STATE OF CONNECTICUT

PUBLIC UTILITIES REGULATORY AUTHORITY

Connecticut Public Utilities Cybersecurity Action Plan

Connecticut Public Utilities Regulatory Authority

Docket No. 14-05-12
PURA Cybersecurity Compliance Standards and Oversight Procedures

April 6, 2016

Arthur H. House, Chairman

Stephen M. Capozzi, Lead Staff

1. Executive Summary

Public utilities in Connecticut and throughout the United States face the credible danger of cyber penetration, compromise and disruption. National deterrence and remediation must include action at the state level including partnership among public utilities, their regulators and emergency response managers. Connecticut's Public Utilities Regulatory Authority (PURA) recognizes the rapidly evolving nature of cyber threats to public utilities and the need for cooperative, flexible collaboration as we strengthen defense. We must also consider unprecedented consequences if or when an attack occurs and plan for the heretofore unseen challenges of recovery as an individual state, as part of the New England/Northeast region and with federal authorities.

With growing national attention to cybersecurity challenges facing public utilities, Connecticut's elected officials recognized the necessity for Connecticut to be a constructive part of future solutions and help protect the state's critical public utility infrastructure. The Governor and legislative leaders made it clear that they need to be assured that Connecticut's public utility companies are taking necessary steps to address challenges in the cybersecurity landscape. On April 14, 2014, Governor Malloy accompanied by legislative leaders and representatives of Connecticut's utilities, issued the Public Utilities Regulatory Authority strategic plan "Cybersecurity and Connecticut's Public Utilities," which presents a roadmap to strengthen the state's cybersecurity defenses.

Since release of Connecticut's strategic plan there has been extensive public discussion of cybersecurity challenges facing public utilities. Several national officials and cybersecurity experts have warned of the increased sophistication of cyber attack tools and systems, broader range of threats and more thorough penetration of public utilities as well as other sectors such as finance, industry and communications. In February 2016 the U.S. Department of Homeland Security warned U.S. power companies that the technology deployed in shutting down parts of the power grid in the Ukraine in December 2015 confirmed that cyber attacks could disable American utilities. Admiral Michael Rogers, Director of the National Security Agency and head of the United States Cyber Command, warned in March 2016 that what he termed the "well-crafted attack" led to the conclusion that at some point the United States will see such action against critical infrastructure in our country.

As a follow-up to its April 2014 report, PURA held a series of collaborative technical meetings with the state's public utility companies to review the standards and guidelines they currently follow as part of their cybersecurity risk management programs. While the utility companies use cybersecurity risk management standards, PURA needs to be satisfied that their programs are effective in decreasing vulnerability to cyber attacks.

In short, PURA has sought to accomplish its cybersecurity directive through collaboration with Connecticut's public utilities. Together, we have been exploring ways to review the adequacy of cyber defenses, reaching concurrence on standards and holding annual meetings with government participants. This voluntary collaboration has produced new solutions for enhanced cybersecurity, public understanding of such collaboration and rudimentary plans with the electricity, natural gas and water sectors. PURA is grateful for the goodwill the leaders of these sectors have demonstrated.

Unfortunately, agreement was not reached in the telecommunications sector. The majority of telecommunications companies responding to the draft of this report expressed the view that the proposed meetings and guidelines for information reporting would, in fact, be compulsory and comprise a mandate, which they consider to be in conflict with federal policy preference for voluntary mechanisms. While it has been PURA's goal that all public utilities and telecommunications service providers operating in Connecticut participate in the state's cybersecurity oversight program, most telecommunications companies to date have refused to join the effort.

PURA will move forward with companies in the three sectors that have chosen to cooperate, and hopes to create both constructive processes and public confidence that will eventually include the telecommunications companies doing business in Connecticut.

In this report, PURA discusses standards and guidelines and the prospect of a Public Utility Company Cybersecurity Oversight Program, wherein the companies will have the opportunity to demonstrate, through annual meetings with government stakeholders, that they are adequately defending against cyber attacks. Government stakeholders include the Public Utilities Regulatory Authority and the Division of Emergency Management and Homeland Security (DEMHS) meeting with the utilities and reporting to the Governor, the General Assembly and the Office of Consumer Counsel. During these annual meetings, the companies are expected to report on their cyber defense programs, experiences over the prior year dealing with cyber threats and corrective measures they expect to undertake in the coming year.[1]

PURA recognizes the changing nature of the cybersecurity landscape and has designed its oversight program to be flexible and to improve over time. That is, this program aims to accommodate the critical components of each industry's infrastructure as well as the size and operational scope of each company. PURA expects this program to evolve with experience as the players learn, share perspectives and concerns and work together to protect Connecticut from the alarming dangers of cyber disruption.

2. The Setting

[1] PURA's Cybersecurity Oversight Program reporting requirements will be limited to annual cybersecurity review meetings and will not require the utilities to submit formal, written reports.

The Public Utilities Regulatory Authority on April 14, 2014, issued a strategic plan, entitled "Cybersecurity and Connecticut's Public Utilities" (PURA Strategic Plan), to help strengthen Connecticut public utility cybersecurity defense. PURA shared this Strategic Plan in advance with Connecticut's public utilities to allow them to understand it and to offer and incorporate their thoughts and perspectives. Governor Dannel P. Malloy announced the PURA Strategic Plan in the presence of representatives from the General Assembly and senior public utility officials. The Governor's charge was to proceed with the PURA Strategic Plan to strengthen cybersecurity in Connecticut's public utilities.

A key point underscored by the Strategic Plan was that communication among Connecticut elected officials, the leadership of Connecticut utilities, public utility regulators and Connecticut's emergency management personnel must be structured and enhanced. DEMHS has a program of periodic consultation with Connecticut's utilities on related matters that provides a constructive foundation for further progress. Public officials must be able to assure their constituents that the officials have a basic understanding of work being done to strengthen cybersecurity. The utilities indicated a strong preference for achieving such enhanced communication through voluntary collaboration, rather than legislation, executive order or regulatory mandate.

In crafting an effective plan against a cyber attack on our public utilities, there is an inherent tension between alarmism and complacency. While probes hit utilities daily, if not hourly, and there have been worrisome instances of compromise, we have not yet lost vital public utility services for a serious duration. It is possible that there will never be a major, successful cyber attack. We should not give in to hysteria or panic in a modern version of Henny Penny's alarm that the sky is falling. At the same time, we need to recognize the risks and consequences of cyber disruption. Given the motivations and capabilities of those who seek to damage the United States, the increasingly accessible means for committing cyber crime and the difficulty of thwarting attacks with hidden attribution, we need to recognize that there will likely be a utility cyber disruption at some point. And given the extent to which both our quality of life and sheer survival depend upon modern utilities, the nascent area of recovery management deserves serious, urgent attention.

Managing cybersecurity in public utilities needs to be a function integrated with both information technology and other forms of risk management. In some smaller companies, such as water utilities, cyber defense is often managed by the chief information officer. Damage inflicted by a cyber attack could be facilitated and amplified by concurrence with another disruption such as a flood, hurricane or ice storm. An attacker could also enhance damage by use of an "intentional electromagnetic interference device," an evolving weapon capable of knocking out a substation or other facility from a mile away. While possible scenarios are alarming, assessment of required defenses and recovery plans require that they be considered.

Journalist Ted Koppel's 2015 book, "Lights Out," adds fresh reporting and authoritative discussion to this subject. He presents assertions previously reported in the media, discussed in unclassified reports and informally weighed by government officials of foreign penetration of U.S. utility control and operating systems. Koppel’s reporting and extensive discussions with national security officials underscores an awkward situation. National security officials' top-level security clearances give them access to intelligence with regard to threats to public utilities. But the leaders and operators of U.S. utilities, with a few exceptions, do not have such clearances. Hence those at the helm do not have all the pertinent intelligence that would permit candid, factual discussions of existing reality.

Federal officials state bluntly that many U.S. public utilities have been penetrated, they do not know that they have been penetrated, and that foreign actors have the ability to "pull the trigger" to knock out utility services extensively in the United States. Some federal officials such as National Security Agency Director Admiral Michael S. Rogers have publicly stated what many refer to indirectly: that non-American groups currently have the ability not just to enter American utilities, but to bring them to their knees. After assessing the December 2015 cyber attack on Ukraine, Admiral Rogers in March 2016 strengthened his warning by stating that the “well-crafted attack” that led to the Ukrainian blackout forced his conclusion that “It is only a matter of the when, not the if, you are going to see a nation state, a group or actor, engage in destructive behavior against critical infrastructure in the United States.”

In remarks delivered on “National Intelligence, North Korea, and the National Cyber Discussion” at the International Conference on Cyber Security on January 7, 2015, Director of National Intelligence James R. Clapper noted the need for state governments to work with federal agencies and commercial partners on the evolving cyber threat.

Indeed, federal officials and national cyber experts have noted, without citing specific companies, that U.S. public utilities have been penetrated and have expressed concern that foreign powers could decide to harvest their penetration. The fact that penetration and compromise are possible or have already taken place suggests that Connecticut should pay attention not just to cyber threats, but also to recovery in this state and the New England region.

As Koppel also reveals, officials sometimes downplay or dismiss too casually Russia's and China's sophisticated cyber skills as well as their ability to penetrate U.S. utility operations. The logic is that there is a rough parallel between the Cold War concept of bilateral, mutually assured nuclear destruction and today's offensive cyber capabilities among the United States, Russia and China. That is, a cyber attack being an act of war, Russia and China would be deterred from “pulling the trigger” to exploit their existing penetrations of U.S. utilities because of the threat of American retaliation.

There are at least two reasons to avoid the false sense of security that comes from this Cold-War era mentality.

The first is that the examples of the Stuxnet computer virus in Iran, Russian military operations in Georgia and the Ukraine, a recent attack on the Ukrainian power grid and North Korea's actions against Sony Corporation demonstrated that offensive cyber capabilities can be both effective and to some extent, anonymous. Despite the difficulty of attribution, the link between North Korea's displeasure over a film produced by Sony and resulting cyber attacks on Sony in late 2015 has been substantially corroborated. While some speculate that the United States and Israel were involved in Stuxnet, there has been no tangible proof. Russian cyber warfare has been difficult to disguise in operations against Georgia and the Ukraine, but more difficult to prove are the allegations that subsequent, retaliatory cyber attacks against American financial institutions by actors in Russia and Eastern Europe were directed or implicitly endorsed by Russian authorities.

A major instance of a cyber attack directly targeting electric power systems was reported on December 23, 2015 by Ukrainian authorities in the capitol and western regions. American investigators concluded that it appears to have been the first utility power blackout caused by a cyber attack. What was described as a coordinated, multi-pronged, digital attack including use of the "BlackEnergy 3" strain of malware developed by a group called the "Sandworm Team" was directed at industrial control systems. The attackers stole system operator's credentials, switched off breakers and disabled electric control systems, causing several hours of power outage in winter conditions for more than 225,000 Ukrainians.

Investigations by American cyber experts in the Ukraine have concluded that the attacks began in the spring of 2015 with a spear-phishing campaign targeting system administrators and information technology staff with a malicious Word document. That document offered a popup that infected systems and opened backdoors allowing hackers to enter supervisory control and data acquisition systems (SCADAs), setting the state for the attack. The cyber assault may have involved both cybercriminals and nation-state actors (probably Russian). The strike hit and took offline about 30 substations and breakers in attacks coordinated to occur within 30 minutes of one another. The interruption also involved a telephone denial-of-service attack to prevent customers from reporting outages. The strike force also hit backup power supplies at two distribution centers, which left operators seeking restoration without power. Service restoration within hours was facilitated by the ability of Ukrainian electricity distributors to use manual operation controls. Control systems in the United States are more highly automated than those in Ukraine, suggesting that restoration by manual operation would be more difficult here.

While exact attribution has not been proven, Ukraine blames Russia, and it has been suggested that the Russian military or Russian "patriotic hackers" were involved. The attackers wiped many of the penetrated systems clean with "KillDisk," thereby erasing files on the systems and eliminating records of human interaction with the computer systems. The incident is a concrete instance of what has been widely known as possible: cyber attacks can shut down public utilities, deny wide populations services necessary for survival and escape precise attribution.

In late February 2016 the U.S. Department of Homeland Security provided an account of the attack (IR-Alert-H-16-056-01) in the Ukraine based on the work of American investigators. Its Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) described the attack in the Ukraine and stated that it "strongly encourages organizations across all sectors to review and employ the mitigation strategies" it lists, which include best practices, review of procurement and licensing of trusted hardware and software systems, prompt patching of systems, refreshed review of strategic technology and limited remote access functionality.

The second reason for ongoing concern is that private and quasi-private mercenary cyber warriors are plentiful and sophisticated. North Korea, Iran, Syria, non-state actors such as ISIS or even an individual with enough money can pay for a cyber attack on the United States. Many knowledgeable in the field believe such attacks have already taken place. It would be possible for an entity seeking to damage the United States to hire cyber actors to replicate of existing penetrations of U.S. utilities or to design new ones – and then execute. To be explicit, our concern cannot end with thinking about how to counter an attack from Russia or China. The capability to shut down American utilities is available for purchase, and should it happen, it may not be possible to complete attribution. Extremists, the deranged and sovereign governments can wreak unprecedented damage on our country.

A concern discussed at the federal level is the nature and duration of potential damage. Koppel has put into print what others previously discussed privately: entire areas of the United States (meaning several contiguous states) could be without electricity, gas and water for months at a time. Outside the military, the American public has not weighed the consequences of protracted suffering and desperation resulting from: the absence of heat in the winter; depletion of water, food and pharmaceutical products; the public health hazards of the inability to dispose of human waste; the absence of fuel to drive away from these deprivations; the inability of neighboring regions to offer relief; and restricted or absent mobile and landline communications, Internet, and financial services.

The military has contingencies for martial law and emergency counter-measures to doomsday scenarios, but state and local emergency management systems are not prepared. Koppel summarizes the understandable shortcomings in preparation for a protracted utility outage:

> "There are emergency preparedness plans in place for earthquakes and hurricanes, heat waves and ice storms. There are plans for power outages of a few days, affecting as many as several million people. But if a highly populated area was without electricity for a period of several months or even weeks, there is no master plan for the civilian population."

Former Assistant Secretary of Defense for Homeland Defense and America's Security Affairs Paul Stockton addressed recovery management in a March 2016 paper published by the Johns Hopkins University Applied Physics Laboratory. Stockton states that the factors that enabled effective power restoration after Superstorm Sandy, "are absent in the cyber realm." Stockton noted that the Sandy recovery drew on the Department of Homeland Security's National Response Framework for response to natural disasters. It called on tens of thousands of linemen, engineers and personnel from more than 80 utilities and formed the largest deployment of such assistance in American history with federal, state, private sector and National Guard involvement. Stockton wrote, "The equivalent document for the cyber realm – the interim National Cyber Incident Response Plan – would almost surely prove inadequate just when the United States needed it most." A critical shortfall of the existing interim plan is that it provides the state governors "with only a minimal role in guiding cyber response efforts, even though state National Guard organizations will likely plan an increasingly significant role in supporting power restoration and other response operations."

In this vein, others have called for the creation of a "cyber mutual assistance program" among states that could identify critical professional skills and equipment that would be needed in the event of a cyber attack on public utilities. States currently have mutual assistance programs for power restoration after storm damage; a cyber mutual assistance program could build on that precedent and prepare for the special needs a cyber attack could present.

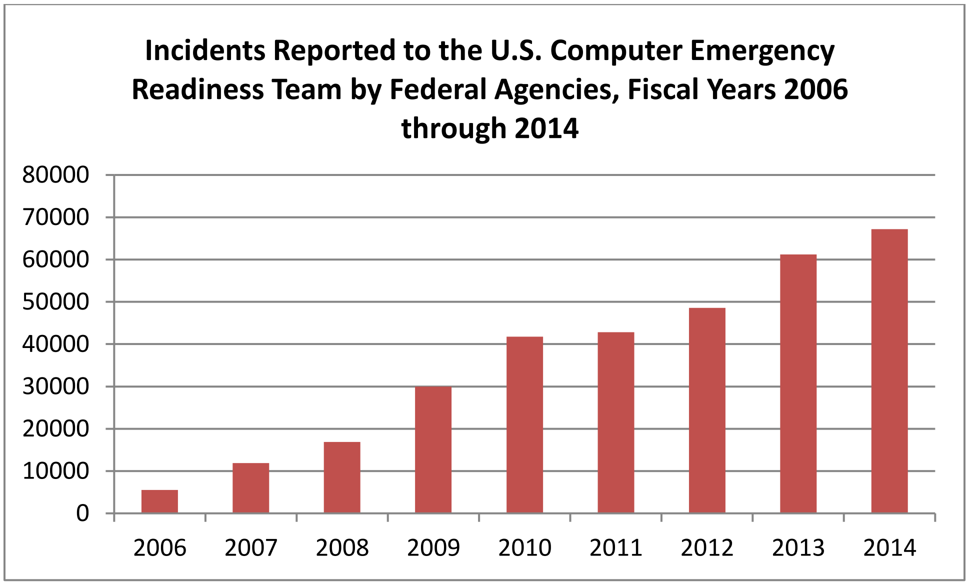
The PURA strategic plan recognizes the importance of establishing a monitoring system that can adapt to the changing landscape of the cybersecurity threat to Connecticut's public utilities. It also notes the importance of accommodating the cyber challenges faced by companies in the different utility sectors, which vary by size and scope of operations. PURA seeks to establish a program that promotes a culture of security, which transcends compliance and encourages dynamic risk management and continual security improvement relative to the threats facing any given utility. And PURA seeks further attention to the new challenges that Connecticut, New England and the United States would face in recovering from a public utilities cyber attack.

As a result, PURA initiated Docket No. 14-05-12 PURA Cybersecurity Compliance Standards and Oversight Procedures to address the points raised in the PURA Strategic Plan. As part of that proceeding, PURA conducted a series of collaborative technical meetings with Connecticut's electric, gas, water and telecommunications public utility companies. The goal of the meetings was to define standards that would enable PURA to determine whether the utility companies were taking adequate, proactive steps to manage cybersecurity.

3. **Updates and Federal Initiatives**

Since PURA initiated Docket No. 14-05-12, there have been several well-publicized events and developments underscoring the increasing frequency and severity of cyber threats and disruptions. These range from the cyber attacks on Sony Pictures Entertainment and the health insurer Anthem Inc. to the attacks on federal agencies. The federal Office of Personnel Management discovered two separate cybersecurity incidents in April and June of 2015. These attacks resulted in the theft of personnel data of several million current and former federal government employees, their relatives and their personal and business associates. Additional information on federal employees and contractors, such as their background investigation records, was also compromised.

To further underscore the increasing number of cyber incidents at the federal level, an article in the Washington Post used this chart to illustrate the cyber incidents involving federal agencies over the past nine years.



Source: June 18, 2015 Washington Post article and Government Accounting Office analysis of United States Computer Emergency Readiness Team data for fiscal years 2006 - 2014.

A number of cybersecurity frameworks have been defined by federal agencies and industry consortia, which may be of use in establishing compliance standards and oversight procedures under Docket No. 14-05-12. These federal-level initiatives include:

1. North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards;

2. National Institute of Standards and Technology (NIST) Cybersecurity Framework;

3. Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2);

4. American Water Works Association's (AWWA) Process Control System Security Guidance for the Water Sector; and

5. Federal Communications Commission (FCC) Communications Security, Reliability and Interoperability Council IV (CSRIC IV) Cybersecurity Risk Management and Best Practices, Working Group 4 Final Report.

The NERC CIP standards and associated compliance framework comprise the only mandatory federal cybersecurity framework for the utility industry. The others are frameworks intended to organize and present industry best practices and security controls; they are not mandatory, they do not establish minimum standards, and they do not specify compliance criteria.

a) **NERC CIP**

In 2007, the Federal Energy Regulatory Commission (FERC), which regulates the interstate transmission of electricity, natural gas and oil, designated the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO) for the U.S. electric grid. As the ERO, the NERC is responsible for developing and enforcing compliance with mandatory reliability standards to include cybersecurity requirements. To this end, the NERC developed cybersecurity standards and requirements, which are referred to as the Critical Infrastructure Protection (CIP) standards and requirements.

NERC CIP standards and requirements apply to Bulk Electric System (BES) Cyber Systems. BESs are generation and transmission facilities and their control systems that are part of the North American interconnected power grid. BESs generally operate at or above 100 kVolts. Compliance with the CIP standards and requirements is mandatory for all users, owners and operators of BESs in the United States. Penalties for non-compliance with the NERC CIP include fines and/or sanctions. Distribution facilities are not considered to be BESs, and therefore, not formally subject to NERC CIP compliance.

The NERC CIP requires BES owners and operators to monitor security events and to have comprehensive contingency plans to respond to cyber attacks, natural disasters and other disruptive events.

NERC CIP Version 5 (Version 5) was approved in 2013 and will become enforceable in 2016 and 2017.[2] Version 5 is considered an enhancement to Version 3 and includes additional standards for Configuration Change Management and Vulnerability Assessments (CIP-010), Information Protection and Media Sanitization (CIP-011) and Physical Security (CIP-014). Version 5 extends the scope of the systems to which it applies and is intended to focus on improving security posture, rather than focusing on compliance alone.

[2] Although there is a CIP Version 4, it is being bypassed in favor of Version 5.

The NERC conducts a number of outreach programs to improve the physical security and cybersecurity of the North American bulk power system. One example is the NERC-sponsored Grid Security Exercise (GridEx), a North American-wide, biennial physical security and cybersecurity exercise. GridEx exercises test the electricity sector's response to simulated cybersecurity and physical security incidents to strengthen crisis response functions and to capture and share lessons learned. GridEx I took place in November 2011, GridEx II in November 2013, and GridEx III November 2015.

b) NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) issued a "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0 (Framework), on February 12, 2014. NIST prepared the Framework in collaboration with government and industry stakeholders to establish a voluntary, risk-based Cybersecurity Framework and to identify a "set of industry standards and best practices to help organizations manage cybersecurity risks." The Framework is not a standard, as such, but instead serves as a common language and structure for developing, managing and describing cybersecurity programs. As the Framework states, it is "a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on business." It is also a methodology that enables organizations "to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure." The Framework is subject to updates and improvements as government and commercial entities apply it to their needs.

The Framework is a process and template for discussion, not a set of required standards or a code of compliance. It does not provide explicit guidance for what cyber defenses should be implemented or for how to achieve an acceptable state of security. PURA may mirror the Framework terminology and concepts when discussing cybersecurity with utilities, but the Framework does not represent a definitive set of compliance standards.

c) DOE ES-C2M2

The U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2) provides a voluntary evaluation process that can be used to measure the maturity of an organization's cybersecurity program relative to industry-recognized best practices and to identify opportunities for improvement. The C2M2 developed for the Electricity Subsector (ES) is referred to as the ES-C2M2.

The C2M2 is not intended to form the basis of regulated compliance programs. Rather, it is intended to facilitate an organization's self-evaluation of the maturity and robustness of its cybersecurity risk management program. Such evaluations are performed at a strategic level and do not represent detailed audits, vulnerability assessments or penetration tests. The self-evaluations are not mandatory.

The ES-C2M2 focuses on the implementation and management of Information Technology (IT) and Operations Technology (OT) assets and their environments. The objectives of the model are to:

- Effectively and consistently evaluate and benchmark cybersecurity capabilities;
- Strengthen an organization's cybersecurity capabilities;
- Share knowledge, best practices and references; and
- Prioritize actions and investments.

Overall, the guidance provided in the ES-C2M2 is descriptive, not prescriptive, and topics are covered at a high level of abstraction. The model is organized along 10 security domains that cumulatively contribute to the overall cybersecurity posture of an organization. The domains are:

1. Risk Management;
2. Asset, Change and Configuration Management;
3. Identity and Access Management;
4. Threat and Vulnerability Management;
5. Situational Awareness;
6. Information Sharing and Communications;
7. Event and Incident Response and Continuity of Operations;
8. Supply Chain and External Dependencies Management;
9. Workforce Management; and
10. Cybersecurity Program Management.

When a utility's cybersecurity program undergoes an assessment in accordance with the C2M2, its maturity level in each domain is expressed as a Maturity Indicator Level (MIL), which can range from MIL0 (an absence of security practices) to MIL3 (extensive implementation of best practices). MILs apply independently to each domain, which means that an organization may be operating at different MILs for different domains.

An MIL rating takes into account both the completeness and development level of cybersecurity practices (Approach Progression) within a domain as well as the extent to which cybersecurity practices are ingrained in daily operations (Institutionalization Progression).

In addition to defining the current state of a cybersecurity program within a domain, an MIL may also be used to establish a target for a more mature state. An organization can identify opportunities for improvement by performing a gap analysis of the practices at the target MIL against those currently followed. Ultimately, opportunities for improving an organization's cybersecurity program should be weighed against business objectives, risk tolerance and cost. The highest MIL in each domain may not be appropriate for every organization. However, the model was developed in such a way that any organization, regardless of size, should be able to achieve MIL1 across all domains.

d) AWWA Process Control System Security Guidance

The American Water Works Association (AWWA), a prominent water sector industry association, works to establish consensus standards for cybersecurity, specifically focused on Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS).[3] The most recent effort to establish water-sector cybersecurity best practices was spearheaded by the AWWA and endorsed by the U.S. Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA). This effort resulted in the AWWA report titled, “Process Control System Security Guidance for the Water Sector” (Process Control System Security Guidance). The goal of this security guidance is to provide water sector utility companies with a recommended course of action to reduce vulnerabilities to cyber attacks. Use of the AWWA guidance is voluntary.

The Process Control System Security Guidance identifies 12 cybersecurity “practice categories.”[4] Under each category, the document recommends specific practices considered the most critical for managing cybersecurity risk in the water sector. The Process Control System Security Guidance identifies 82 cybersecurity controls that describe more granular measures to support implementation of the recommended security practices.

The Process Control System Security Guidance maps the water sector-specific controls to the NIST Cybersecurity Framework. The mapping is intended to demonstrate that the AWWA guidance represents the water sector’s voluntary approach to implementing the NIST Cybersecurity Framework.

e) FCC CSRIC IV WG4 Final Report

The Federal Communications Commission (FCC) Communications Security, Reliability and Interoperability Council IV (CSRIC IV) Cybersecurity Risk Management and Best Practices, Working Group 4 (WG4) Final Report was released on March 18, 2015. The efforts of the WG4 and the resulting report were partially driven by the telecommunications sector’s need to determine how best to apply the NIST Cybersecurity Framework and to consider the potential role of the FCC in the process.

The WG4 Final Report prioritized and analyzed the NIST Cybersecurity Framework security controls for applicability to the communications sector. A detailed analysis was conducted for each of the five major segments of the communications

[3] AWWA refers to ICS as Process Control Systems (PCS).

[4] The 12 AWWA security practice categories are similar to, but different from, the 10 security domains of the DOE’s C2M2.

industry: Broadcast, Cable, Satellite, Wireless and Wireline. Each segment assessed the applicability, implementation difficulty and overall priority of each of the NIST Framework security controls and best practices.

In their respective analyses, the cable, wireless and wireline segments identified about 25 highest priority controls or practices (out of a total of 98). There is considerable overlap among the three segments' lists.

A key recommendation of the WG4 Report is the development of a voluntary program for periodic meetings among the FCC, DHS and individual communications companies. It is anticipated that, during the meetings, the companies would discuss their efforts to develop risk management practices consistent with the NIST Cybersecurity Framework. To quote the report, "During the meetings, the participating companies would share information regarding cyber threats or attacks on their critical infrastructure, and the organizations' effort to respond or recover from such threats or attacks." (WG4 Report, p. 7). This concept of periodic cybersecurity program reviews between individual companies and regulatory authorities is consistent with the oversight procedures that PURA seeks to establish under Docket No. 14-05-12.

4. PURA Technical Meetings

A. Meeting Overview

PURA held a series of collaborative technical meetings with Connecticut's public utility companies to design an approach that would enable PURA to meet the mandate of its strategic plan. Specifically, the meetings sought to find common ground in addressing the following core questions:

1. What standards are appropriate to determine the state of a utility's cybersecurity defense; what progress is being made and what areas require greater attention?

2. With whom should the utilities share assessment of their cybersecurity programs and processes in order to strengthen their programs?

3. What format would be appropriate for reviewing a company's cybersecurity program, and how frequently should reviews take place?

PURA held an initial meeting on January 15, 2015, attended by representatives of all utility sectors, the Office of Consumer Counsel (OCC) and the Attorney General's (AG) Office. The purpose was to set the stage for industry-specific technical meetings, which were held over the course of several months.

A meeting was held on February 4, 2015, with Frontier Communications of Connecticut (Frontier) to satisfy Order No. 4 in the Decision dated October 15, 2014, in

Docket No. 14-01-46, Joint Application of Frontier Communications Corporation and AT&T Inc. for Approval of a Change of Control. Frontier briefed PURA on its cyber defense and management capabilities and the results from a third-party cybersecurity assessment.

A March 5, 2015 meeting focused on the gas and electric utilities, and the attendees included UIL Corporation (UIL) and Eversource Energy (Eversource).

A March 18, 2015 meeting focused on the water industry, and the attendees included Connecticut Water Company, Aquarion Water Company and Valley Water.

A June 16, 2015 meeting focused on the wireline and cable telecommunications industry, and attendees included Frontier, Verizon New York, Inc. (Verizon), AT&T Corporation (AT&T), Cablevision Connecticut (Cablevision), Lightower Fiber Networks I, LLC; Lightower Fiber Networks II, LLC and Fibertech Technologies Networks, L.L.C. (collectively, Lightower), Comcast and Cox Communications (Cox). Also in attendance were representatives from the New England Cable and Telecommunications Association (NECTA), the National Cable and Telecommunications Association (NCTA) and the United States Telecom Association (USTelecom).

A July 23, 2015 meeting focused on the wireless telecommunications industry and included representatives from Verizon, Sprint, T-Mobile and AT&T Corporation.

Based on the discussions and findings from these technical meetings, which included representatives from the OCC and AG, PURA will establish a Cybersecurity Oversight Program, which will be structured and managed for each industry, as described in Section 5 below.

B. Meeting Outcomes

The technical meetings with the utility sectors revealed general willingness to participate in annual cybersecurity reviews with a small number of PURA and Connecticut government stakeholders.[5] Companies reluctant to agree to annual meetings indicated that such meetings might be duplicative with required federal reporting and potentially other states' reporting requirements. Furthermore, some companies expressed reluctance to share detailed information on their security programs (e.g., whether they implemented certain measures, had known vulnerabilities in their systems or provided details concerning cyber breaches) because release of such information could expose them to fines, prosecution and/or litigation.

Utility company representatives expressed preference to leverage their reporting and auditing requirements for various federal regulatory agencies (e.g., NERC, FCC). PURA recognizes the potential burden of duplicative undertakings and reporting

[5] The OCC requested that it be included in the annual cybersecurity meetings with utilities.

requirements and is open to leveraging utilities' existing cyber activities and reporting requirements.

Some utility sectors expressed support for different reporting standards for annual review meetings. For example, the electric and gas companies expressed a preference for using the framework of the DOE ES-C2M2. The water companies considered following the AWWA Process Control System Security Guidance, but subsequently also expressed preference for the DOE C2M2. The telecommunications companies suggested following the WG4 Final Report. Whatever the appropriate framework, the utility companies contended that it was unreasonable to specify which cybersecurity controls or measures a company should implement, because each has business needs that require a unique balance of risk against the cost of risk mitigation.

a) Electric and Gas Meeting Results

Representatives of UIL and Eversource expressed support for an oversight process based on annual meetings between each utility company and Connecticut government stakeholders. However, they are concerned about the potential number of government stakeholders attending those meetings. In addition to limiting attendance to those with a true “need to know,” the companies noted that attendees, many of whom may have only limited cybersecurity backgrounds, may not appreciate the sensitivity of the information being presented and risk inadvertent disclosure. As a result, PURA would require all attendees to enter into non-disclosure agreements and be briefed on sensitive information that could be harmful if discussed outside of the meeting(s). The companies also proposed a confidence-building measure: that the participants agree on external messaging for possible release after the meetings, seeking to inform the public while protecting sensitive defenses.

In light of utility companies' concerns regarding the number of government participants, PURA proposes that the meetings include PURA and DEMHS, each of which would have one Commissioner or Deputy Commissioner and one staff member specialist. This team of two government organizations would then present a report to the Governor or his or her designee, the General Assembly's Energy and Technology Committee leadership and the Consumer Counsel on the results of the annual meetings.

Regarding cybersecurity reporting standards, UIL and Eversource prefer to use the ES-C2M2. They said they are already following the ES-C2M2 for their respective cybersecurity programs and believe it would be more meaningful and easier to use than state reporting requirements. They also suggested that the ES-C2M2 concept of MILs might be useful for reporting to satisfy the PURA reporting requirements. However, they cautioned that numerical indicators may be misinterpreted by uninformed audiences. They also suggested using “heat maps” of their cybersecurity posture as an annual reporting mechanism to convey a general sense of the areas requiring the most attention.

The electric and gas companies opined that ES-C2M2 provides a good structure to frame the cybersecurity discussion, whereas an MIL rating model would be too subjective. Additionally, they were concerned that each company might apply the rating model differently. They do not want the process to be comparative in nature. Moreover, they were uncomfortable with a quantitative rating system for the ES-C2M2 detailed scorings, but would accept reporting maturity levels. They indicated it might be possible and expected that not all security domains would be at the highest level of maturity. Each company would balance the risk and value from moving to a higher level, while explaining their rationale for maintaining a certain maturity level in each category. PURA acknowledged that many factors contribute to a company's maturity level for a specific set of controls and assured the companies that they would be allowed to justify their reporting.

UIL and Eversource indicated that they would adopt and follow ES-C2M2 in support of the PURA process. They claim to have been mapping their own programs against ES-C2M2 during development of the model and have noticed no gaps in either direction between their current programs and the emerging maturity model. However, the extent of coverage for each topic may differ. The companies noted that the ES-C2M2 model provides the framework through which the utilities communicate with DHS and DOE at the federal level.

PURA's consultant, Applied Communications Sciences (ACS), suggested that the companies' reports should describe their operational cybersecurity status over the prior year. Further details should also include discussion of the changing threat environment, level of attacks and number of attacks detected and thwarted. The companies saw this request as already covered by the ES-C2M2 reporting domain.

b) Water Meeting Results

Representatives of Aquarion Water Company (AWC) and the Connecticut Water Company (CWC) participated in the water sector technical meeting. The representatives indicated that their companies are open to participating in annual cybersecurity review meetings. Like the electric and gas utilities, the water companies expressed concern over the potentially large size of the government audience at the annual meetings.

The water company representatives were also concerned about reporting details of how they are addressing specific security controls and the ones they might emphasize. PURA expects all meeting attendees be aware of the sensitivity of that information and ensure its confidentiality.

In discussing reporting standards, PURA mentioned the electric and gas companies' preference for the DOE's ES-C2M2, and ACS suggested the AWWA Process Control System Security Guidance as an alternative. The AWWA Process Control System Security Guidance is geared specifically for water utilities. AWC has been using the AWWA Process Control System Security Guidance to structure and assess its security program. CWC claimed to be investigating the use of the NIST Cybersecurity Framework to structure its security program.

Following the water sector technical meeting, both water companies expressed support for using the DOE ES-C2M2 for their reporting.

AWC and CWC agreed that the choice of security controls to be implemented by a utility should be a function of current threats to their systems, the likelihood of future threats and the potential damage that could result. Both companies expressed a preference for self-reporting on their security posture, rather than mandated third-party assessments, even though they currently use consultants to conduct periodic security audits.

c) Wireline, Cable and Wireless Telecommunications Meeting Results

The telecommunications meetings began with presentations on the CSRIC IV WG4 Final Report with respect to the cable, wireline and wireless sectors. These presentations discussed the voluntary mechanisms the report recommended, which include company-specific meetings with the FCC and DHS, sector annual reports and participation in the Critical Infrastructure Cyber Community C^3 Voluntary Program run by the DHS. The companies and trade associations acknowledged that these mechanisms have not been formalized, and they did not define what actual reporting might take place or what information might be compiled in sector annual reports during company-specific meetings.

NECTA expressed general support of the CSRIC IV WG4 report but emphasized that the report's proposal for annual meetings with the FCC would be voluntary. NECTA also emphasized that the meeting discussions would likely include highly sensitive, company-proprietary information. Thus, the association maintained that the participating companies should be afforded protections against disclosure under the government's Protected Critical Infrastructure Information PCII Program.[6] The telecommunications companies are especially concerned that information divulged in such meetings could expose them to fines, prosecution and/or litigation.

Verizon expressed willingness to participate in closed-door meetings with state regulators to discuss the status of its cybersecurity program, but not to participate in annual meetings with other state officials. Verizon is already required to provide such reports regularly to various regulatory bodies, but it was concerned that, if every state and the 130-plus countries in which it currently operates all required periodic review meetings, such a requirement would be excessively burdensome.

Frontier and AT&T also expressed willingness to work with PURA in developing an annual review process that works for all stakeholders. AT&T indicated that it

[6] Information authorized as PCII satisfies the requirements of the Critical Infrastructure Information Act of 2002 and is protected from the Freedom of Information Act (FOIA), state tribal and local disclosure laws, uses in regulatory actions and civil litigation proceedings.

regularly performs third-party cybersecurity audits and would be willing to share with PURA at the annual meetings certification that such audits had been conducted. Both companies also expressed discomfort with having annual meetings with state officials.

Lightower emphasized the importance of flexibility in reporting requirements for smaller companies. It noted that what is required of a large company may not be necessary for one of Lightower's size. PURA noted that guidance provided by the WG4 Final report allows for flexibility for company size and operational needs.

Lightower has a network of more than 3500 miles of fiber in Connecticut serving healthcare and educational institutions, private businesses, cell phone sites, state agencies and other telecommunications agencies. Lightower offered constructive points in affirming its commitment "to attending an annual cybersecurity review meeting with PURA, if requested to do so, and otherwise participating in the proposed cybersecurity oversight program." Among its recommendations was that PURA designate the first year of its program as a trial period, focus reports on the six broad reporting areas listed on pages 20 and 21 of this report and hold one or more technical meetings after the first round of annual meetings to receive suggestions "for refining or improving the process." PURA welcomes these constructive contributions and will proceed to work with Lightower and any other companies sharing this perspective.

PURA noted the concerns about the possible burden of excessive reporting and reiterated its intent to avoid duplicative efforts. For example, what a company reported to the FCC at an annual cybersecurity review might also be used at a Connecticut review meeting. To the extent that PURA and other state officials might participate in federal-level meetings recommended by the WG4 Final Report, PURA might accept materials used at such meetings to satisfy some or all of its basic reporting requirements. At present the scope and details of possible federal reporting mechanisms have not been established, nor has the level of state involvement been fully addressed.

An area of growing interest and potential value in strengthening cybersecurity capabilities is the use of consultants, auditors and other partners. As the range and specialization of cyber threats grow, it will be increasingly difficult for one company to have all the expertise necessary to detect and manage threats and penetrations. Consultants can reinforce and complement in-house professionals, both through their awareness of utility-specific issues and through their own awareness of new threats and defenses. In future years, third-party partners could benefit both the utilities and public authorities, bolstering utility defense while concurrently reassuring government stakeholders and the public of the soundness of cyber defense and the application of appropriate remediation.

PURA noted that since many utilities currently obtain third-party audits, the results might be used to satisfy reporting requirements to help limit duplicative efforts. The telecommunications companies were reluctant to agree, citing information-sharing concerns. These concerns are outlined below; they include anxiety about misuse of information and the risk of exposure to fines, prosecution or litigation.

The telecommunications sector has communicated to PURA its concern that information proffered during meetings would result in comparisons between the individual companies, which could be later be held against them or used to point out potential strengths or weaknesses in another company's program. They also expressed fear of and resistance to state-level regulation. Additionally, company representatives questioned whether the government can mandate changes to a company's practices and what leverage the government might hold. PURA emphasized that the intent of the program was not to compare or rate companies, but rather to seek assurance for itself and government stakeholders that the public utility companies were effectively managing cyber risks.

The company and trade association representatives also expressed reservations about the potentially large number of government attendees at annual meeting. First, they are worried about divulging sensitive technical information to participants with limited cybersecurity background; that is attendees might misinterpret the information and/or inadvertently reveal highly sensitive information. Second, Frontier noted that the number of government participants acquiring company-specific and sensitive information will increase with time, due to the changeover of elected officials. Therefore, PURA has significantly curtailed participation to itself and the Division of Emergency Management and Homeland Security.

With the exception of Lightower the telecommunications companies, NECTA and the wireless companies through their trade associations, CTIA-The Wireless Association, notified PURA that they continue to be concerned with PURA's proposed cybersecurity oversight program. They questioned PURA's ability to ensure the confidentiality of sensitive or proprietary information under the state's Freedom of Information Act, noted that its proposed cyber framework does not provide the assurances of federal programs such as the Protected Critical Infrastructure (PCII) program and feared that the PURA program would not prevent possible disclosure of sensitive information that could jeopardize public safety and national security. Instead of PURA's oversight program, the telecommunications companies recommend that PURA work within a national framework instead of developing a single-state solution. They further notified PURA that they consider the proposed voluntary meetings and the information reported through them to be a mandate, a compulsory imposition that would compel the "broad disclosure of highly sensitive and confidential information."

PURA respectfully disagrees. Connecticut's Governor and members of the General Assembly have noted the need for state leadership to contribute to national efforts to strengthen cybersecurity. The majority of communications companies continues to urge PURA to delay its cyber oversight program and wait for initiatives being considered at the federal level, even though no such initiatives have been adopted and no future date has been offered for eventual adoption. While it might be convenient to wait for federal programs to align and stand up in harmony, experience has proved that such expectations are frequently not realized and years pass before even partial results ensue. In good faith, PURA sees the need to proceed with its modest program. We share the view that a PCII program to develop a mechanism for receipt of cybersecurity-related information and protect confidentiality would be a positive step. But to withhold cooperation until such a mechanism is created in effect means that it could be years before the communications companies cooperate with Connecticut and other states in meaningful cybersecurity defense.

PURA has presented its proposal as voluntary, not compulsory, and it has not ordered consideration of any cyber best practices. Similarly, PURA's strategic plan did not direct compulsory reporting standards or a cyber security checklist. What the plan proffered were annual meetings with the state’s public utility companies that would allow them to demonstrate to state government how they are defending themselves and their Connecticut customers against cyber attacks.

The communications companies perform a dual role in cybersecurity. Their networks are vital cybersecurity infrastructure that underlies other public utility companies’ information systems. Companies such as AT&T, Comcast, Frontier and Verizon have some of the nation’s most knowledgeable cybersecurity experts. Thus, the telecommunications field is a vital, integral part of the U.S. cyber picture, and effective national cyber defense is incomplete without their full participation. National security in the United States has always depended upon participation and support of the private sector in concert with government to identify and address challenges. Given that tradition and the need for effective corporate citizenship to counter cyber threats at the state level, the absence of telecommunications involvement is regrettable.

It is increasingly clear that the states need to be part of the U.S. cyber defense of our public utilities. While seeking to strengthen American cybersecurity defense with voluntary, flexible joint efforts responding to and accommodating concerns of the public utilities – an effort that could be replicated in other states – PURA applauds the positive attitudes demonstrated by electricity, gas and water and unfortunately must note that telecommunications has declined to join. We remain open to eventual cooperation. The public interest and the work of the other utility sectors would both be better served by telecommunications cooperation than by its current abstention.

In crafting a plan to execute its state strategy, PURA seeks to protect Connecticut’s utility companies and their customers. While a national approach would be attractive, none is imminent, and states concerned with cybersecurity cannot wait for one to emerge. PURA will work with the state’s public utility company sectors, and looks forward to working with those telecommunications companies willing to participate in the state’s Public Utility Company Cybersecurity Oversight Program.

The telecommunications companies that are unwilling to participate said that they want “to forge and strengthen an effective partnership with PURA on cybersecurity issues.” PURA welcomes such interest but finds this language rather hollow given their disinterest in participating in the Connecticut program.

In fact, if the telecommunication companies continue to resist joining the Connecticut program alongside their colleagues in the electricity, natural gas and water industries, PURA will be unable to state with any degree of confidence that Connecticut's telecommunications sector is providing an adequate defense against cyber disruption for their Connecticut customers and the other state public utility companies.

C. Cybersecurity Oversight Program

Based on the discussions and findings from the technical meetings, PURA will establish a Cybersecurity Oversight Program, which will be structured and implemented for each industry, as described below.

The foundation of PURA's Cybersecurity Oversight Program will be its annual cybersecurity review meetings. PURA anticipates holding the first set of meetings during the third quarter of 2016. Each participating company will meet with the PURA and Division of Emergency Management and Homeland Security representatives. These meetings will afford each company an opportunity to explain what it is doing to secure critical infrastructure while balancing the cost of security against the risks. The review meetings also will give attendees the opportunity to understand each utility company's security posture, cybersecurity practices and current challenges, in order to assess the effectiveness of the company's cybersecurity program. Utility companies should be prepared to set cyber defense within an overall risk management context and discuss the tools, intelligence and expertise it has to mount effective defense, its reasons for selecting certain measures and the courses of action it plans to take.

The annual review meetings are not intended to assign a grade or score to a utility company's cybersecurity program, or to compare one company to another. If the government participants see a gap in a company's cybersecurity program or have questions, they may request that the utility develop and subsequently report on corrective measures.

The annual review meetings will follow similar agendas to determine if the utility is taking necessary steps to defend against cyber attacks, detect and respond to attacks and restore capabilities or services affected by such events. The following topics are candidates for discussion at these meetings. These topics have been deemed by PURA and some of the utilities as appropriate for cybersecurity discussion.

a) **Management's commitment to cybersecurity**

Security requires the commitment of everyone in a company. The company should be prepared to discuss its management's focus on cybersecurity, including, but not limited to, security-related organizational roles and responsibilities, security budgets and explicit acknowledgements in corporate policies and publications of management’s commitment to cybersecurity.

b) **Company’s culture of cybersecurity**

A successful cybersecurity program requires a pervasive security culture in which all employees are aware of the importance of maintaining a secure workplace and supporting infrastructure, understanding their roles and responsibilities and practicing good security in all work activities. The company should be prepared to demonstrate that a cybersecurity culture permeates the organization, including security aspects of a corporate code of conduct, periodic security training for employees and other measures to promote security and privacy.

c) **Cybersecurity program status**

In addition to a technical discussion of a company’s cybersecurity program and practices, the company should provide an executive-level summary of the company’s security posture, addressing both strengths and weaknesses. The company should also describe new security solutions, planned or in place, new threats to the organization and its infrastructure, recent attacks detected and thwarted and resolution of any recent security breaches.

In support of threat and risk management, the company will be asked to maintain a cybersecurity risk register and to review it with PURA and the other government participants. PURA acknowledges utility company concerns regarding provision of detailed information about vulnerabilities, attacks and security-related solutions and will permit the flexibility of an overview. However, the company should be prepared to respond to PURA questions regarding such overviews.

The company will also note and track actions requested by meeting participants to enable review at subsequent annual meetings. Such action items will be reviewed and agreed upon following the end of each meeting. Action items will not be formal orders, but PURA will expect a follow-up discussion at the ensuing annual meeting.

d) **Engagement with external cyber expertise**

Information sharing is a critical dimension of cybersecurity. An organization’s security program can be improved through lessons learned by other organizations as well as by leveraging the cybersecurity expertise of other industries and government agencies. In the annual review, companies will be expected to demonstrate that they take advantage of external cybersecurity resources appropriate for their size and industry, including: participating in cyber-focused industry consortia; leveraging government cybersecurity resources, such as ICS-CERT and US-CERT toolkits and exercises; participating in cyber exercises; and engaging third-party assessors to conduct independent audits of security programs, controls and practices.

e) **Results of recent third-party security assessments**

Many organizations engage third-party security experts to conduct periodic reviews of their cybersecurity programs. The utility companies should be prepared, during the annual meeting, to provide the results of third-party security audits or assessments.

f) **Technical review of cybersecurity program and practices**

The companies will describe the status of cybersecurity programs, including specific reporting standards, security controls and industry best practices, such as NIST security controls guidance or ISO security standards.

The reporting standards described earlier in this report refer to the measures and controls on which a company builds its cybersecurity program and on which the effectiveness of the program can be assessed. PURA will not require any particular set of standards be used. To enable PURA and Connecticut's government participants to understand the state of a company's cybersecurity program and assess progress in improving infrastructure security, utility company reports will need to use an industry-accepted standard. PURA expects those standards to cover the 14 basic functional areas outlined below.

Examples of acceptable frameworks, as identified earlier, include the ES-C2M2, the AWWA Process Control System Security Guidance, FCC's CSRIC IV WG4 Priority Controls and the NIST Cybersecurity Framework 1.0. Work within these standards will not achieve absolute cybersecurity; relative cybersecurity also requires dynamic assessment of risks, benefits and a commitment to continual improvement. A utility company's defense, like that of any other enterprise, must adapt and evolve as threats and risks change.

As Connecticut proceeds with its cyber defense effort, PURA recognizes that regional, national and international companies are in more than one regulatory jurisdiction and must comply with security requirements of bodies such as the Federal Communications Commission, the Environmental Protection Agency, the Department of Energy and the North American Electric Reliability Corporation. PURA encourages utilities to seek as much uniformity as possible in working with their regulators and will do all it can to increase consistency and reduce the burden of reporting requirements.

Useful reports will describe management processes, controls and safeguards, successes and obstacles in a company's cybersecurity program. Working within a reporting standard, the following are basic functional components of a cybersecurity program:

1. Security Governance & Planning;
2. Risk Assessment & Management;
3. Asset and Asset Configuration Management;
4. Continuous Security Monitoring;
5. Disaster Recovery/Business Continuity Planning;
6. Incident Response;
7. Personnel Security;
8. Employee Security Awareness & Training;
9. Physical Security;
10. User Access Control;
11. Threat & Vulnerability Management;
12. IT/OT Network Security;
13. Service Infrastructure Security; and
14. Data Protection (At Rest and In Transit).

Protection measures and controls comprising a reporting standard should be measurable, enabling an observer to assess how effectively it is being managed, how well controls are performing, the maturity of the security program and progress being made. PURA understands that the maturity level of a specific reporting standard does not indicate a score but is instead useful for understanding the ongoing development of specific cybersecurity capabilities. PURA challenges the utilities to propose meaningful metrics appropriate for the size and scope of their operations in order to make clear both macro-level performance and assessment of key components.

Drawing on the technical sessions, PURA proposes the following initial guidelines for the annual cybersecurity review meetings, which include protection against disclosure of sensitive information:

1. Utilities will hold private, closed-door meetings with the designated PURA and Division of Emergency Management and Homeland Security representatives. No other companies will be present, and there will be no government participation other than PURA and DEMHS unless agreed in advance by the host utility.

2. Meetings will be at the utility's office or another mutually agreed place;

3. Meeting participants shall be bound by a non-disclosure agreement not to release or otherwise reveal information shared or divulged through the cybersecurity review;

4. PURA and the other government participants will not retain records, in hardcopy, electronic or other format. Neither PURA nor the government participants will take custody of confidential information;

5. Each utility will maintain a cybersecurity risk register, which will be reviewed during the annual meeting; and

6. Each utility will document and track actions requested by PURA and DEMHS to enable follow-up and review at subsequent meetings.

5. Summary of Findings and Next Steps

Voluntary annual meetings with public utility companies to discuss cybersecurity defense performance relative to agreed standards will be a significant step toward enhanced cybersecurity in Connecticut. These meetings will also improve communications and understanding between public utilities and public officials. PURA will seek to establish annual review procedures appropriate for each company's business needs, size and operating environment using standards and controls described in this report. Such meetings will be confidential, without written records and with safeguards in place to protect against public disclosure.

Due to the rapid pace of change in both cyber threats and defenses, and recognizing that the processes set forth in this report are starting points that will need to evolve, PURA expects revisions of and improvements to the Cybersecurity Oversight Program, over time. PURA will pursue additional opportunities to strengthen the security of Connecticut's critical public utility infrastructure and anticipates that Connecticut's public utilities will do the same.

PURA reserves for future consideration the potential, additional contribution of cybersecurity program review by objective, third-party assessors. The results of such audits could be discussed during annual review meetings.

PURA recognizes company concerns regarding the need to guard the confidentiality of the reviews this plan establishes. The federal Cybersecurity Act of 2015, enacted in December 2015, as well as Sections 1-210(b) (19) and (b) (20) of the Connecticut General Statutes, provide robust exemptions from disclosure of the kind of information to be included in the annual meetings with public utilities, thereby removing the need to ensure such protection through additional state legislation.[7] Additionally,

[7] Subsection (B) of Section 104(d)(4) provides: A cyber threat indicator or defensive measure shared by or with a state, tribal, or local government, including a component of a state, tribal, or local government that is a private entity, under this section shall be— (i) deemed voluntarily shared information; and (ii) exempt from disclosure under any provision of state, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

the procedures outlined in section C of this report ensure that the content of the technical review meetings will remain confidential.

Beyond the formal Cybersecurity Oversight Program, PURA may consider facilitating other programs that have the potential to strengthen the security of Connecticut's critical utility infrastructures. For example, PURA may work with state government agencies and the utility companies to plan and conduct statewide cyber exercises. Because company infrastructures are interdependent, PURA also may consider facilitating cross-utility and cross-sector cyber emergency planning and recovery. Focus on increasing security through greater decentralization of generation and distribution ties in directly with cybersecurity efforts; the two areas need to be approached in concert.

PURA has two overriding goals for the processes discussed in this report and the participation of public utilities and government authorities. Those goals are to strengthen cybersecurity in Connecticut's public utilities and to enable public officials to communicate with knowledge and assurance that reasonable steps are being taken to ensure cybersecurity in Connecticut.