STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

Cybersecurity and Connecticut's Public Utilities

Connecticut Public Utilities Regulatory Authority
10 Franklin Square
New Britain, Connecticut 06051

April 14, 2014

Arthur H. House, Chairman

www.ct.gov/pura

Cybersecurity and Connecticut's Public Utilities

I. Executive Summary

Cyber threats pose serious potential damage to Connecticut's public utilities. Connecticut's public officials and utilities need to confront these threats and detect, deter and be prepared to manage the effects of a cyber disruption.

Governor Dannel P. Malloy and Connecticut's General Assembly initiated this report through adoption of the state's Comprehensive Energy Strategy in 2013. They directed the Public Utilities Regulatory Authority (PURA) to review the state's electricity, natural gas and major water companies and to assess the adequacy of their capabilities to deter interruption of service and to present to the Governor and General Assembly recommended actions to strengthen deterrence.

This report is offered as a starting point toward defining regulatory guidance specifically for defensive cyber strategies. It documents PURA's findings and recommendations, including the following points:

- Connecticut's public utility cyber vulnerabilities and increasing capability to counter them are part of a larger, national effort to come to terms with cyber issues affecting virtually all activity involving use of computers and other micro-processors.

- Hostile probes and penetrations of utilities occur frequently. Defenses in Connecticut so far have been adequate, but security challenges are constantly evolving and becoming more sophisticated and nefarious.

- Utilities must accept the priority of effective cyber security. Most do, and they are addressing the need for material and human resources that form the core components of cyber defense.

- Most Connecticut utilities have established and update, maintain and practice cyber defense and management capabilities commensurate with high industry standards.

- The breadth and trans-geographic nature of cyber challenges require complex, multi-tiered governance and cooperation among public and private, national, regional and state-level resources.

- The National Institute of Standards and Technology has issued a "Framework for Improving Critical Infrastructure Cybersecurity" that recommends processes to improve cybersecurity and serves as a template for dialogue. It does not set standards or offer ways for state regulators to determine the adequacy of utilities' cybersecurity programs.

- Connecticut should consider the value of self (utility)-regulated cyber audits and reports, while it weighs any potential risks and enhancements, the costs and benefits of moving toward a required external, third-party audit system.

- Use of outside, third-party experts and utility participation in government and professional associations to inform and bolster cyber defenses need to be vital dimensions of Connecticut's cyber defense.

- Connecticut should be among the states leading the way in cybersecurity through innovative, collaborative, responsible defense and management.

Serious work is already underway within Connecticut's public utilities. Next steps to explore with them through discussions, technical meetings or other means include:

- Setting performance criteria;
- Seeking concurrence regarding the role of regulators;
- Establishing consistent regulation;
- Identifying reporting goals and standards;
- Sharing information and best practices;
- Maintaining confidentiality of sensitive cyber information;
- Rethinking procedures for ensuring personnel security;
- Defining appropriate cost thresholds and cost recovery guidelines;
- Identifying effective training and situational exercises; and
- Integrating public utility cyber issues into Connecticut's emergency management operations.

The evolving nature of cyber threats compels utilities and regulators to work together and coordinate actions. Cybersecurity is not an end state or single

accomplishment, but rather a process of continuous attention, vigilance and innovation. Connecticut can and should be a leader in the national effort to defend against a possible cyber disruption visited upon public utilities.

II. Introduction

In 2013, the Connecticut General Assembly ratified Connecticut's Comprehensive Energy Strategy. Among its provisions, the legislation directed the Public Utilities Regulatory Authority (PURA) to prepare an unclassified "cybersecurity review" for the Governor and General Assembly. The report would assess Connecticut's electric, natural gas and major water companies' capabilities to deter cyber-related service interruptions and present "recommended actions to strengthen deterrence." This report is PURA's cybersecurity review.

Although this report has benefited from access to classified information, its contents are unclassified and available for public dissemination without restriction. Connecticut's electric, natural gas, major water, municipal water, telephone and cable television companies have all cooperated in preparing this report. Their support almost unanimously reinforces the report's main conclusions concerning Connecticut's utilities: They face serious cyber threats and take them seriously; they are upgrading their information technology systems to strengthen their ability to deter, detect and defend against a cyber disruption; and in the future they need to collaborate with PURA and other Connecticut agencies, in ways consistent with federal processes, to agree on standards that will improve both cyber defenses and Connecticut's ability to manage a cyber attack.

III.The Challenge

Although a cyber threat to public utilities is most frequently associated with use of the Internet, cyber disruption could come from a multitude of sources both internal and external to a utility. The Internet and the other avenues of attack represent a modern form of warfare, and the threats are real. There have been a number of indications that cyber threats are of growing concern to the national security community. In August 2013, U.S. Rep. Mike Rogers (R-MI), Chair of the House Permanent Select Committee on Intelligence, called cyber espionage "the greatest national security threat," one that the United States is "not even close to being prepared to handle." Federal Bureau of Investigation (FBI) Director James Comey

testified before the Senate Homeland Security and Government Affairs Committee on November 14, 2013, that cyber attacks are likely to eclipse terrorism as a domestic danger over the next decade. A November 2013 ***Defense News*** poll of senior officials in the White House, Pentagon, Congress and the defense industry underwritten by United Technologies found that 45 percent of respondents believe a cyber attack is the greatest threat to the United States, about 20 percentage points above terrorism.

The Bipartisan Policy Center, a Washington group led by former Central Intelligence Director Michael V. Hayden, former Federal Energy Regulatory Commissioner Curt Hebert Jr. and former Massachusetts Department of Public Utilities Commissioner Susan Tierney completed in February 2014 an authoritative assessment entitled "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat." The Center's report on evidence collected from U.S. Government sources states that "cyber attacks on key energy infrastructure – and on the electricity system in particular – are increasing, both in frequency and sophistication."

The report further notes that the potential consequences of a cyber attack, or a combined cyber and physical attack are "difficult to overstate" and that prolonged power outages would "wreak havoc on millions of people's daily lives and could profoundly disrupt the delivery of essential services…" They cite expert concurrence that the risk of a successful is significant and that the operators of the North American electric grid "must be prepared to contain and minimize the consequences."

There is a profound distance in perspective between the consumer of electricity, natural gas and water, who sees consumption as a normal, secure part of life, and the U.S. Intelligence Community, which sees threats to such consumption. The latter witnesses sophisticated, daily probes and penetrations of U.S. institutions, including not only corporate information technology networks but also regional electric distribution networks and private utilities. In the August 16, 2013 ***New York Times***, reporter Matthew L. Wald noted that both government and private experts describe the U.S. electric grid as "the glass jaw of American industry." Such experts fear that a successful strike by an adversary "could black out vast areas of the continent for weeks; interrupt supplies of water, gasoline, diesel fuel and fresh food; shut down communications; and create disruptions of a scale that was only hinted at by Hurricane Sandy and the attacks of September 11."

Though the prospects of a cyber attack on public utilities may seem remote to those outside of intelligence, law enforcement and some public utilities, hostile probes and penetrations take place all the time. Efforts to hack into public utilities are significant, and by many reports, growing both in volume and sophistication. Public utility regulators and state authorities would be derelict to ignore what national security personnel call ongoing "battlefield preparation" – the penetration and exploration of U.S. management systems that control the flow of electricity, natural gas and water. The nature of cyber threats in other industries has also caused some public utilities to focus more intensely on their equipment and service vendors.

Cyber-caused denial-of-service attacks are frequent in some businesses, such as the banking industry. Some sources count approximately 400 serious cyber attacks on American banks during 2012 ("serious" being defined as capable of "bringing down" the ability of the bank to serve customers). Such threats exist in other businesses and industries as well, obviously including the public utilities. ***The stark fact is that the United States is vulnerable; probes are active, dangerous and widespread. This national pregnability pertains directly to Connecticut. There is no option but to acknowledge this reality and resolve to resist, defend and take countermeasures to ensure operational security in our public utilities.***

Federal experts advise, and some company officials acknowledge, that Connecticut's electric, natural gas and major water companies and the regional distribution management systems to which they are linked have been penetrated to varying extents. Defenses to date have prevented interruption, but the security challenges are constantly evolving and becoming more sophisticated and nefarious. Thus, the utilities' ability to deter, detect, thwart and manage penetration must constantly improve.

Along the spectrum of known risks in Connecticut, cyber disruption is relatively new and has increased in potential scope and damage during the past decade. In managing risk, Connecticut should excel at the familiar and predictable threats (e.g., hurricanes, ice storms, floods and heat waves) and be prepared for the less familiar but nonetheless possible (e.g., a major aircraft or train calamity, conventional bombing or hostage situation). Cyber risk falls into a hybrid category – we know it exists and we must prepare, but we do not fully understand its consequences, as with use of a weapon of mass destruction or the spread of an epidemic.

Public utilities' cyber vulnerability affects a large portion of Connecticut citizens. When risk assessors draw "concentric circles of vulnerability" in Connecticut they include our manufacturing tied to national security, such as the production of aircraft engines, helicopters and submarines, as well as our insurance, financial management, retail banking, and health industries. Cyber warriors and economic soldiers continually probe and attack all of these for industrial espionage or national security reasons, or both.

Public utilities historically (and understandably) have been more focused on safety than security. The security imperative is a relatively new challenge. Utilities are considered security-related targets because they provide services vital to life, health and the normal functioning of society. Disruption could be considered an act of war by hostile nation-state actors or terrorists.

On February 12, 2013 President Obama signed Executive Order13636 on Improving Cyber Security for Critical Infrastructure, along with an accompanying Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21). The Executive Order had broad implications for a number of industries, including the energy sector, and established a framework for potential changes regarding:

(i) Cyber threat information sharing;

(ii) Voluntary cyber security risk management consisting of standards, guidelines and best practices to promote the protection of critical infrastructure; and

(iii) Critical infrastructure identification.

The Presidential Executive Order has been viewed as an overture to stimulate Congressional action on broad-based cybersecurity legislation. PPD-21 draws upon existing authorities and directives and adds to them to give the Secretary of Homeland Security overall responsibility for critical infrastructure protection, and identifies the Department of Energy as the sector-specific agency responsible for the energy sector. The Department of Energy may draw upon the North American Electric Reliability Corporation's (NERC) expertise.

The Executive Order also called for the National Institute of Standards and Technology (NIST) to develop a "voluntary framework to improve cyber security in the nation's critical infrastructure." NIST held workshops with industries and

received public comments on this project to enable it to issue its framework, which it completed on February 12, 2014.

The NIST "Framework for Improving Critical Infrastructure Cybersecurity" noted that it was "Version 1.0." ***It is critical to note that the report did not establish federal cybersecurity standards.*** The report reiterated that Executive Order 13636 established the U.S. policy to "enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."

These quite general objectives were addressed in the framework as a process to develop "a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organization manage cybersecurity risks." The resulting framework is a process, not a set of standards or rules. The report explains that the framework uses "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." NIST and Department of Homeland Security officials describe the framework as a basis for having a discussion or a template to start a conversation. That characterization, as well as references in the report to the framework as a methodology and something that enables organizations "to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure," underscore that the report is a beginning. The report also calls the framework "a living document" that will continue to be updated and improved, and says that there will be future versions.

NERC's mandatory federal reliability standards for bulk power system do offer some cybersecurity protections. The Bipartisan Policy Center report affirms the incomplete nature of federal guidance regarding cybersecurity, stating that although "standards provide a useful baseline level of cybersecurity, they do not create incentives for the continual improvement and adaptation needed to respond effectively to rapidly evolving cyber threats…Our recommendations in this area aim to elevate cybersecurity at both the bulk power system and at the distribution system levels."

The NIST Cybersecurity Framework has three parts:

- **The Core**, which is "a set of cybersecurity activities, outcomes and informative references that are common across critical infrastructure sectors,

providing the detailed guidance for developing individual organizational 'Profiles;'"

- **The Profiles**, which will be used to help an organization "align its cybersecurity activities with its business requirements, risk tolerances and resources;" and

- **The Tiers**, which will "provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk." There are four self-ranked tiers, starting with organizations that do not have formal risk management practices and rising to organizations with cybersecurity practices "based on lessons learned and predictive indicators derived from previous and current cybersecurity activities."

Because the Cybersecurity Framework is a process and template for discussion, not a set of standards or a code of compliance, state regulators and public utilities cannot use it as guidance for what cyber defense programs should be or for how to achieve an acceptable state of security. Both state regulators and utilities want to avoid duplication and conflicting regulatory standards. The NIST report offers no solution. Federal guidance offers only NERC CIP reliability standards, not cybersecurity standards. Connecticut and other states may borrow from the NIST Cybersecurity Framework terminology and processes to discuss the subject and start a dialogue, but federal standards and determination of adequate performance currently do not exist. If states want to establish standards and seek compliance with them, they have to do that without the benefit of federal guidelines.

Tracking federal work in cybersecurity covers several agencies and requires recognition of several acronyms. At present, the most extensive centers of knowledge and contributors to cybersecurity and resilience are at the national level. The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas and oil. NERC develops and enforces reliability standards for the electric industry. Both have been leaders in the U.S. cyber defense effort. And regionally, the Northeast Power Coordinating Council (NPCC) promotes "development of regional reliability standards and [standards] compliance assessment and enforcement."

Some Connecticut utilities report productive support from the National Cybersecurity and Communications Integration Center, which is in the Office of

Cybersecurity and Communications of the Department of Homeland Security. This center provides resources to state and local governments and private companies to assist in awareness, detection and early warning of cyber intrusions, vulnerabilities, threats, mitigation and recovery actions.

In June 2007, FERC granted NERC the legal authority to enforce reliability standards among all users, owners and operators of bulk power systems in the United States. Connecticut's electric distribution companies currently deliver at peak load approximately 7,600 megawatts of electricity over almost 27,000 miles of distribution lines. Compliance with reliability standards is mandatory and enforceable in the United States. The same standards are generally enforceable in Canada under provincial authority.

To improve the North American power system's security, NERC developed the critical infrastructure protection (CIP) program, consisting of nine standards and 45 requirements covering security of electronic perimeters, protection of critical cyber assets including personnel, training, security management and disaster recovery planning. CIP requires organizations to deploy systems for monitoring security events and to have comprehensive contingency plans for cyber attacks, natural disasters and other unplanned events. Penalties for non-compliance can include fines, sanctions and other actions. Intelligence officials consider the NERC standards to be useful starting points, but not adequate protection against constantly evolving threats.

Given this extensive federal attention to cyber issues, what is the appropriate role of state authorities? Cyber, by its nature, is not a geographic matter, yet when emergencies strike, state and local authorities are responsible for the wellbeing of their citizens, and citizens naturally look to state and local entities for security, protection and relief. A cyber attack could potentially result in loss of electricity and heat, tainted fresh water supplies, disrupted financial and health systems, interrupted air and ground traffic and public chaos. A cyber attack could be launched in combination with a physical attack or a natural disaster, thereby both hampering recovery and adding a new, unexpected threat dimension.

States need to be part of a multi-tiered approach to cyber defense and management, ranging from international cooperation to national leadership and integrated state and local involvement. States need to recognize and use federal resources and competence wherever possible. Given that the states regulate public utilities, their goal should be to make only the necessary additions to federal processes and standards, tailoring any further regulations as precisely as possible to the specific

challenges facing the electric, natural gas, water and communications industries. That said, given the current absence of federal cybersecurity standards outside of NERC reliability standards for bulk power systems, Connecticut may want to identify areas to focus on and ways to address them as it moves forward to strengthen cybersecurity.

States have adopted a variety of approaches to public utility cyber threats. The California Public Utility Commission is on the aggressive side of cyber involvement. Its commission has professional staff with cybersecurity training, and California directly asks its utilities what steps are being taken to protect against infrastructure threats. Texas also has had cybersecurity experts on its utility regulation staff, but has a more limited budget and is less heavily involved in direct work with the utilities. Illinois does not mandate specific actions but does require its utilities to submit cybersecurity plans. The February 2014 Bipartisan Policy Center report noted that the state public utility commissions are not well set up for the new cyber challenges they face, especially with regard to determination as to whether related security costs are prudent. "Many regulators lack expertise" to make judgments regarding such expenditures, the report states.

There is far less, and sometimes no, state regulatory involvement in municipality-owned and cooperative utilities in the United States, some of which are overseen by the U.S. Department of Agriculture. In Connecticut, municipal electric utilities (MEUs) are regulated at the community level but operate without the oversight PURA exercises over Northeast Utilities and United Illuminating. Because they are part of the regional electric transmission grid, MEUs and the Connecticut Municipal Electric Energy Cooperative (CMEEC) must comply with federal cyber security requirements including those prescribed by FERC through Independent System Operator – New England (ISO-NE), and thereby must meet the same regional and federal cybersecurity requirements as Northeast Utilities and United Illuminating. PURA has no authority to require cybersecurity compliance of municipal utility companies, but the MEUs have informally indicated their willingness to cooperate in efforts to strengthen cyber defense. Their participation is vital, both because they provide electricity to Connecticut citizens and because they are on the grid. Municipal cyber programs should include:

- Identification of a person in charge of overall security and a person with authority for cybersecurity assurance (they may be the same person);

- Basic cybersecurity training for the cyber officer;

- Periodic penetration exercises and table-top reviews to assess "what if" situations and anticipated results; and

- An assessment of capability with gap analysis and recommended remediation.

Given the interdependence of electric grids, some have suggested that the nation would be better protected by more consistency at all levels and by FERC-issued guidelines for states. At this point the question is theoretical in two ways: Should FERC create such guidelines, and if so, should they be voluntary or legislated and mandatory?

It should be noted that electricity generators are also key to cybersecurity. While not addressed in this report, future work in the assurance of cybersecurity for Connecticut's utilities needs to account for the ability of electricity generators, both those located in Connecticut and those providing power to Connecticut local distribution companies, to ensure sound cyber defense. Without that, some cyber authorities worry that only a portion of the nation's total electric power infrastructure is subject to the NERC CIP.

The breadth of the cyber challenge understandably involves complex governance at all levels of government. As exercises and scenarios have demonstrated, an attack could be focused on a function (directed against an operations system) or a given region. The effects of offensive cyber activity could be geographically limited or pervasive. It is quite possible that a cyber attack in one state could wreak havoc in another, even a state some distance from the attack. An example is a wintertime attack on electric facilities in the southern United States that serve a national gas pipeline, resulting in disruptions of both home-heating natural gas flows and electricity generation in New England.

State emergency management authorities vary considerably in their size, resources and ability to help detect and manage cyber challenges. Connecticut's Division of Emergency Management and Homeland Security (DEMHS) has an active cyber detection and defense unit that collaborates with national and local agencies. The State of Connecticut participates in local "InfraGard" efforts. InfraGard is a voluntary public/private partnership between U.S. businesses and the Federal Bureau of Investigation that promotes information sharing on critical infrastructure. The collaboration specifically includes sharing information and intelligence on terrorism, criminal and other security matters.

Threats and their consequences do not discriminate based on state borders. No state can defend itself alone, yet each is obligated to protect its citizens as best it can. If every state had effective utility defenses, the collective result would be enhanced national security.

Connecticut should be among the states leading the way in cybersecurity through innovative, collaborative, responsible defense and management. Leadership in this arena requires managing the tension between seeking consistency with federally recommended processes and concurrently addressing gaps or inadequacies at the state level.

IV. Connecticut's Utilities and Regional Defense

American utilities are advancing their cyber defenses as cyber offense evolves. Few utilities would claim to be where they would like to be, and most acknowledge their need for more effective detection and deterrence and more emergency management support from and collaboration with state authorities.

Concern has moved from theoretical planning to realization that actual attacks are taking place. During the past year, local distribution companies in the United States have been attacked and penetrated both through cyber attacks and physical assaults. The alarmingly sophisticated and professionally executed attack on April 16, 2013, on the Metcalf Transmission Substation near San Jose, California owned by Pacific Gas and Electric Company, demonstrated that a small, well-trained group is capable of doing extensive damage to a large population. The potential loss of electricity service from a substation attack could last from hours to months: The estimated time to replace knocked-out equipment in a power substation (more likely to be accomplished by direct assault than cyber attack) is, in some cases, six to nine months or longer, with restoration potentially impeded by the fact that some components are not manufactured in the United States.

For several years, Connecticut's two major public utilities, Northeast Utilities and United Illuminating Company, and their respective electric and gas distribution companies have taken cyber challenges seriously. They have established comprehensive NERC CIP compliance programs to protect infrastructure and have developed capabilities to deter interruption of service. The CEOs of both utilities have taken personal interest in cyber threats within the context of overall risk management. Both CEOs are well aware of cyber matters, readily discuss the state

of threat and management and have assigned senior officers to direct cyber work. In doing so, the CEOs have explicit, engaged support from their boards of directors.

Their common approach to cyber vulnerability inspection is to monitor routinely, conduct management status assessments and deliver at least semi-annual reports to their boards of directors. Each company also has an employee awareness communications program, including tests and planned "phishing" programs aimed at reminding employees of the need for strong cybersecurity habits and practices.

When it comes to discussing cyber threats with or soliciting support from utility outsiders, the attitude of public utilities has changed radically and positively. In the past, utility discussion of cyber matters was in some instances characterized by defiance and resistance. The standard line was frequently that all is well: The company has a solid defense; operations are completely separated from the Internet, and hence there is no opening for compromise; the company has the best experts available; and the outside world should rest assured that the company is cyber-safe. In some cases, challenges and inquiries were seen as impertinent. Such attitudes regarding cyber security have all but vanished within the two major Connecticut utilities.

Both major utilities have retained recognized consulting companies in the cyber field, thereby supplementing their own staff capabilities and exploring potential weaknesses in their programs. Each monitors and manages a range of current and emerging risks and threats, including those arising from equipment and system integrity. Both utilities also recognize that federal government agencies have experts skilled in threat profiles and specific penetration efforts. Both report close cooperation and collaboration with federal authorities and trade associations.

Given the heightened profile of cyber threats, Connecticut's utilities have also reevaluated how to structure management of cyber matters and where to house such management. Northeast Utilities debated whether to place cyber oversight in its information technology (IT) area or in operations, but as one official stated, cyber clouds the bright line between those functions. The result was to place it in emergency preparedness, with both IT and operations coordinated through its work. Through its location in emergency management, cyber is addressed along with other forms of risk, such as physical security. United Illuminating, similarly, considers cyber to be a top priority. It tracks cyber security within its risk management framework and manages cyber security within its IT organization for both operational and corporate networks.

Because the NERC-CIP standards provide a good foundation, it is encouraging that both utilities have taken extensive measures to comply with, and in certain cases exceed, them and that many of these practices are also used for the distribution systems. These programs include reporting to PURA, local agencies and federal authorities, including NERC, about cyber security events, such as suspected and actual attacks at critical facilities, vandalism targeting security systems, and suspected or actual cyber or communications attacks that could affect the adequacy or integrity of the New England bulk electric system.

As part of ongoing training, both Northeast Utilities and United Illuminating participated in GridEx II, a NERC-directed exercise designed to test the readiness of the electric sector to respond to a cyber and/or physical incident, strengthen utilities' crisis response capabilities and review areas of internal security program improvement. GridEx II took place on November 13 and 14, 2013, with more than 200 organizations nationwide. It simulated attacks reaching utilities' centralized operations management systems, referred to as supervisory control and data acquisition (SCADA) systems, and it tested crisis response and information sharing between cybersecurity and physical security components.

Both Northeast Utilities and United Illuminating assess their sophistication and their detection and defense systems based on the realization that probes and potential compromises are a matter of daily management, that some of those who probe the systems have extraordinary, world-class skill and power, and that an attitude of humility and constant vigilance are both wise and necessary.

Managing public utilities' cybersecurity in New England, as throughout the United States, involves regional and national systems. The ISO-NE is charged with overseeing the grid system reliability of the six New England states, and it takes cyber matters seriously. ISO-NE's cyber integrity work is critical to Connecticut because compromise anywhere in New England or even the eastern United States and Canada could result in outages in Connecticut.

ISO-NE has an extensive, sophisticated cybersecurity program with skilled professionals and advanced cyber defense systems. Outside experts have assessed its cybersecurity program to be well-guided in its policy focus, architecturally strong and technically at the top level. The interdependence of the cyber challenge, discussed elsewhere in this report, is especially evident in ISO-NE's load management work.

A recent FERC audit of ISO-NE's cyber work underscored the strength of its cyber team. While its operations management exhibits some of the defensive posture attributes the utilities formerly displayed, ISO-NE's top management and board of directors recognize the existence of vulnerabilities and the need to stay ahead of the threat and improve the response processes required for today's cyber defense.

With many players involved in the effort to increase regional cyber defense capabilities, obviously some entities are stronger than others. Some experts note that ISO-NE understandably has a more sophisticated cyber defense capability than those of the individual utilities whose work it coordinates in load management. ISO-NE is constantly being probed, as are all of New England's utilities, many of which have been compromised or penetrated in the past. ISO-NE's strength, therefore, depends on both its own cyber defense capabilities and those of each of the utilities with which it works. Weaker utilities in and contiguous to New England need to be monitored, as failure in one of them could affect the resilience of the regional system.

How do utilities "wrap their arms around" a challenge as diverse and complex as cybersecurity? A first step is to accept that cybersecurity is a priority, understand that every utility is vulnerable and recognize that every part of the company – from the chairman of the board of directors to the security officer in the parking lot and the cleaning crew – has a role in cyber safety. A second step is to establish a flexible, replicable framework to break cyber threats into core components. One such framework, implemented in Connecticut, is built on five action items:

- Know;
- Prevent;
- Detect;
- Contain and respond; and
- Recover

Each action item follows best practices, is broken into subcategories and designates specific responsibilities for each level of management.

A third step is to use outside, or third-party, experts and to participate in government and professional associations to inform and bolster cyber defenses. Both major Connecticut utilities actively benefit from such associations. As noted above, they employ consultants with trained cyber experts, who advise on current threats and defense systems and organize mock "attacks" to challenge company

detection and defense capabilities and search for weak points to exploit. External associations include the U.S. Government; professional organizations, such as the Edison Electric Institute and American Gas Association; regional groups, such as the Hartford Area Security Managers Association; and local and national cybersecurity associations, such as the Information Systems and Security Association and the Information Security Audit and Control Association.

One of the key challenges for any company managing cyber threats is to establish and manage a working barrier between its corporate communications systems, including the Internet, and its SCADA systems. This subject is controversial and sensitive in cyber management. The goal is to be able to distinguish between internal and external communications systems and between communications and operations systems. The distance meant to be established between communications and SCADA is sometimes referred to as an "air gap." A few utility officials and notably New England regional network officials insist that the integrity of the two communications systems (corporate communications and operational communications) has been sustained, and that defense against penetration is effective, but that view is rapidly losing credibility.

Some federal intelligence officials directly assert that, even when "air gaps" exist between communications and operations, ways to compromise such separation are extensive and are probed and penetrated by foreign national operatives. Moreover, there are ways to penetrate operations and corporate networks unrelated to air gap defenses. Officials observe that foreign agents can move from one system to another, compromising the intended defense.

Although most of the public utilities' cyber attention has been directed to electricity generators and distributors and secondarily to natural gas companies, all the lessons learned and preventative measures discussed also apply to water companies. A few years ago, both physical security and cybersecurity in the water industry were, understandably, not priority matters. Today, unfortunately, they must be.

It is imperative that we include a cyber attack or other security attack on a water company in a review of public utility security. The motivation for endangering a public water supply and the consequences of doing so cannot be ignored in today's world.

Cyber threats to water are not as prevalent or as sophisticated as those to gas and electricity, and water systems are generally not as interconnected as electricity and

gas systems. But cyber threats to water utilities do exist, and Connecticut water companies have moved aggressively in the past few years to address them. As with gas and electricity, the question is: How much defense is enough? The companies have raised cultural awareness and security attention among their employees and have invested in software and other defensive programs. One of Connecticut's water companies brought in its first cyber consultants in 2008, establishing a cyber defense program and initiating enhanced security awareness. It also conducts threat exercises and assesses all new technology for security implications.

The National Association of Water Companies has a cyber program to which Connecticut companies belong, and they concurrently use private vendors to bolster their defenses.

When it comes to personnel security, discussions with the electric, natural gas and major water companies revealed universal issues:

1. Personnel security requires a delicate balance between prudence and overkill. When does a security check lead to inappropriate personal invasion and unnecessary expense?

2. The traditional reliance on and comfort from having employees with clean police records is inadequate. Terrorists, hackers and spies rarely have damaging, discoverable police records.

3. Compromise could come from employees with ideological or other personal identifications that motivate disruptive behavior.

4. It is virtually impossible to do thorough security checks on and issue clearances for all personnel with potential contact to operations, including maintenance, food services and other vendors.

Both the public utilities and the state public utility commissions that regulate them have few people with security clearances, making it difficult to deal with and share classified information regarding cybersecurity. The Bipartisan Policy Center report noted this problem and recommended that the security clearance process for selected utility personnel, as required by Executive Order 13636, continue while concurrently, "intelligence agencies should declassify relevant threat and vulnerability information when possible and use other methods, such as tear lines,

to separate classified and unclassified information in order to facilitate the sharing, for official use only, of otherwise classified reports with power sector partners."

At the same time, the United States Intelligence Community, and in particular the Department of Homeland Security and Department of Energy ought to explore ways to share intelligence regarding cybersecurity. On this point, the Bipartisan Policy Center report recommends that the Intelligence Community "conduct regular outreach to state utility commissions, other relevant state agencies and public and municipal utilities on cyber threats and vulnerabilities" to help protect critical infrastructure.

V. Communications

The legislation calling for this report did not specifically include evaluation of the communications industry, and PURA has limited oversight powers in the communications field. However, PURA continues to regulate landline telephony, cable television service and wireless communications with regard to public safety. Since communications networks are vital components of cybersecurity and are used in the operation of public utility information system infrastructure, disruption of utilities' ability to use communications services would have damaging, if not catastrophic, effects. In addition, the communications industry has some of the nation's top cyber experts. The communications industry must continue to be a partner in Connecticut's cyber defense.

Discussions with the communications industry underscore some key points. First, companies assume that there are ongoing probes requiring constant defense. Thus, their risk management approaches take into account what actions can be taken to identify, deter and remedy cyber threats at acceptable cost, what is a tolerable cyber risk and what is an unacceptable one.

Second, the communications companies can see cyber threats and attacks taking place on their networks. They monitor their networks 24 hours per day and have established baselines of normal activity. They look for anomalies, such as an increase in a specific type of traffic, traffic destined for a certain website or the use of a specific port. Such activity may indicate a potential (or ongoing) cyber attack. Such monitoring can enable communications companies to be among the first to detect the evolution of "malware" and "botnets." Malware is malicious software. A botnet is a group of Internet-accessible computers that are controlled from a

single source and run related software programs and scripts. While botnets can be used for distributed computing purposes such as scientific processing, the term usually refers to multiple computers that have been infected with malware to carry out tasks assigned by the controller. Normal practice for communications companies is to seek the root cause of an anomaly, then take measures to work with the company, organization or individual customer to block the malicious traffic and reroute it.

Third, communications companies may be in a position to identify and follow the flow of sustained efforts to exfiltrate information from a customer or to usurp operational command and control, in many cases facilitated by a nation-state. A sustained effort of this sort when supported by significant resources and advanced skills is called an "advanced persistent threat" (APT), and may involve the use of social engineering, such as spear phishing, to place malware on an end user's device and exfiltrate sensitive, proprietary information or intellectual property. These types of attacks are among the activities drawing most concern from federal officials dealing with cyber matters. During the past year, some non-governmental, private organizations have been the targets of APTs, placing at risk their ability to communicate.

Communications companies have long partnered with government in response to cyber threats. Their work has included participation in the National Security Telecommunications Advisory Council (NSTAC), which was started in 1982 to advise the President regarding security policy matters, and the Communications Sector Coordinating Council, established in 2005 to lead planning efforts of private companies partnering with the U.S. Department of Homeland Security. More recently, communications companies have supported the Communications Information Sharing and Analysis Center (C-ISAC), which works with government agencies to establish a real-time, 24-hour operational response capability to manage cyber threats.

Communications companies' marketplace success is linked to their customers' use and consumption of network-based products and services in a safe, secure network environment. Consequently, communications companies need to stay abreast of and adapt their particular network architectures and business models to the leading-edge cybersecurity protocols and practices. PURA's efforts to keep up to date with cyber defense measures require working with representatives of the communications industry.

Given its central presence in cyber matters, the communications industry has the potential to contribute significantly to cybersecurity, and several companies appear willing to do so. Communications companies emphasize the need to remain flexible and able to innovate continuously, and some of them express concern about the prospect of prescriptive standards and regulation in the cyber field. That said, they generally welcome partnership with state and local governments.

The communications industry can participate in strengthening Connecticut's cyber security by:

1. Working closely with PURA and Connecticut's Department of Emergency Management and Homeland Security in crisis management;

2. Participating in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and ensuring that it addresses Connecticut's needs. MS-ISAC, which is a focal point for cyber threat detection and prevention for U.S. state, local, territorial and tribal governments, monitors early cyber threat warnings and advisories and identifies vulnerabilities; and

3. Supporting efforts to educate the public about cybersecurity, the need to practice computer safety, and what to do in case of a cyber attack.

VI. Moving Forward

The advent of cyber threats to public utilities is profound and raises issues at the heart of the relationship between regulators and public utilities. The basic contract in the United States allowing monopoly, privately-owned utilities to provide essential services to the public has focused on price, reliability, resilience and other matters related to service, all under regulatory oversight of public utility commissions making decisions on each according to the "just and reasonable" standard. When there have been threats to reliability and resilience, such as Connecticut's hurricanes and ice storms, a core responsibility of PURA has been to assess utility performance and take steps to ensure reasonably secure service in the future. When utilities seek rate increases, they account for maintenance and infrastructure investment to ensure their ability to continue serving the public. The possibility of cyber attack and the need to defend against it combine the issues of reliability and resilience with the appropriateness of cost for cyber defense. Cyber presents a new challenge for state regulators: What kinds of investments and what

kinds of technology, training and employee preparation are fair and reasonable costs?

Cyber is now part of the social contract between public utilities and state public utilities commissions.

The seriousness of cyber challenges and the breadth of their potential effects also underscore the common ground shared by Connecticut's utilities, regulators, and emergency management team. It takes all parties to prevent or manage the effects of an attack. Moving forward, the classic regulatory positioning of challenge and oversight from the regulators and defense and justification from the utilities must, at least initially, be set aside or held in abeyance until there is concurrence regarding appropriate cyber defense. Our shared obligation is to find ways to provide reliable utility services and concurrently protect utility customers, the people of Connecticut. That work should lead to agreed rules of the road, but the first steps are understanding and concurring on design of the common effort.

A starting point is to recognize where the expertise resides regarding the international challenge of cybersecurity. The federal government has outstanding cyber specialists in several areas, including intelligence, national security, homeland security, finance, communications and energy management. State government has officers who understand the scope of the challenge and the policy needs they present, but who, understandably, have less experience and scope than their federal colleagues. Beyond government capabilities, a great deal of technical expertise – understanding at the design level exactly what cyber issues are, how they are managed, how offense and defense work, and how communications systems create and sustain evolving security – lies in the private sector.

Government needs to listen to and work with the companies whose professionals work in this space. Private sector expertise in cybersecurity is a national asset. In his November 14, 2013, Senate testimony, FBI Director James Comey noted that private industry is "the key player in cybersecurity." He further stated, "Private sector companies are the primary victims of cyber intrusions, and they also possess the information, the expertise and the knowledge to address cyber intrusions…We intend to build more bridges to the private sector in the cybersecurity realm." State governments have the same obligation.

Public/private partnerships are the core foundation for cyber defense. The White House Cyberspace Policy Review of June 2009 addressed the need for close collaboration with the private sector and collaboration among all levels of

government. These two citations from the Policy Review underscore the administration's priorities:

> ***The United States cannot succeed in security cyberspace if it works in isolation.*** The federal government should enhance its partnerships with the private sector. The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure… The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike.
>
> The United States needs a comprehensive framework to ensure a coordinated response by the federal, state, local and tribal governments, the private sector, and international allies to significant incidents… The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

The United States is at the starting point of formulating a comprehensive cybersecurity strategy, and that strategy will depend heavily upon active contributions from and participation by the private sector and state, local and tribal governments. In addition to strategy, the important work of managing operational activities and ensuring the integrity of specific operations is a local obligation. Connecticut should not and cannot wait for a complete federal framework into which its own cyber defense strategy and local operational security can be integrated, especially now that the federal posture is one of communication and experience sharing, rather than establishment of standards. Rather, we and the other states should move forward to recognize threats, consider the adequacy of our defenses and practice emergency exercises, while staying apprised of what the federal government and other states are doing. This is a learn-as-you-go challenge, not one of waiting for the big picture to clarify, before becoming a constructive player.

If the starting points are learning, recognizing the key role of the private sector and collaborating, what should Connecticut's regulators know about the defense capabilities of public utilities?

Oversight currently incorporates review of the financial soundness and profitability of regulated utilities and their resiliency – the ability to prepare for and provide

essential services during a storm or other foreseeable disruption. Given the potential damage of cyber disruption, the Governor and General Assembly are certainly within the bounds of normal regulatory inquiry in asking that PURA oversee the cyber competence of the regulated utilities. This issue compels partnership and regulatory oversight.

The need to understand, evaluate and agree upon the cybersecurity capabilities appropriate for electric, gas and major water companies; their notification and reporting requirements; and what PURA should do to assure the Governor, General Assembly and public that it has taken reasonable steps to ensure public safety are all new territory.

To develop a basic foundation of information and judgments, we must make multiple determinations:

- Do the leaders in the public utilities serving Connecticut and their boards pay appropriate attention to risk management in general and cyber as part of that challenge?

- Do they have skilled personnel and necessary hardware and software? Are their budgets for cybersecurity adequate?

- Do they train and keep up with the constantly evolving set of threats?

- Do they run mock drills with outside assistance to test the strength of their deterrence?

- Do they have access to outside consultants and experts to stay up to date and to fill in gaps not covered by their own personnel?

- Are they active participants in trade association activities geared toward sharing best practices?

The answers to such questions (and there are others) are matters of legitimate regulatory and public concern. But what are the criteria of appropriateness and adequacy, and who should assess performance against such criteria? Self-regulation by the utilities could be a starting point, but cannot be the ultimate solution. The subject is too important to rely solely on self-reporting.

One potential solution would be to borrow from the world of finance and accounting. Just as accounting firms review the finances of companies and report their findings according to uniform standards, such as generally accepted accounting principles, so too could there develop a utility cyber analyst industry that audits public utilities and reports on their performance, measured against agreed criteria. If states decide to develop regulations, their standards should seek as much uniformity and consistency as possible to avoid the problem of having differing and potentially conflicting state-created standards applied to multi-state utilities.

Use of third-party cyber audits and assessments could potentially resolve some serious and legitimate concerns. Some state-regulated utilities are understandably reluctant to open their cyber doors to state regulators, thereby sharing sensitive, secret and extremely important information. One could anticipate greater comfort in sharing that information with firms they hire, using the same sorts of confidentiality protocols that pertain to the retention of financial analysts. In fact, some Connecticut utility officers have indicated their strong support for moving away from self-regulation toward a system of mandatory third-party verification, especially because they believe the amounts of money and personnel needed to ensure comprehensive security could be "insurmountable and unfeasible." They further state that, given the stakes, the risks should be shared with credentialed audit firms. Others resist migration away from self-regulation, citing the proprietary nature of cyber defense information and desire to keep such information and capabilities private. Use of external auditing processes would need to be preceded by concurrence on evaluation standards.

Use of cyber auditing firms would address two challenges facing state public utility regulators: personnel and storage. No U.S. state regulator has cyber expertise on its staff capable of performing a thorough cyber audit. It would be prohibitive in terms of cost, time and training to acquire such competence – and not necessarily a wise investment for this focused purpose. Furthermore, what would state regulators do with the sensitive, secret and important cyber management information derived from an audit? State regulators do not work within secure compartmented information facilities (SCIF). However, there are consulting firms with cyber experts who have or have had advanced security clearances, and who have the capabilities to store sensitive information as part of carefully managed, confidential relationships.

If third-party experts were to conduct cyber audits, what public officials should be made aware of the results? It would not be appropriate to make such assessments

public because descriptions of weaknesses could then be exploited. But the public should have a reasonable expectation that such findings were reported and understood by public officials, acted upon constructively and that, if needed, remedial actions were taken. The list of those apprised should be short but include the officials most directly involved in oversight. A starter list might include the Governor or his or her designee, the public utility regulatory commissioners, the head of emergency management and the chairs and ranking members of the appropriate legislative committee.

Connecticut should consider starting with self-regulated cyber audits and reports and moving toward a third-party audit and assessment system.

The communications companies pose a different set of challenges. The scope of state regulation is far smaller than for electric, gas and water companies. Several communications companies operate on a global scale, observe international and national standards and operate in multiple states. Despite the vital nature of their service to Connecticut customers and the need for assurance of cybersecurity, it is difficult to conceive of a state-directed audit system that would constructively enhance their cyber defense, without duplicating or contradicting the standards they currently seek to meet.

There are no "quick fix" solutions. The complex responsibility of ensuring security for public utilities is assigned to PURA, but all of our political and community leaders and the utilities themselves own the obligation to provide strong cyber defense. This is not a challenge to be resolved by appointing a state "cyber czar." This serious work has just begun and will evolve in the years to come. Connecticut should approach cybersecurity for its public utilities in terms of phased work: efforts that are continually examined and improved upon. As we learn, we must adjust. As we understand, we must update, improve and build better defenses.

To start, there are a number of basic questions that should be explored with Connecticut's utilities to determine where concurrence exists and where further discussion, through technical meetings or other venues, is necessary. Here are a few:

1. **Performance Criteria.** Given the need to detect, prevent and manage cyber threats, what performance criteria should be established, and what information should be made available to regulators? To what standards should utilities be held, and who should concur in their creation?

2. **Role of Regulators.** What role should be expected of public utilities regulators? Should they develop basic competence to oversee the cyber defense capabilities of Connecticut's utilities? Given that most regulation requires reviews of prior performance, and given that cybersecurity is dynamic and subject to technological evolution and innovation, how can public utility oversight include necessary performance assessments and consistently support efforts to prepare for future challenges?

3. **Consistency of State Regulation.** Most current attention to cyber defense is at the federal level. Given that public utility regulation is in the hands of state regulators and that the challenge of cyber threats is regional and national, what roles can the states play to be effective, consistent and reliable contributors to cybersecurity? How can state regulation strengthen cyber defense and also avoid duplicating or complicating other efforts to set standards and strengthen defense?

4. **Reporting on Cyber Threats.** What level of incidence reporting to public regulators distinguishes between necessary security and cumbersome overkill? What type of intrusion should be considered a "routine probe," and what should be flagged as a potential "tip of the spear" of a harmful cyber event and therefore reported to regulators? Should reports to regulators be "for information only," leaving the details for agencies such as the FBI or Department of Homeland Security, or should regulators receive full reports?

5. **Information Sharing: Proprietary Practices and Best Practices.** To what extent should regulators endorse and support information sharing and best practices for cybersecurity among regulated utilities? In other words, should individual firms use proprietary and confidential processes and methods to manage cybersecurity, or collaborate on and share best practices?

6. **Confidentiality.** There are limits to sharing sensitive, secret technical information with state regulators. Given the complex nature of cyber defense, and because state regulators normally do not have secure facilities to store reports and other information, what ground rules should be set regarding which state officials receive confidential or sensitive cyber information, and what steps should be taken to protect it?

7. **Personnel Security.** We must rethink screening procedures for personnel working on cyber matters. As noted above, reliance on clean police records is inadequate. Terrorists, spies, hackers as well as company insiders and vendors with malign intensions do not necessarily have criminal records. The Intelligence Community can help by streamlining the security clearance process for both utility and regulatory personnel. What is a reasonable, prudent level of investigation and vetting of personnel? How do issues of personal privacy and expense factor into security determinations?

8. **Reporting Standards.** Should specific reporting standards be crafted for each utility: electric, gas and major water companies? Should incident reporting be disclosed only if security measures have been put in place to ensure confidentiality?

9. **Municipal Utility Oversight.** What should the cybersecurity oversight system be for municipal utilities? Should regulatory authority be expanded beyond the current cooperative relationship to include legislated oversight powers?

10. **Cost/Benefit Considerations.** How should costs be factored into cyber risk management? At what point should a risk be deemed tolerable because additional steps to counter it would be too expensive? How would such costs be recovered?

11. **Training and Exercise.** Training should be recognized as a special, ongoing, required expense. Since cyber defense is, in essence, an effort to keep one's knowledge, software and ability to deter more advanced than that of the adversary, education is key. How should regulators encourage and evaluate as core expenses the costs of training, mock drills and assessment programs?

12. **Emergency Management.** What information and cooperation should the utilities provide to emergency management officials? How should public utility cyber risk management be integrated into the state's other emergency management preparedness plans? If there are actual incidents, what state capabilities should be in place to help respond to and manage them? More broadly, to what extent should utilities' and regulators' cybersecurity efforts intersect with other companies' and agencies' concerns regarding infrastructure protection? How should communities prepare to respond to

the broad array of public and social dysfunction that a cyber attack could bring?

Conclusions

Cyber threats increase in seriousness and potential impact as fast as the private sector and federal, state and local governments prepare for and manage them. The process of keeping up, understanding innovations and thwarting new dangers never stops. Defense is a process and part of a risk management culture, not an installed system or capability.

Connecticut has in place a process whereby its head of public utility regulation receives intelligence briefings on cybersecurity matters. The U.S. Intelligence Community should be encouraged to enhance its outreach efforts to keep state utility commissions and public utility officials apprised of cybersecurity threats and vulnerabilities. It is possible that the Connecticut model could be further developed and be of benefit to other states.

Individual public utilities have recognized the danger of cyber threats and taken serious steps to defend against them. The far-reaching scope of potential damage that could be wreaked by a cyber attack, the disregard for geographic and corporate boundaries and the still unknown ramifications of cyber mischief are vast. Federal and state agencies, national security and domestic emergency management agencies overlap, and the sheer unpredictability of effects make preparation for a cyber attack a challenge virtually without boundaries. Americans know how to react to crises they have experienced: hurricanes, ice storms, fires and floods. We do not know all the adversities they may face from a cyber attack, nor how they would react to being without communications, electricity or water for a prolonged period of time. In Connecticut we have seen such effects and know that it does not take long before life and health are threatened and public order and safety require emergency intervention and management.

We have to prepare for an attack by starting our defense system with the most logical steps. This report outlines some steps that should be evaluated, discussed and possibly introduced into the regulation of public utilities. We must also integrate the possibility of a cyber attack into the more familiar array of threats facing Connecticut.

State-level strategies and emergency exercises must be part of the solution. A good place to start would be to design a credible scenario applicable to New England: a cyber attack involving both the electric and gas industries during the winter, thereby knocking out both electricity generation and home heating. We should consider systemic defense against such an attack; the roles utilities and federal, state and local governments would take in managing such an attack; and the more general emergency management implications of its effects.

Connecticut utilities share the obligation to defend against cyber attack, just as all other sectors of society do, including health management, industry, banking and transportation. Their performance and our regulatory obligation need to address the new realities, leading to processes and standards that strengthen our defenses against and improve our ability to recover from an attack. Such work is now a necessary dimension of basic public security, operationally compelling and feasible to manage. It should be approached not with a massive stroke of definitive action, but rather in incremental stages with lessons learned and ongoing adjustments. Cybersecurity is not an end state or an accomplishment, but rather a process and culture of continuous attention, vigilance and innovation.

Unfortunately, the genuine potential for such an event compels us to confront the difficult issues posed in this summary report. With guidance from Connecticut's Governor and General Assembly, PURA is prepared to address its share of the challenges we face.

Connecticut can and should be a leader in the national effort to defend against a possible cyber disruption directed against public utilities.

Acronyms Used in This Report

APT Advanced Persistent Threat

CIP (NIST's) Critical Infrastructure Program

C-ISAC Communications Information Sharing and Analysis Center

CMEEC Connecticut Municipal Electric Energy Cooperative

DEMHS (Connecticut's) Division of Emergency Management and Homeland Security

FERC Federal Energy Regulatory Commission

ISO-NE Independent System Operator-New England

MEU Municipal Electric Utility

MS-ISAC Multi-State Information Sharing and Analysis Center

NERC North American Electric Reliability Corporation

NIST National Institute of Standards and Technology

NPCC Northeast Power Coordinating Council

NSTAC National Security Telecommunications Advisory Council

PPD-21 Presidential Policy Directive on Critical Infrastructure Security and Resilience

PURA Public Utilities Regulatory Authority

SCADA Supervisory Control and Data Acquisition

SCIF Secure Compartmented Information Facility