October 17, 2014, and is irrelevant to this study.

EO 13636 issued on February 12th, 2013, with twelve sections regarding critical infrastructure cybersecurity and the agencies responsible for it. It identifies what infrastructure is vital and the steps to take to ensure that they are sufficiently protected and recognized.

EO 13556issued on November 04, 2010, and covers establishing an open uniform program for managing information that must be protected or disseminated by law, regulations, and government policies.

Two presidential policy directives (PPD) regarding cybersecurity remain active.

PPD 41 issued on July 26, 2016, and sets forth principles governing the federal government's response to any cyber incident.

PPD 21 issued on February 12th, 2013, and establishes national policy on critical infrastructure security and resilience.

Appendix H

Title 24-A, §2266: Notification of cybersecurity event

Title 24-A, §2264: Information security program

Title 24-A, §2265: Investigation of cybersecurity event

Title 24-A, §2263: Definitions

Title 24-A, Chapter 24-B: MAINE INSURANCE DATA SECURITY ACT

Title 24-A, §2262: Construction

Title 35-A, §3143: Declaration of policy on smart grid infrastructure

Appendix I

	Identify	Protect	Detect	Respond	Recover
Reconnaissance	9	1			
Resource Development		6	2		
Initial Access		5	4		
Execution			14		
Persistence			13	1	
Privilege Escalation			13		
Defense Evasion	1	4	30	7	
Credential Access	2	7	7		
Discovery	29		2		
Lateral Movement		3	6		
Collection	1	6	3	6	
Command and Control		1	11	4	
Exfiltration		6	1	2	
Impact				1	12