

**BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF DELAWARE**

**IN THE MATTER OF THE COMMISSIONS')
REVIEW OF THE NECESSITY FOR)
CYBERSECURITY GUIDELINES OR) PSC DOCKET NO. 16-0659
REGULATIONS FOR DELAWARE)
INVESTOR OWNED ELECTRIC, GAS)
AND WATER UTILITIES)**

**PETITION OF THE DELAWARE COMMISSION STAFF SEEKING REVIEW
AND DETERMINATION OF THE NEED FOR CYBERSECURITY
GUIDELINES OR REGULATIONS TO MAINTAIN RELIABLE UTILITY
SERVICES IN DELAWARE**

The potential for a cybersecurity breach of utility customer information system and/or service control systems continues to expand exponentially with the advent of many new technologies and the vulnerability of older technologies. Given the obligation of the Commission to ensure quality customer service to all regulated utility customers, it is essential that Delaware utilities be prepared to manage today's cybersecurity risks. Several nearby States are having discussions or are in process of issuing high level guidelines or regulation to ensure utilities are properly prepared to handle system security breaches. The Delaware Commission Staff ("Staff" or "Petitioner") respectfully submits this petition ("Petition") requesting the Public Service Commission (the "Commission") to authorized a review of cybersecurity issues for the purpose of determining the need for guidelines or regulations to ensure the continuation of quality regulated utility services for the utility customers. And if such need is determined, the authorization to draft and submit the appropriate documents for the Commission's consideration.

BACKGROUND

1. The statutory authority of the Commission provides for the supervision and regulation of investor owned utilities in the State of Delaware. 26 *Del. C.* §201¹ provides the general regulatory authority and 26 *Del. C.* §209² requires the Commission to ensure that every public utility provides safe, adequate and proper service. In today's new technological environment, utility services are exposed to additional risks through individual's or organizations' abilities to inappropriately access utility electronic customer information systems and/or service systems. Those with malicious intentions may be able to extract personal customer information or to disrupt operational control of various utility systems leading to service outages and potential system damage. While, each utility is well aware of these risks and works to ensure the security of their electronic systems, it will become increasingly more important for this Commission to fully understand cybersecurity risks and to take any actions they feel will ensure the continuation of safe, adequate and proper utility services.

2. In October 2014, the Pennsylvania Public Utility Commission announced its publication of Cybersecurity Best Practices for small and medium Pennsylvania utilities. The guide outlined red flags to look for and ways to prevent identity or property theft, how to manage vendors and contractors who may have access to a company's data, what to know about anti-virus software, firewalls and network infrastructure, how to protect physical assets, such as a

¹ § 201 General jurisdiction and powers.

(a) The Commission shall have exclusive original supervision and regulation of all public utilities and also over their rates, property rights, equipment, facilities, service territories and franchises so far as may be necessary for the purpose of carrying out the provisions of this title.

² § 209 Standards, classifications, regulations, practices, measurements, services, property and equipment of public utility.

(a) The Commission may, after hearing, by order in writing:

(1) Fix just and reasonable standards, classifications, regulations, practices, measurements or services to be furnished, imposed, observed and followed thereafter by any public utility;

(2) Require every public utility to furnish safe and adequate and proper service and keep and maintain its property and equipment in such condition as to enable it to do so

computer in a remote location or a misplaced employee device, how to respond to a cyber-attack and preserve forensic information after the fact, and how to report incidents.³ (Exhibit A)

3. On March 13, 2016, the New Jersey Board of Public Utilities (“BPU”) issued guidelines that utilities are required to follow to help mitigate the threat of cybersecurity attacks. After the events of 9/11, the New Jersey legislature enacted the New Jersey Domestic Security Preparedness Act. The Act established a security preparedness planning taskforce to enhance and integrate security and preparedness measures throughout the State. One result of that effort was the formulation of the guidelines adopted by the New Jersey BPU. (Exhibit B)

4. The State of Maryland established a cybersecurity working group in May of 2011 as part of the Automated Meter Infrastructure (“AMI”) review. The working group was comprised of PEPCO, BGE and interveners (AARP, OPC, MEA, etc). The Group worked through how BGE and PEPCO would share Cyber Security information with the Commission. In Order Number 83571 the Maryland Commission, as part of the AMI approval process, required periodic reviews to include cybersecurity metrics. At this time reviews of cybersecurity specifics are conducted in private meetings with the Commission as permitted by Maryland law. (Exhibit C)

5. In the District of Columbia, cybersecurity issues have been the main focus of a special D.C. Homeland Security Commission taskforce since early 2010. The first annual report of that taskforce was released to the mayor and the D.C. Council in early 2014. However, two years after advisers urged the District of Columbia to take key actions to better manage potentially life-threatening cyber risks in the nation's capital, officials have not yet implemented

³ Pennsylvania Public Utility Commission News Release, October 2014, http://www.puc.state.pa.us/about_puc/press_releases.aspx?ShowPR=3425

the recommendations – leaving the seat of federal power lagging behind states nationwide and facing questions from the council overseeing D.C. agencies.⁴ (Exhibit D)

6. While each of these jurisdictions has taken the actions they feel are appropriate, there is no specific requirement for the Delaware Commission to take corresponding actions. Indeed, it would be premature to consider guidelines or regulations without further research and high level discussions with the regulated utilities that are dealing with this potential risk on a daily basis. However, it is important for this Commission to fully understand the cybersecurity issues and to ensure that our public utilities are appropriately managing this new electronic risk. Toward that end, Staff believes it would be extremely important for this Commission to conduct public workshops on the need for guidelines or regulations to ensure that all utilities are properly addressing this new technological risk.

7. Staff would not anticipate discussion of any specific cybersecurity threat risks or how the various utilities are addressing those specific risks. Staff does anticipate focusing the workshops on the general principles of cyber threat risk avoidance, the management actions that would be expected of all utilities within the cybersecurity environment and whether it would be appropriate to adopt general guidelines or regulations in support of Delaware's public utilities.

REQUESTED RELIEF

8. The Petitioner is requesting the Commission's authorization for Staff to issue public notice of and to schedule/conduct two (2) public workshops on the need for cybersecurity guidelines or regulations in Delaware to ensure the maintenance of safe, adequate and proper

⁴ Inside Cybersecurity, January 15, 2016, <http://insidecybersecurity.com/share/4254>

utility services in Delaware. Staff anticipates a “white paper” report back to the Commission that may include any proposed guidelines or regulations as the workshop reviews might suggest.

WHEREFORE, the Petitioner respectfully requests this Commission to:

- 1) authorize the Commission Staff to publicly notice, schedule and conduct two (2) public workshops, designed to provoke a high level discussion on the need for cybersecurity guidelines or regulations in Delaware, and
- 2) to require the Staff to report back to the Commission by no later than October 31, 2016, the results of the workshops and the positions of the participants with respect to the need for cyber security guidelines or regulations



On Behalf of Commission Staff
Robert J. Howatt
Executive Director
Delaware Public Service Commission

**BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF DELAWARE**

**IN THE MATTER OF A STAFF REVIEW OF THE)
NECESSITY FOR CYBERSECURITY GUIDELINES)
OR REGULATIONS FOR DELAWARE INVESTOR) PSC DOCKET NO. 16-0659
OWNED ELECTRIC, GAS AND WATER UTILITIES)**

CERTIFICATE OF SERVICE

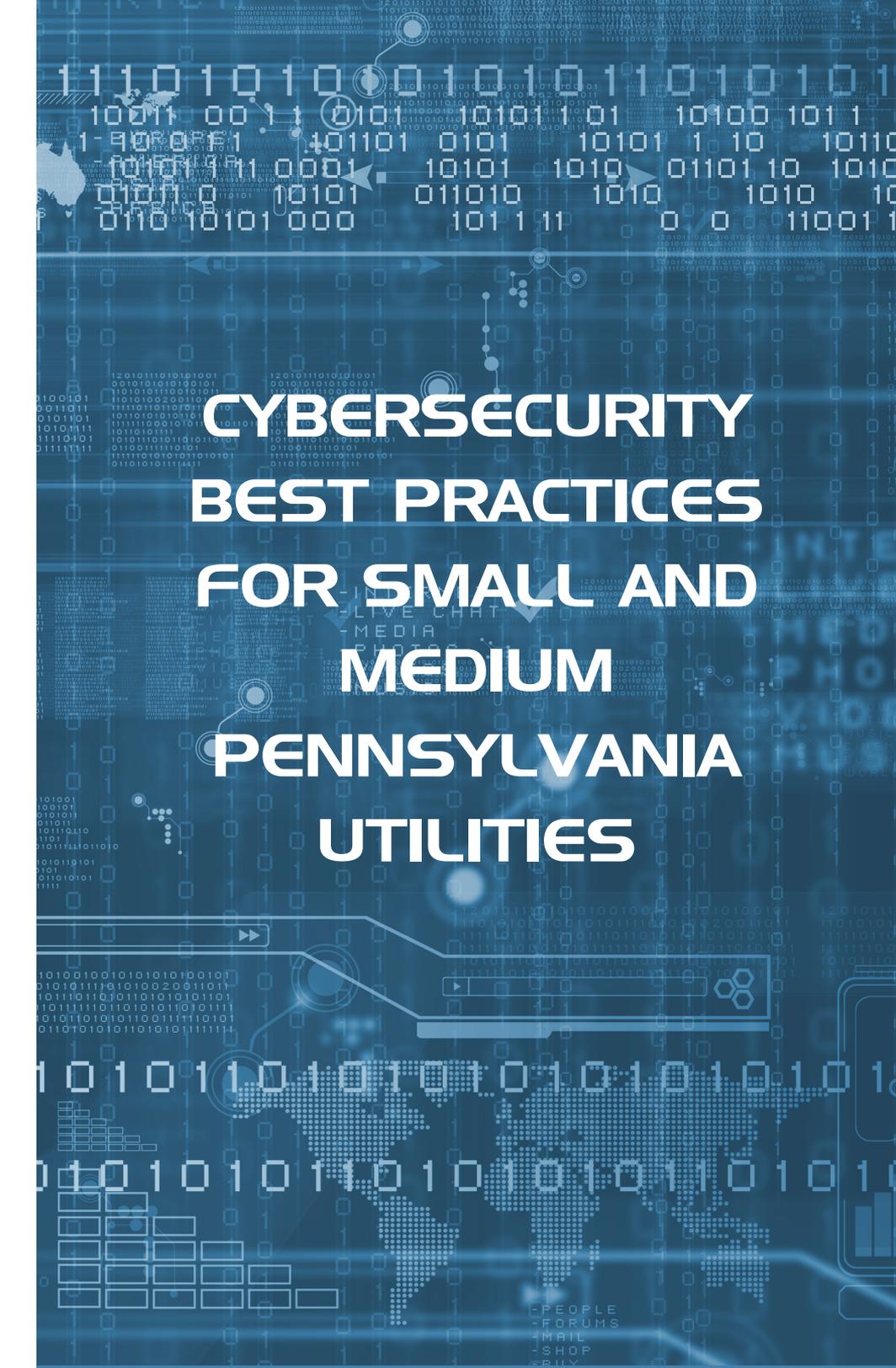
I hereby certify that on May 23, 2016, I caused the attached **PETITION OF THE DELAWARE STAFF TO REQUEST THE DELAWARE PUBLIC SERVICE COMMISSION AUTHORITY TO PUBLICLY NOTICE, SCHEDULE AND CONDUCT TWO (2) PUBLIC WORKSHOPS TO CONSIDER THE NEED FOR CYBERSECURITY GUIDELINES OR REGULATIONS** to be filed with the Delaware Public Service Commission via Delafile and to be served on the following persons via electronic mail:

Robert J. Howatt	robert.howatt@state.de.us
Jo Donoghue	julie.donoghue@state.de.us
Bob Willard	robert.willard@state.de.us
Matthew Hartigan	matthew.hartigan@state.de.us
Connie McDowell	connie.mcdowell@state.de.us
Donna Nickerson	donna.nickerson@state.de.us
Amy Woodward	amy.woodward@state.de.us
David Bonar	david.bonar@state.de.us
Andrea Maucher	andrea.maucher@state.de.us
Regina Iorii	regina.iorii@state.de.us
Pam Scott	pjscott@pepcoholdings.com
Bill O'brien	bobrien@chpk.com
Dave Spacht	dspacht@artesianwater.com
Jerry Esposito	jesposito@tuiwater.com
Larry Finnicum	lfinnicum@suez.com

/s/ Robert J. Howatt _____
Executive Director
Delaware Public Service Commission
861 Silver Lake Blvd., Suite 100
Dover, DE 19904

On behalf of the Delaware Commission
Staff

Dated: May 23, 2016



CYBERSECURITY BEST PRACTICES FOR SMALL AND MEDIUM PENNSYLVANIA UTILITIES

- PEOPLE
- FORUMS
- MAIL
- SHOP
- BUY

THE INFORMATION PROVIDED IN THIS DOCUMENT IS PRESENTED AS A COURTESY TO BE USED FOR INFORMATIONAL PURPOSES ONLY. THIS INFORMATION IS NOT INTENDED TO CONSTITUTE LEGAL ADVICE OR COUNSEL NOR IS IT A SUBSTITUTE FOR OBTAINING LEGAL ADVICE FROM YOUR OWN PRIVATE ATTORNEY.

CYBERSECURITY BEST PRACTICES FOR SMALL AND MEDIUM PENNSYLVANIA UTILITIES

I. ASK QUESTIONS

Cybersecurity is the responsibility of every employee; however, there are basic questions to which executives and employees should know the answers. For example:

- Who in my organization is responsible for cybersecurity?
- What are the rules that govern my use of company resources (computers, smartphones, tablets)? How can I be kept aware of updates to these rules?
- If I suspect I have a cybersecurity issue (malware, spyware), who should I contact within my organization?
- Does my organization have a policy on bringing personal devices into the workplace?
- What am I allowed to connect to my company's system and could my device infect the system?

There are any number of questions a company may wish to add to this list. Additional ideas can be found by using the resources mentioned in or attached to these best practices.

2. FOCUS ON HUMAN CAPITAL

When thinking about cybersecurity, the instinct is to focus on computers and keyboards, networks and servers. However, one of the biggest immediate cyber risks to most utilities comes from employees and vendors. It has been reported that one in five employees will click on a "bad" link. Robust security systems can be compromised by an employee clicking a link in a phishing email or accidentally installing malicious pieces of software on a computer. Human error remains a point of vulnerability and one that companies should address.



- Train and test staff regularly and repeatedly so that they understand and fully appreciate their role in maintaining a cyber safe work environment.
- Institute strong security rules for vendor access to systems, facilities and equipment.
- Develop strong policies concerning employee access to sensitive information especially at separation of employment.

3. COVER SOME OF THE BASICS

There are some basic rules all companies should follow in practicing good cybersecurity.

- Every user should have their own account with particular rights and restrictions. These rights should be limited to what the employee needs to perform their job duties.
- Users should have strong passwords requirements and should be prompted to update those passwords at regular intervals.
- Employees' cybersecurity responsibilities should be clearly identified in job descriptions, policy statements, or other company documents (like procedures manuals). Companies should update their employees' and contractors' security credentials as they move through the organization. Often, employees will still have access to systems despite moving to new areas that do not require such access or even upon leaving the company. Contractors may retain remote access to systems or sites even after their work is completed; companies should make concerted efforts to limit and prevent this remote access once outside vendors' contracts are complete.
- Security patches on software should be updated regularly.
- Older versions of software should be removed.



The U.S. Department of Homeland Security (USDHS) provides additional detailed advice on maintaining safe computer networks and systems.

4. RISK MANAGEMENT

Approaching cybersecurity in an organization can be overwhelming. Look at all of your company's systems and business processes, then start prioritizing.

- Which systems, IT or SCADA, and functions are most critical?
- Which data systems house your company's most sensitive information?

Concentrate efforts and resources there first.

5. USE AN ASSESSMENT TOOL

If your company is not sure where to begin on a risk assessment, the USDHS has created a Cybersecurity Evaluation Tool to guide users through a step-by-step process to assess their cybersecurity readiness. Companies can download this free tool at <https://ics-cert.us-cert.gov/Assessments>.

6. MANAGING VENDORS AND CONTRACTORS

Often, companies must rely upon third parties to handle aspects of their information technology infrastructure, control systems and security. It is critical that companies understand the security services that contractors provide.

- If your company uses an Internet Service Provider, it should ask about the various levels of security they offer including protection from distributed denial of service (DDOS) attacks.
- If vendors are going to be able to access your company's data, ensure that transfers of the data are properly protected and that the vendor has the necessary controls and procedures in place to maintain and protect confidential information.
- Be sure to draft requests for proposals (RFPs) that include requirements that support and consider your utility's security policies. This should include restricting employee access based on their job descriptions and responsibilities, and preventing access to systems based on vulnerabilities in existing infrastructure.

7. SECURITY AS A STARTING POINT

Decades of familiarity with anti-virus programs have conditioned people to think of cybersecurity as a separate tool to be added on top of other products. Today's software and control systems should be developed and designed from the outset with security in mind. Networks should be constructed to minimize possible intrusions and to allow a company to recognize when it is under attack.

- When possible, speak with vendors about the security characteristics of their products and incorporate cybersecurity as a key component in any new specifications your company develops.

8. DON'T OVERLOOK THE PHYSICAL

Discussions of cybersecurity tend to focus upon firewalls, network infrastructure and control systems. It is important not to forget about protecting your company's physical assets as well. For example, if your company has a computer on its network in a remote location, ensure that access is controlled and monitored. Employees or contractors who log in to your system remotely may inadvertently compromise your security by misplacing their devices.

- Understand the physical attack vectors that exist into your network and restrict access to those points.

9. TESTING

Training, assessment and system hardening are good, but they need to be tested regularly. In the same way utilities conduct exercises focused on physical security and disaster response, they should also focus upon cybersecurity scenarios. These exercises might range from sending a phishing email to employees to see if they click on the link to hiring a third party to attempt to penetrate your company's cyber defenses. USDHS's website offers some helpful tips for planning your own cybersecurity exercise.

IO. LEARN FROM YOUR PEERS

Some of the best resources out there are your peers. Trade associations and other forums can provide a great outlet for sharing best practices and learning measures that other companies are undertaking. National and state organizations like the National Association of Water Companies and the Energy Association of Pennsylvania have actively engaged their members on issues of cybersecurity. These groups can be a great resource on everything from the latest threat information to sample questions for vendors within your industry.

II. SO YOU'VE BEEN HACKED...

In today's world, it is not a question of whether your company has had a cybersecurity intrusion, it is whether your company knows about an intrusion or not. USDHS provides a useful



checklist for companies who have been infiltrated by cyber attackers. Your company's ability to detect the intrusion is critical, but do not forget to take steps to preserve forensic information after the attack. For example, running anti-virus software after the incident can change file names and dates, impeding the chances of discovering what caused the intrusion.

12. VIGILANCE

Your company's cybersecurity defenses are only as good as they are timely. State of the art technology and techniques for both attackers and defenders changes constantly. Be sure your company is keeping up with and aware of the latest threats and issues.



Government agencies, trade organizations and your company's own vendors can be great resources in ensuring that your organization is on top of the latest cybersecurity developments.

13. REPORTING INCIDENTS

The best way to support your company's and your industry's cybersecurity defenses is to ensure that your company timely reports incidents through the appropriate channels. Utilities and others can report attempted or successful intrusions through the U.S. Department of Homeland Security. If your company has been the victim of a cyber-crime, notify the appropriate regional office for the Federal Bureau of Investigation. The FBI has also established InfraGard, a public-private partnership for members to report and receive threat information.

14. DEVELOPING AND MAINTAINING APPROPRIATE WRITTEN CYBERSECURITY, EMERGENCY RESPONSE AND BUSINESS CONTINUITY PLANS PURSUANT TO 52 PA. CODE §§ 101.1-101.7

According to state regulations, most utilities are required to develop and maintain written security, emergency response and business continuity plans. In addition, utilities are required to file an annual self-certification form with the Public Utility Commission that affirms their compliance with this requirement. Information about the self-certification as well as the form are available on the Commission's website.

CYBER INCIDENT RESOURCES

PEOPLE
FORUMS

FEDERAL RESOURCES

DEPARTMENT OF HOMELAND SECURITY

The Office of Cybersecurity and Communications (CS&C) works with state and local government as well as private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C's National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training, recommended practices, as well as a large list of standards and references.

The ICS-CERT website can be found here: <https://ics-cert.us-cert.gov/>. ICS cyber incidents can be reported to: ics-cert@hq.dhs.gov.

FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation (FBI) has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyber-attack or suspected cyber incident. The

FBI encourages reporting of suspected cyber-attacks by critical infrastructure owners.

The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC)

The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Cyber incidents can be reported to the NCCIC watch desk at: NCCIC_WatchandWarning@hq.dhs.gov.

INFRAGARD

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide



range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators.

More information, including information on membership, can be found here: <https://www.infragard.org/>.

IGUARDIAN

The FBI recently release the iGuardian portal as a pilot program designed to give companies a designated location to report cyber threats they've encountered. Initially, the program will be open only to members of the InfraGuard Network (see above). The iGuardian portal offers a one-stop-shop for cyber incident reporting. Reports received by iGuardian will go to the local FBI office and the FBI may follow up with the reporting entity. More information on becoming an InfraGard member can be found here:

<https://www.infraguard.org/>.

STATE RESOURCES

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER (PACIC)

The PaCIC was formed in 2003 by the Pennsylvania State Police with the goal of proactively addressing the threats posed to our citizens from criminal and terrorist acts by sharing state police intelligence resources with criminal justice agencies in Pennsylvania and nationwide. The PaCIC's mission has expanded to include providing information bulletins to critical infrastructure partners as well as providing a means to report suspicious activities or emerging threats.

For more information on PaCIC, including applying to receive informational bulletins, please email or call: SP-ProtectPA@pa.gov, 855-772-7768.

PENNSYLVANIA OFFICE OF ADMINISTRATION – INFORMATION SECURITY OFFICE

The Pennsylvania Office of Administration (OA) is responsible for ensuring the cybersecurity of the Commonwealth network systems. OA has a website with information and resources related to cybersecurity that is available to the public.

The website can be accessed here: www.cybersecurity.state.pa.us.

PENNSYLVANIA PUBLIC UTILITY COMMISSION

Utilities are responsible for managing cybersecurity as part of their overall security planning and readiness. Jurisdictional utilities are required to self-certify that they have developed and maintained their security plans on an annual basis. Utilities cybersecurity plans are subject to audit by the Commission.

For more information on the Commission’s self-certification forms, visit:

www.puc.pa.gov/general/onlineforms/pdf/FAQ_PUSPR_Self_Certification.pdf (PDF)

or

www.puc.pa.gov/general/onlineforms/doc/FAQ_PUSPR_Self_Certification.doc (Word)

To download a Commission self-certification form, visit

www.puc.pa.gov/general/onlineforms/pdf/Physical_Cyber_Security_Form.pdf (PDF)

PENNSYLVANIA GOVERNOR’S OFFICE OF HOMELAND SECURITY

The Office of Homeland Security (OHS) coordinates homeland security functions among federal agencies, state government, regional task forces, local government, and the private sector. OHS is a source for general information about cybersecurity in the state.

More information is available at www.homelandsecurity.state.pa.us.



Agenda Date: 3/18/16
Agenda Item: 6A

STATE OF NEW JERSEY
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, New Jersey 08625-0350
www.nj.gov/bpu

RELIABILITY & SECURITY

IN THE MATTER OF UTILITY CYBER SECURITY)
PROGRAM REQUIREMENTS)

ORDER

)
)
)
)
) DOCKET NO. AO16030196

(SERVICE LIST ATTACHED)

BY THE BOARD:

The New Jersey Board of Public Utilities ("Board") initiated this matter in order to establish requirements to mitigate cyber risks to critical systems of electric, natural gas, and water/wastewater utilities ("Utilities"). As technology advances, Utilities' computerized systems are increasingly susceptible to cybersecurity attacks, including data breaches, corporate theft, and sabotage perpetrated by actors throughout the world. Due to the critical nature of the Utilities' services, the Board recognizes that action is necessary to mitigate cyber security risks to Utilities' computerized systems. In addition, to the extent information is shared and provided by the Utilities; the Board recognizes that such information is confidential and sensitive and requires appropriate confidentiality protections.

BACKGROUND

The New Jersey Domestic Security Preparedness Act was enacted after the events of September 11, 2001 to establish a domestic security preparedness planning group and task force to enhance and integrate security and preparedness measures throughout the State. N.J.S.A. App. A:9-68. "No record held, maintained or kept on file by the [New Jersey Domestic Security Preparedness Task Force ("Task Force")] or planning group shall be deemed to be a public record under the provisions of [the Open Public Records Act, N.J.S.A.] or the common law concerning the access to public records." N.J.S.A. App. A:9-74a. Pursuant to Executive Order No. 5 (Corzine), the Task Force is now part of the New Jersey Office of Homeland Security and Preparedness ("NJOHSP").

In the wake of the September 11 attacks, it became evident that Utilities could be prime targets for additional attacks. The State of New Jersey has found it necessary to develop standard utility industry security practices. In 2004, the Board ordered all utilities to implement the Best Practices and Recommended Response Protocols to the Homeland Security Advisory Systems ("Security Documents") developed by the Task Force, which superseded the preliminary utility security protocols and best practices initially implemented by the Board on December 11, 2001. See I/M/O Revised Security Best Practices For All Public Utilities and Cable Television Companies, BPU Dkt. No. AO04070733, Order dated August 20, 2004.

Pursuant to N.J.S.A. 48:2-36.1, the Board "may by order in writing require any public utility to ... submit to the Board any data, material and relevant to any inquiry, investigation, or proceeding."

Pursuant to N.J.A.C. 14:3-6.7, utilities are required to report various suspicious activities, including (a)(2) "forced entry to any utility facility, or entry achieved by deception;" and (a)(5) "intentional damage to any utility facility or equipment."

In 2011, the Board directed public utilities to report to Reliability and Security Staff regarding operation and use of their Industrial Control Systems ("ICS"). See I/M/O Cyber Incident Reporting for Utility Industrial Control Systems, BPU Dkt. No. EO11090575, Order dated October 23, 2011. The Board directed utilities under its jurisdiction to identify whether they use ICS, including Supervisory Control and Data Acquisition ("SCADA"), to monitor and/or remotely control utility facilities. It further directed those utilities who responded affirmatively to report cyber incidents involving those systems directly to the Director of Reliability and Security and Reliability and Security Staff designated by the Director of Reliability and Security ("Reliability and Security Division Staff") and to NJOHSP.

In 2013, President Barack Obama identified cyber threats to critical infrastructure as one the most serious security challenges facing our nation. See Executive Order No. 13636, February 19, 2013. To demonstrate his point, the President cited repeated attempts to sabotage the power grid and similar infrastructure by a host of enemies from hackers to nation states. He suggested that more needed to be done. (2013 State of the Union Address).

In 2015, pursuant to Executive Order No. 178 (Christie), the Governor established the New Jersey Cyber Security and Communications Integration Cell ("NJCCIC") under NJOHSP to coordinate cybersecurity information sharing and analysis between and among the government and private sectors. Specifically, NJCCIC was created to "receive relevant cybersecurity threat information from appropriate sources, including public utilities and private industry."

The U.S. Department of Homeland Security reported that attacks against utilities' digital infrastructure doubled in 2014. Moreover, a cyber-attack on the power distribution system in Ukraine in late 2015 underscored the risk for utilities in the U.S. The attack, triggered by unauthorized access to industrial control systems, caused regional disruptions to more than 225,000 people. See Alert (IR-ALERT-H-16-056-01), U.S. ICS-CERT, February 25, 2016.

Staff met with cyber security professionals from electric, natural gas, and water utilities on multiple occasions to discuss the approach to and specific requirements of cyber security for critical utility systems. These Utilities were given opportunities to review and provide comments to Staff on draft requirements. Substantive comments were incorporated into the final recommendations presented for Board consideration. Additionally, Staff consulted with cyber experts from the Federal Bureau of Investigation ("FBI") and NJOHSP.

DISCUSSION AND FINDINGS

As technology evolves, entry into a facility can be accomplished by means other than physical entry. In this case, the Board is concerned that unauthorized persons could be accessing Utilities' critical systems. Such access may be accomplished by forceful hacking or deception, such as social engineering. Pursuant to N.J.A.C. 14:3-6.7, such "entry" or damage to Utilities' computer system would constitute a reportable incident.

As described above, Utilities' systems are increasingly susceptible to cyber-attack, which jeopardizes safety, reliability, and customer privacy. Due to the critical nature of Utilities' services, action beyond information sharing and implementing best practices is necessary to safeguard the Utilities' critical systems.

The goal of cybersecurity is to safeguard the confidentiality, integrity, and availability of an organization's digital information assets. Risks associated with unauthorized access, changes or destruction of these assets must be effectively managed. A comprehensive Cyber Security Program represents both a strategic and tactical approach to risk identification and assessment, mitigation and monitoring, and audit and reporting.

To this end, Reliability and Security Division Staff developed a set of cyber security requirements that apply equally to Utilities to reduce cyber security risks to critical utility systems. For purposes of this Order, these systems include industrial control systems, including SCADA, and systems that contain customer personally identifiable information. Furthermore, the cyber security requirements generally focus activities at the program level rather than prescribe specific and detailed practices and technologies. In this way, Utilities may retain the flexibility necessary to meet the continuously evolving cyber threat landscape while remaining compliant to overarching cyber security program goals.

Reliability and Security Division Staff sought out and included input from cyber security experts at electric, natural gas, and water utilities. Additionally, Reliability and Security Division Staff consulted with FBI and NJOHSP during the development of these requirements.

Reliability and Security Division Staff recommends that the Board direct electric, natural gas, and water/wastewater utilities to meet certain cyber security program requirements to reduce cyber security risks to ICS and computer systems that contain customers' personally identifiable information. Reliability and Security Division Staff further recommends that these issues continue to be reviewed to determine whether these requirements should be extended to other parties subject to the Board's jurisdiction or otherwise broadened in scope by the Board.

The Board **HEREBY FINDS** that the Utilities must safeguard their computerized systems against cyber-attacks. The Board **FURTHER FINDS** that the sharing of information by the Utilities through NJCCIC is useful and vital to cyber security safeguarding. Therefore, pursuant to N.J.S.A. 48:2-36.1 and N.J.A.C. 14:3-6.7, the Board **HEREBY DIRECTS** that electric, natural gas, and water/wastewater utilities implement the following Cyber Security Program requirements, at a minimum, to manage cyber security risks, and that these measures would supersede the 2011 Cyber Security related order:

Scope of Assets

For purposes of this Order, covered assets, hereafter called critical systems, include the following:

- 1) industrial control systems (ICS), defined as a computerized system capable of gathering and processing data from utility facilities or applying operational controls to utility facilities; and
- 2) customer information systems that contain "personal information" as defined at N.J.S.A. 56:8-161.

Cybersecurity Requirements

Utilities must have a Cyber Security Program that defines and implements organizational oversight, accountabilities, and responsibilities for cyber risk management activities, and that establishes policies, plans, processes, and procedures for identifying and mitigating risk to critical systems to acceptable levels.

Additionally, the Cyber Security Program must meet the following minimum requirements:

1. Cyber Risk Management:

- a. Identify – Annually inventory critical systems and document changes.
- b. Analyze – Annually assess and prioritize cyber risks, including physical risks, to identified critical systems. At a minimum, incorporate information from the following as input into the risk analysis: vulnerability assessments; current threat assessment; and, relevant disaster recovery and business continuity requirements. Document risk assessment methodology and criteria used to assess and prioritize risks. A prevalent cyber security framework, such as those promulgated by National Institute of Standards & Technology ("NIST"), Department of Energy ("DOE"), and ISACA, should be considered when selecting a risk methodology.
- c. Control – Implement administrative, technical (logical and physical), and compensating controls, alone or in combination, to mitigate prioritized cyber risks in accordance with the assessment performed in 1b above.
- d. Measure and Monitor – Annually review risk assessment methodology to identify and incorporate revisions as appropriate.

2. Situational Awareness:

Utilities must maintain situational awareness of cyber threats and vulnerabilities so that cyber risks to critical systems are identified, mitigated, and remediated on an ongoing basis. At a minimum, Utilities shall:

- a. Monitor log files of critical systems, in accordance with the risk identified in 1b;
- b. Monitor internal and external sources of threat and vulnerability information, including vendor and industry-appropriate Information Sharing and Analysis Center ("ISAC") or Information Sharing and Analysis Organizations ("ISAO") advisories; and establish a review process to determine applicability and response.
- c. Review vendor security patches in a timely manner, and implement as appropriate.

3. Incident Reporting:

Utilities shall report the following, at a minimum, to designated Reliability and Security Division Staff:

- a. Utilities shall report cyber events relating to ICS, as set forth below:
 - i. A person, including any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity that accessed the ICS without authorization or exceeded authorized access. For purposes of this order, "exceeds authorized access" means a person who accesses the ICS with authorization and uses such access to obtain or alter information in the ICS that the person is not entitled to obtain or alter.
 - ii. Unauthorized programs, information, code or commands discovered on an ICS.
 - iii. A person extorted any money or other thing of value by threatening to cause damage to your industrial control system. For purposes of this order, damage includes any impairment to the integrity or availability of data, a program a system, or information.
 - iv. Reports must be submitted to Reliability and Security Division Staff through the NJ Cybersecurity and Communications Integration Cell ("NJCCIC") and in accordance with the prevailing rules, requirements, and submittal forms and formats designated by the NJCCIC. Pursuant to N.J.A.C. 14:3-6.7, reports shall be made within 6 hours of the detection of an incident.
- b. Utilities shall copy Reliability and Security Division Staff on notifications to law enforcement agencies of the State of New Jersey regarding information breaches involving the personally identifiable information of customers to the extent such notifications are required by the laws of the State of New Jersey, including, but not limited to, N.J.S.A. 56:8-163.
- c. Utilities shall report unusual cyber activity that has the potential to compromise critical systems and for which controls are ineffective. Reports must be submitted to Reliability and Security Division Staff through the NJCCIC and in accordance with the prevailing rules, requirements, and submittal forms and formats designated by the NJCCIC.

4. Response and Recovery:

- a. Establish a Cyber Security Incident Response Plan ("Plan") that addresses the life-cycle of an incident, including identification of, response to, and recovery from a cyber event. The Plan must include protocols for log file retention to support forensic analyses.
- b. Conduct an exercise to test the Plan once every 24 calendar months, at a minimum. The exercise can be a tabletop or a response to an actual cyber incident. Subsequent to the exercise or cyber incident, the utility shall document and incorporate lessons learned into the Plan, as appropriate.

5. Security Awareness and Training:

- a. Develop and implement a cyber security awareness program.
 - i. The cyber security awareness program must include general cybersecurity topics as well as emerging threats.
 - ii. The cyber security awareness program must be reviewed biannually and updated as appropriate.
- b. Cyber security awareness communications must be provided periodically throughout the year.
- c. Develop and implement cyber security training that details cyber security roles and responsibilities, for individuals who have access credentials to industrial control systems and for administrators of customer information systems that contain personal information.
- d. Develop and implement protocols for training new personnel as well as periodic training re-enforcement.

Implementation

1. Utilities must join the NJCCIC and create a cyber security incident reporting process no later than 60 days after the effective date of this order. Utilities must submit written confirmation of compliance with this requirement to Reliability and Security Division Staff no later than June 1, 2016.
2. Utilities must submit a written report to Reliability and Security Division Staff no later than June 1, 2016 that documents the assignment of organizational oversight, accountabilities, and responsibilities for cyber risk management activities.
3. Utilities must comply with all other requirements no later than October 1, 2017. Utilities must submit a written certification of compliance to Reliability and Security Division Staff no later than October 31, 2017. The certification must be signed by appropriate executive-level personnel with authority for the Utilities' Cyber Security Program.
4. Utilities must submit a written report to Reliability and Security Division Staff no later than December 31, 2016 describing progress toward compliance with these requirements and defining potential barriers that may interfere with meeting the defined implementation date.

Accountability and Board Review

1. Utilities shall certify on an annual basis compliance with the minimum requirements set forth above. Such certification must be submitted to Reliability and Security Division Staff no later than December 31 of each year following the implementation period. Further, each certification must be signed by appropriate executive-level personnel with authority for the Utility's Cyber Security Program.
2. In cases where Utilities have critical systems that are also subject to North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards, certification of compliance with those standards is sufficient to meet the annual certification requirement under this order for those critical systems. Such certification of compliance must be submitted to Reliability and Security Division Staff in accordance with the timeline noted above.
3. Utilities shall cooperate with Reliability and Security Division Staff in evaluations of the effectiveness of the Utilities' Cyber Security Program.

The Board further **DIRECTS** Reliability and Security Division Staff to review incidents of cyber intrusion into critical systems as defined in this Order. The Board **HEREBY FINDS** that in order to facilitate this review it must gather information from the Utilities. The Board further **DIRECTS** the Utilities to report and certify on the adequacy of the utility security arrangements as set forth in this Order. Reliability and Security Division Staff will continue to monitor the Utilities' performance and compliance with the Cyber Security Program requirements documented in this Order.

The Board further **DIRECTS** Staff to share information with NJCCIC regarding Utilities' cyber intrusions.

The Board further **DIRECTS** Reliability and Security Division Staff to continue to review and determine the appropriateness of a Cyber Security Program for any public utilities and other entities subject to the Board's jurisdiction not subject to this Order.

Reliability and Security Division Staff shall further review the Cyber Security requirements set forth in this order to determine whether additional requirements or program refinements are appropriate.

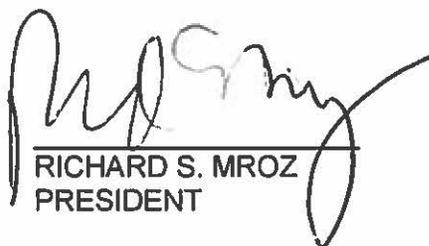
The Board has given consideration to the sensitive security nature of the information and reports required by this order, including the Utilities' Cyber Security Programs and the Utilities' ability to defend against cyber intrusions. The Board **FINDS**, consistent with Executive Order No. 21 (McGreevey), that public disclosure of such information would "substantially interfere with the State's ability to protect and defend its citizens against acts of sabotage or terrorism or would materially increase the risk or consequences of potential acts of sabotage or terrorism". The Board **FURTHER FINDS** that similar Cyber Security information reported to NJCCIC, within NJOHSP, would be deemed confidential. Therefore, the Board **HEREBY ORDERS** that in exercising its authority pursuant to N.J.A.C. 14:1-12.1(e), any reports and other information submitted, collected or exchanged in accordance with this Order shall be deemed confidential and shall not be considered to be a government record consistent with N.J.S.A. 47:1A-1 et seq. As such, when submitted by Utilities, such information shall be appropriately labeled and protected consistent with the Board's confidentiality rules. The Board directs staff to develop a Memorandum of Understanding, to be negotiated between the BPU and the New Jersey

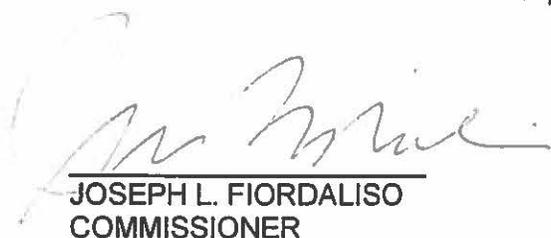
Cybersecurity Communications and Integration Cell ("NJCCIC"), to address how cybersecurity information submitted to NJCCIC will be handled and shared with the BPU. The Board **FURTHER AUTHORIZES** the President to execute such a Memorandum of Understanding on behalf of the BPU.

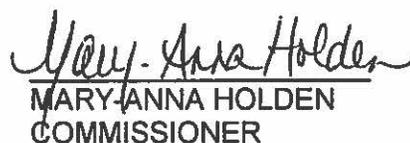
This Order shall be effective on March 28, 2016.

DATED: 3-18-16

BOARD OF PUBLIC UTILITIES
BY:

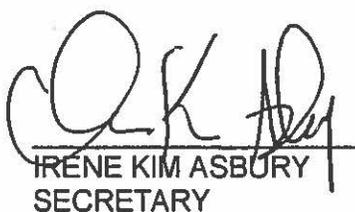

RICHARD S. MROZ
PRESIDENT


JOSEPH L. FIORDALISO
COMMISSIONER

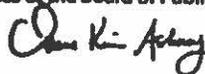

MARY-ANNA HOLDEN
COMMISSIONER


DIANNE SOLOMON
COMMISSIONER


UPENDRA J. CHIVUKULA
COMMISSIONER

ATTEST: 
IRENE KIM ASBURY
SECRETARY

I HEREBY CERTIFY that the within
document is a true copy of the original
in the files of the Board of Public Utilities



IN THE MATTER OF UTILITY CYBER SECURITY PROGRAM REQUIREMENTS

Docket No. AO16030196

SERVICE LIST

Irene Kim Asbury, Esq.
Secretary of the Board
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Irene.asbury@bpu.state.nj.us

Kenneth Sheehan, Esq.
Chief of Staff
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Kenneth.Sheehan@bpu.state.nj.us

Paul Flanagan, Esq.
Executive Director
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Paul.Flanagan@bpu.state.nj.us

James Giuliano, Director
Division of Reliability & Security
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
James.Giuliano@bpu.state.nj.us

Lynn Costantini
Division of Reliability & Security
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Lynn.Costantini@bpu.state.nj.us

Tim Davies, President & CEO
Applied Wastewater
2 Clerico Lane
Hillsborough, NJ 08844-1615

William Davis, President
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08691

John Hildabrandt, Manager Operations
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08691

David Watson, Acting Superintendent
Berlin Borough
59 South White Horse Pike
Berlin, NJ 08009

John Walls, Supervisor
Bordentown City
324 Farnsworth Avenue
Bordentown, NJ 08505

Burt Lundbert, President
Cedar Glen Lakes Water
Michigan Avenue
Whiting, NJ 08759

Robert Cutter, Business Admin
Kathy Olsen, CFO
Clinton Town of
43 Leigh Street
PO Box 5194
Clinton, NJ 08809

Jan Kokes, President
Thomas O'Gara, Manager
Crestwood Village Water
55 Schoolhouse Road
Whiting, NJ 08759

Carol Artale, Esq.
Legal Specialist
Counsel's Office
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
Carol.Artale@bpu.state.nj.us

James Kane, Esq.
Legal Specialist
Counsel's Office
Board of Public Utilities
44 South Clinton Avenue, 3rd Floor, Suite 314
Post Office Box 350
Trenton, NJ 08625-0350
James.Kane@bpu.state.nj.us

Geoffrey Gersten, Esq.
Department of Law and Public Safety
Division of Law
124 Halsey Street
Post Office Box 45029
Newark, NJ 07102-45029
Geoffrey.gersten@dol.lps.state.nj.us

Roger Pederson
Manager, NJ Regulatory Affairs, External
Issues and Compliance
ACE – 63ML38
5100 Harding Highway
Mays Landing, NJ 08333

Philip J. Passanante, Esq.
Associate General Counsel
ACE – 92DC42
500 North Wakefield Drive
Post Office Box 6066
Newark, DE 19714-6066

Alison Regan
Pepco Holdings, Inc. – 79NC59
401 Eagle Run Road
Post Office Box 9239
Newark, DE 19714-9239

Luis Acevedo, Interim Superintendent
Dover Town of
100 Princeton Avenue
Dover, NJ 07801

James Carroll, Manager
John Sanclimenti, President
Jeff Kalajian, Vice President
John Cannie, Treasurer
Fayson Lakes Water
160 Boonton Avenue
Kinneelon, NJ 07405

Dorothy Gorman, Owner
Charles Gartland, Chairman
John McDonough, President
Bob Chozick, VP
Forest Lakes Water
45 Sleepy Hollow Road
PO Box 264
Andover, NJ 07821

Gary Ern, President
David Ern, Vice President
Gordon's Corner Water
475 County Road 520
Marlboro, NJ 07746

Jeffrey Fuller, President
Lake Lenape Water
83 Eagle Chase
Woodbury, NY 11797

Steve Parah, Superintendent
Lawrenceville Water
12 Gordon Avenue
Lawrenceville, NJ 08648

Dennis Doll, President
Middlesex Water
1500 Ronson Road
PO Box 1500
Iselin, NJ 08830-0452

Mario A. Giovannini
Pepco Holdings, Inc. – 79NC22
401 Eagle Run Road
Post Office Box 9239
Newark, DE 19714-9239

John L. Carley, Esq.
Consolidated Edison Co., of NY
Law Department, Room 1815-S
4 Irving Place
New York, NY 10003

Margaret Comes, Sr. Staff Attorney
Consolidated Edison Co., of NY
Law Department, Room 1815-S
4 Irving Place
New York, NY 10003

Brian MacLean
Elizabethtown Gas
52 Green Lane
Union, NJ 07083
bmaclean@aglresources.com

Mary Patricia Keffe, Esq.
Elizabethtown Gas
520 Green Lane
Union, NJ 07083
pkeefe@aglresources.com

Kevin Connelly
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Mark A. Jones
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Jim O'Toole
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

John Brunetti, President
John Brunetti Jr., Vice President
Midtown Water
1655 U.S. Highway 9
Red Oak Lane
Old Bridge, NJ 08857

Lawrence Schumacher, President
John Stover, VP & Secretary
Steven Lubertozzi, VP & Treasurer
Montague Water
2335 Sanders Road
Northbrook, Illinois 60062

Henry Schwarz, President
Salvatore Garofalo, VP
Mt. Olive Villages Water
200 Central Avenue
Mountainside, NJ 07092

John Bigelow, President
New Jersey American
131 Woodcrest Road
Cherry Hill, NJ 08034

Bill Beattie, Director Operations
George Mehm, President
John Poulestsos, Vice President
Park Ridge Borough
53 Park Avenue
Park Ridge, NJ 07565

Robert Bebee, Superintendent
Dennis Doll, Chairman
Richard Risoldi, President
Bruce O'Connor, VP & Treasurer
Pinelands Water
1500 Ronson Road
Iselin, NJ 08830-0452

Frank J. Moritz, Director
Ridgewood Village of
13 North Maple Avenue
Ridgewood, NJ 07451

Mark A. Mader
First Energy
300 Madison Avenue
Post Office Box 1911
Morristown, NJ 07962-1991

Lauren Lepkoski
FirstEnergy Corp.
2800 Pottsville Pike
Reading, PA 19612
llepkoski@firstenergycorp.com

Bradley A. Bingaman
FirstEnergy Corp
76 South Main Street
Akron, Ohio 44308
bbingaman@firstenergycorp.com

Andrew Dembia, Esq.
Director, Regulatory Affairs Counsel
New Jersey Natural Gas 1415 Wyckoff Road
Wall, NJ 07719
adembia@NJNG.com

Alexander C. Stern, Esq.
Assistant General Regulatory Counsel
PSEG Services Corporation
80 Park Plaza, T5
Newark, NJ 07102
Alexander.stern@pseg.com

Martin C. Rothfelder, Esq.
Law Department
PSEG Services Corporation
80 Park Plaza, T5G
Newark, NJ 07102-4194

Shawn P. Leyden
PSEG Energy Resources & Trade, LLC
80 Park Plaza, T19
Newark, NJ 07102

Hesser McBride, Esq.
PSE&G Services Corp.
80 Park Plaza, T5
Newark, NJ 07102
Hesser.mcbride@pseg.com

John (Jack) Hosking, President
Roxbury Water
79 Sunset Strip
PO Box 560
Succasunna, NJ 07876

Roger Hall, Vice President
Lawrence Zucker, Controller
Roxiticus Water
1920 Frontage Road
Suite 110
Cherry Hill, NJ 08034

Roger Hall, Vice President
S. B. Water
1920 Frontage Road Suite 110
Cherry Hill, NJ 08034

Daniel T. Stephano, Acting VP
Seaview Water
102 South Manor Avenue
Longport, NJ 08403

Samuel J. Faiello, President
Shore Water
105 23rd Avenue
South Seaside Park, NJ 08752

Michael Walsh, President
Shorelands Water
1709 Union Avenue
Hazlet, NJ 07730

David Simmons, President
Simmons Water
PO Box 900
Branchville, NJ 07826-0900

Frida Salvigsen, President
Tranquility Springs
PO Box 99
West Milford, NJ 07480

Robert Iacullo, President
United Water New Jersey
200 Old Hook Road
Harrington Park, NJ

Stacy A. Mitchell, Esq.
Cozen O'Connor, PC
457 Haddonfield Road, Suite 300
Post Office Box 5459
Cherry Hill, NJ 08002
smitchell@cozen.com

John F. Stanziola
Director, Regulatory Affairs
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
istanziola@sjindustries.com

Gina Merritt-Epps, Esq.
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
gmerritt@sjindustries.com

Abbey Greenberg
Public Affairs Specialist- Government &
Regulatory Affairs
South Jersey Gas Company
One South Jersey Plaza, Route 54
Folsom, NJ 08037
agreenberg@sjindustries.com

Nicholas Rizzo, President
Tanya Rovner, Edgewater Assoc
Walkkill Sewer
3331 Rt. 94 South
Hamburg, NJ 07419

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Arlington Hills
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Great Gorge
200 Old Hook Road
Harrington Park, NJ 07640

Nadine Leslie, Regional Mgr
James Mastrokalos, Superintendent
United Water Matchaponix
103 Wilson Avenue
Manalapan, NJ 07726

Nadine Leslie, Regional Mgr
United Water Toms River
15 Adafre Avenue
Toms River, NJ 08753

Michael Janel, President
Vernon Water
P.O. Box 376
Pompton Lakes, NJ 07442

Nicholas Rizzo, President
Walkkill Water
3331 Route 94 South
Hamburg, NJ 07419

Tim Davies, President/CEO
Applied Wastewater
2 Clerico Lane
Suite #1
Hillsborough, NJ 08844

William Davis, President
John Hildabrandt, Manager Operations
Aqua NJ
10 Black Forest Road
Hamilton, NJ 08054

Robert Fitzgerald, President
Atlantic City Sewerage
1200 Atlantic Avenue
Suite 300
Atlantic City, NJ 08404

Jan Kokes, President
Crestwood Village Sewer
55 Schoolhouse Road
Whiting, NJ

Thomas Dillon, President
Environmental Disposal
Rt. 202/206
Bedminster, NJ 07978

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Princeton Meadows
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water Vernon Sewer
200 Old Hook Road
Harrington Park, NJ 07640

Robert Iacullo, President
James Glozzy, VP & Gen Mgr
United Water West Milford
200 Old Hook Road
Harrington Park, NJ 07640

Lawrence N. Schumacher, President
Montague Sewer
2335 Sanders Road
Northbrook, IL 60062

Henry Schwarz, President
Mt. Olive Villages Sewer
200 Central Avenue
Mountainside, NJ 07092

John Bigelow, President
New Jersey American Water
131 Woodcrest Road
Cherry Hill, NJ 08034

Jeffrey Goldstein, VP
Oakwood Village Sewer
308 Vreeland Road
Florham Park, NJ 07932

Robert Risoldi, President
Dennis Doll, Chairman
Bruce O'Connor, VP & Treas
Pinelands Wastewater
1500 Ronson Road
Iselin, NJ 08830-0452

David R. Monie, President – GPM
Roger M. Hall, VP
Larry Zucker, Treasurer
S. B. Sewer
1920 Frontage Road
Suite 110
Cherry Hill, NJ 08034

Cyber Security

Introduction:

Pepco and BGE are deploying Advanced Metering Infrastructure based on Silver Spring Networks technology. The utilities, along with Silver Spring Network and our system integrator vendors have developed these solutions with security in mind. The utilities have taken a holistic approach to address security. Cyber security has been evaluated from the meter to the backend systems.

The Utilities place a high level of focus on the security and protection of all aspects of the electric system, including customer information and associated sub systems. The Utilities are designing the Smart Grid systems and components so that it will guard against cyber and physical attacks. As the Smart Grid is implemented applicable prudent security practices, policies and standards will be incorporated into these systems.

Cyber Security methods that are used to protect the Smart Grid systems must **remain** confidential. Based on the need to keep such measures confidential and security requirements evolve, Pepco and BGE will provide separate annual face to face briefing to the Maryland Commission. The briefings will provide up-to-date information on the protection of these systems and future enhancements required to continue protecting the systems. This briefing will remain confidential; similar to other trade secrets or contractual matters. The procedures for these updates are identified in section titled "Guidelines for Cyber Security Update". This forum will allow the commission to obtain an understanding of protection of these systems and determine the effectiveness of the employed security methods.

Cyber Security Research

Pepco and BGE's Smart Grid cyber Security approach is in line with other utilities that have experience in deploying Smart Grid networks. To that end, we conducted telephone interviews with a number of utilities and asked them how they are handling their respective Smart Grid Cyber Security information requests by their local Interveners and Commission Staff.

Attached is a table that summarizes the utility responses. The consensus response is that these utilities have basically done what we've done so far –

provide an overview of their Cyber Security approach and discussed why it's such a critical part of their Smart Grid network. However, none of the utilities we spoke with have shared the "how" their respective Cyber Security plans work with anyone outside their respective utility. That's where the confidentiality issues arise.

What has been provided, if anything, is an overview of the importance of Cyber Security and to reiterate how seriously each utility takes this topic. None of the utilities we spoke with get into the "how" their respective Cyber Security systems operate.

Structure of Report:

Pepco and BGE agree that each utility will provide a separate update to the commission. These annual updates shall include at a minimum the following sections:

Project Overview:

Utilities to provide an overview of the Smart Grid systems that accurately describe the overall project. This should include the Home Area Network (HAN), Local Area Network (LAN), Wide Area Network (WAN), manufactures, vendors, communications systems, key components and back end systems.

Security Framework:

Utility to describe overall framework that will be used as the guiding principles to develop the Advanced Metering Infrastructure. This framework should include examples of how this framework applies to the systems that support the Smart Grid.

Overview Security Risk:

Utility to describe the overall risk associated with the Smart Grid. This should include communications systems, end components, and data facilities that house the smart grid and backend systems.

Overview Security Protections:

Utility to describe overall cyber security protections of the Smart Grid. This should include communications, authentication, encryption, data integrity checks, overview of security for the data facilities that house Smart Grid components and access control.

Security Governance Structure:

Utility to describe the organizational structure and governance process required to support cyber security within their company.

Security Assessments:

Utility to describe security assessments that have been conducted on the Smart Grid systems. This could include internal assessments as well as 3rd party assessments.

Risk Mitigation Strategies:

Utility will provide an update on the risk mitigation strategies that have been used to evaluate risks associated with the Smart Grid. The risk mitigation strategy should cover architecture, countermeasures, risk assessments, incident response, training, and employee awareness.

Changes or Additions from Prior Report Out:

The utility will report any Cyber Security modification since the last report. These should include changes in technology, vendors, standards, new features and functionality, and communications methods that could affect the security of the Smart Grid systems.

Roadmap Cyber Security Items:

The utility will provide future cyber security protections that will be designed into the Smart Grid systems.

Guidelines for Cyber Security Update:

Ordering Paragraph 5 of Order No. 83571 in Case No. 9207 directed Pepco and the parties in that case to develop performance metrics for cyber security. Because metrics reporting on cyber security could reveal information that third parties could exploit in order to detect vulnerabilities in the Companies' AMI systems, the Companies propose to brief the Commissioners and their advisors on cyber security matters in a confidential session to be held at the Commission's offices, in lieu of the submittal of metrics on this topic. Due to the highly sensitive nature of the information that will be disclosed, it is imperative that the persons having access to cyber security information be closely controlled. A filing made even confidentiality could expose the Companies'

systems, and accordingly, reliability of the electric system, to risk because further dissemination could not be controlled and thus the protection of such materials and information could not be guaranteed. Therefore, the confidential briefing should be limited only to representatives of the Companies, the Commissioners and their advisors. BGE and Pepco propose to provide a verbal presentation to the Commissioners and their advisors, and if any written documentation is distributed at the presentation, the Companies propose to collect those written materials at the conclusion of the meeting for their destruction to ensure confidentiality. During the deployment period, the Companies recommend annual meetings. This process meets the requirements of the Commission's order to enable it to monitor the progress of the Companies' AMI initiatives, while maintaining the highest level of confidentiality.

DRAFT



District of Columbia
Homeland Security Commission
2013 Annual Report

Letter from the Homeland Security Commission

We are pleased to present the first District of Columbia Homeland Security Commission Annual Report.

The Homeland Security Risk, Reduction, and Preparedness Amendment Act of 2006 tasks the Homeland Security Commission (Commission) with gathering and evaluating information on the status of homeland security in the District of Columbia, measuring progress and gaps in homeland security preparedness, and recommending security improvement priorities in consultation with major public and private entities.

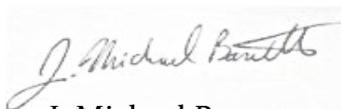
With such a broad statutory agenda confronting it, the Commission decided that it could most effectively contribute by focusing on a single topic, rather than undertaking a cursory overview of the many subjects within its purview. This report outlines our general findings on the state of cybersecurity within the District Government, and recommendations for improving upon the efforts already underway to protect the information management and cyber assets of the District.

The Commission would like to thank Chris Geldart, Director of the District of Columbia Homeland Security and Emergency Management Agency, and his staff, for the administrative and logistical support provided to Commission members; and the Deputy Mayor for Public Safety and Justice, Paul Quander, for his support in our efforts. Finally, the Commission thanks Mayor Vincent C. Gray for the opportunity to serve in this trusted capacity.

The District of Columbia Homeland Security Commission



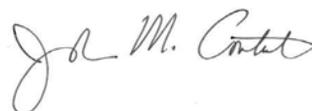
Darrell Darnell
Chairman



J. Michael Barrett
Commissioner



Barbara Childs-Pair
Commissioner



John M. Contestabile
Commissioner



Andrew Cutts
Commissioner



Glenn S. Gerstell
Commissioner



Daniel Kaniewski
Commissioner

Table of Contents

Executive Summary.....4

General Findings.....6

Recommendations9

Appendices.....16

Appendix A: Commission and Stakeholder Meetings.....16

Appendix B: Agency Findings.....17

Appendix C: Background Information about the Commission.....25

Appendix D: List of References.....27

Executive Summary

The Homeland Security Commission (Commission) was established by the Homeland Security, Risk Reduction, and Preparedness Amendment Act of 2006¹ and the primary function of the Commission is to make recommendations for improvements in homeland security and preparedness in the District of Columbia and report its findings to the Mayor and the District of Columbia Council. The Commission met on a quarterly basis throughout the year to discuss and evaluate the status of homeland security within the District.²

With such a broad statutory agenda confronting it the Commission decided that it could most effectively make a contribution by focusing on a single topic, rather than undertaking a cursory overview of the many subjects within its purview. This way the Commission could best harness the expertise of its members and provide assessment, analysis, and recommendations that could have a meaningful effect on the state of homeland security for the District.

In selecting its initial topic for review, the Commission considered such factors as the importance of the topic to the District's overall security, the extent of attention and resources already devoted to the topic relative to the perceived homeland security threat, the likelihood of generating recommendations that could genuinely improve security, the ability of the District Government and the local community to implement any such recommendations (as opposed to, for example, regional or federal matters or matters wholly within the private sector), and the expertise available to the Commission both within its members and the staff of the District Government.

Cyber threats affect all sectors of critical infrastructure and key resources, whether in government or private hands, and have the potential for disrupting the four lifeline sectors – energy, transportation, water, and telecommunications.

It quickly became clear to the Commission, in evaluating these and other factors, that the topic of cybersecurity fully warranted becoming the subject of the Commission's initial undertaking. There is a consensus among industry experts and national security officials

¹ The Homeland Security Risk, Reduction, and Preparedness Amendment of 2006, District of Columbia Code §7-2201.02 and §7-2201.03.

² See Appendix A for a full list of Commission and stakeholder meetings held throughout this year.

that the cybersecurity threat represents the greatest overall disparity between the potential for damage relative to the ability to thwart such a threat.

During the past year, the Commission met with a select group of District agencies and private sector stakeholders to discuss their efforts in bolstering cybersecurity protections and mitigating against cyber attacks to its systems. The Commission interviewed representatives from the Office of the Chief Technology Officer, the Metropolitan Police Department, the District of Columbia Water and Sewer Authority, and the Washington Metropolitan Area Transit Authority. These agencies were selected due to their critical role in developing and implementing cybersecurity measures and their importance to life sustaining processes including maintaining the District's technology infrastructure, protecting the safety of District residents, managing the treatment of District wastewater, and providing multiple modes of reliable transportation.³

In addition, the Commission interviewed the District of Columbia National Guard to better understand the potential role and assistance the military could provide during a potential cyber attack in the District. Finally, the Commission requested an informational briefing from Pepco (a subsidiary of Pepco Holdings, Inc.) as it is the supplier of electric power to the District and is central to understanding potential cyber disruptions to the District's electrical grid, and the cascading effects any disruption would have on other lifeline critical infrastructures.

As a result of these discussions the Commission found that the lack of a senior executive level Chief Information Security Officer (CISO) hampers the ability of the District to establish and maintain a District-wide strategy and program to protect information management assets; that communication and coordination between District agencies and with private sector stakeholders needs to be strengthened; and that additional investments in cyber workforce education and training would enhance the overall cybersecurity preparedness and protection efforts for the District.

In the future, the Commission hopes to revisit the cybersecurity topic as well as other critical issues impacting homeland security in the District.

³ See Appendix B for more detailed descriptions of each District agency that was interviewed for the Annual Report.

General Findings

1) The District of Columbia lacks a senior executive-level Chief Information Security Officer (CISO).

Currently, the District of Columbia's Chief Technology Officer is also the official CISO for the City. The Office of the Chief Technology Officer (OCTO) has created a CISO position under the auspices of its agency and has posted this position online in the past, but that position remains unfilled. There are no explicit CISO roles within any other District agency and the CISO position within OCTO would not have either the bureaucratic independence or authority necessary to oversee citywide risk reduction efforts.

The lack of an enterprise-level CISO that serves the entire City without affiliation to any one District agency hampers promotion of a City-wide vision and strategy to reduce information technology risk, respond to incidents, establish appropriate standards and controls, and maintain regulatory compliance.

2) There is a need for stronger communication and coordination among cybersecurity partners.

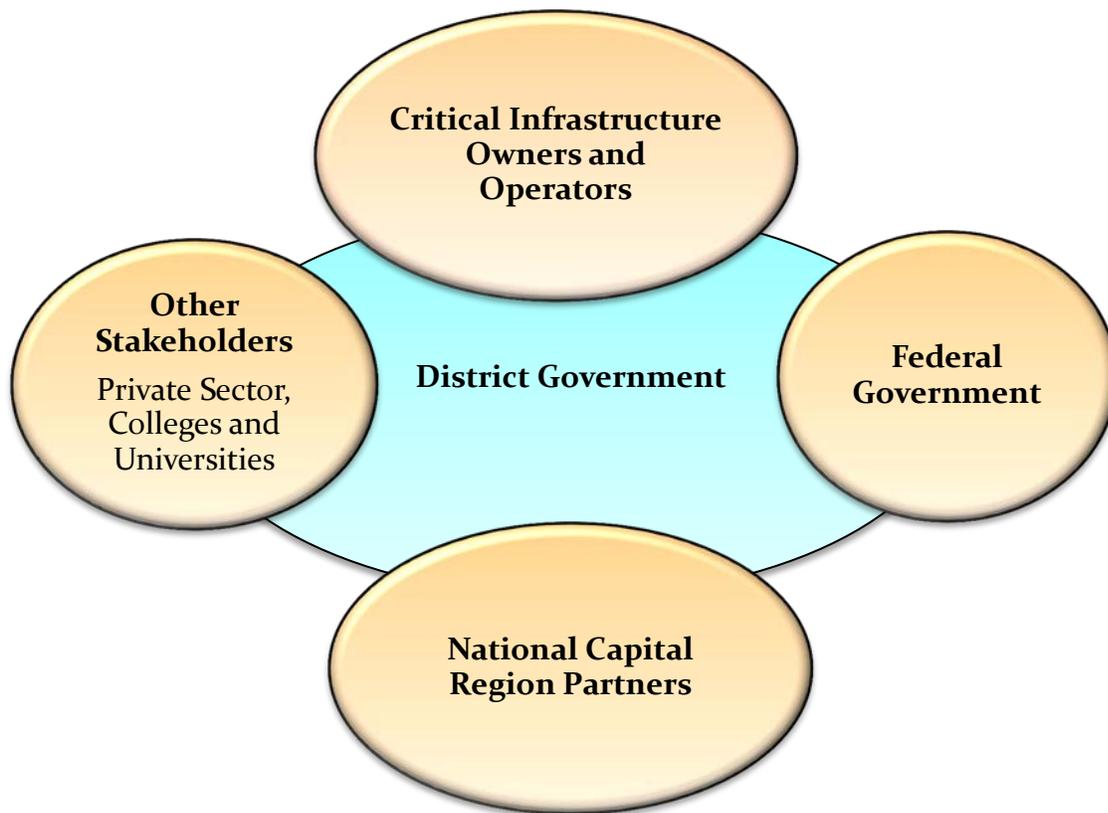
While much effort is being expended by hardworking and qualified personnel, the Commission found that there is a lack of communication between District agencies when trying to identify, manage, and address cyber threats. Several agency officials expressed to the Commission that they were unsure of either their or OCTO's official roles and responsibilities in combating cyber incidents, including how, to whom, and when to report an incident. They also expressed the need for clearer policies outlining each agency's obligations and duties when addressing cyber threats.

District officials informed the Commission that, while the responsibility for the security of many of the critical infrastructure components in the District lies in the hands of the systems' owners, *effective mitigation and response depend on collective situational awareness and coordination*. Agency officials desire and need to build stronger relationships amongst each other and with outside stakeholders, including the private sector and the Federal Government, in an effort to enhance mutually beneficial collaboration. Several District agencies also expressed their desire to engage in more cyber awareness outreach and training that is co-sponsored by multiple District agencies. It is important to harness this positive attitude and willingness to cooperate as soon as possible.

In addition, if the District established official communication and coordination policies regarding cyber incidents, clearly delineating the roles and responsibilities of each District agency and the proposed CISO, this would help eliminate confusion and educate more personnel on their designated duties in the prevention of or response to a cyber attack. This would also ensure that District agencies are working towards expanding their response activities beyond existing limited information sharing relationships.

The graphic below conceptually demonstrates the interlocking cybersecurity relationships between various partners needed when coordinating an integrated incident response to a cyber incident. These partners may include, but are not limited to: National Capital Region partners, the Federal Government, the District Government, critical infrastructure owners and operators, private-sector stakeholders, and institutions of higher learning. The graphic demonstrates how multiple agencies and partners could work together in a collaborative risk reduction process which, of necessity, includes various stakeholder groups.

The District of Columbia's Interlocking Cybersecurity Relationships



3) The lack of a larger cyber workforce and a dedicated budget has negatively impacted cyber risk mitigation efforts.

A key finding from the U.S. Department of Homeland Security's 2013 National Preparedness Report concluded that states continue to have low overall awareness of risks to their information systems and low confidence in their ability to protect them against cyber threats.⁴ State CISOs view a lack of funding and skilled staff as top barriers to improving cybersecurity capabilities.⁵ This nationwide review coincides with our own findings about bolstering efforts to build a stronger cyber workforce within the District government.

Several District agencies expressed that the lack of manpower and a dedicated budget are both major limitations to protecting against cyber threats. Several District agencies have very small cybersecurity operations with only a handful of personnel who are trying to protect against threats. Other District agencies expressed the need for additional personnel to assist in revamping areas of particular risk within their systems and developing additional alerts in their security operations.

Costs to upgrade or implement solutions to combat new threats and vulnerabilities that require immediate resolution need to be determined and assessed against funding dedicated elsewhere in operational budgets. The ability to fund operational requirements is a major impediment that needs long-term budget support. Budget considerations have also limited agencies ability to implement processes capable of providing continuous network and security activity monitoring, thereby increasing the District's exposure to cyber risks.

While the Commission recognizes that the District, like all local governments, faces fiscal challenges, our sense is that the lack of funds committed to cybersecurity stems not from overall resource constraints but more from a lack of coordination and prioritization. The Directive suggested in Recommendation 1 discussed below would be an important step in underscoring the importance of cybersecurity in the context of annual budget-making.

⁴ US Department of Homeland Security National Preparedness Report, March 2013, pgs 24-25, available at: http://www.fema.gov/media-library-data/20130726-1916-25045-0015/npr2013_final.pdf, (accessed on September 25, 2013).

⁵ *Id* pgs 24.25.

Recommendations

Based on the findings from our review of the District agencies, the Commission has developed a list of recommendations outlined below that we believe will help to bolster protection against cyber attacks to the District of Columbia.

1. Issue a Cybersecurity Directive.

The leadership of the District of Columbia needs to recognize and elevate the importance of bolstering cybersecurity protection in the City by issuing an official directive. This Directive should:

- Establish the position of CISO for the District;
- Establish a governance structure⁶ capable of prioritizing and overseeing cyber risk mitigation efforts across the City and with key stakeholders outside of the City including the private sector and Federal government;
- Enumerate the roles and responsibilities of each District agency involved in cybersecurity protection;
- Establish an adjudication process to resolve any disputes or disagreements that may arise between District agencies responsible for managing cybersecurity preparedness and protection; and
- Create a taskforce or committee to complete a District-wide cybersecurity risk assessment.

The need for such a Directive cannot be overstated. The District is an urban area with great reliance on systems and functions that are vulnerable to cyber attacks including a complex overlay of federal and local government facilities and functions, as well as critical infrastructure under both public and private control.

⁶ The governance structure could be similar to the District's Statewide Interoperability Coordinator (SWIC). The District has appointed a SWIC to handle interoperable communications of voice, data, and video throughout the District. The SWIC's position also involves developing and delivering reports and briefings, coordinating interoperability and communications projects, assembling interoperability working groups to develop key recommendations and programmatic implementation, and building relationships with those involved in the District's interoperability efforts. District of Columbia Homeland Security and Emergency Management Agency, available at: <http://hsema.dc.gov/page/statewide-interoperabilty-coordinator-swic> (accessed on November 4, 2013).

2. Appoint a Chief Information Security Officer for the District.

The District of Columbia should appoint a senior executive level CISO. A recent report by the National Governor's Association highlighted the importance of CISOs encompassing greater authority and responsibility over statewide cyber networks in order to implement effective cybersecurity programs for their jurisdictions.⁷ The District's CISO should be charged with establishing and maintaining the District-wide strategy and program to ensure the protection of information management assets, and maintaining coordination with private sector CISO counterparts.

Statewide CISO positions in Maryland and Virginia, and the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) provide a framework and examples of functional responsibilities that might fall under an enterprise-level CISO. Those duties include, but are not limited to:

- Information Regulatory Compliance
- Information Security and Assurance
- Information Risk Management
- Cybersecurity
- Information Privacy
- Disaster Recovery and Business Continuity

In addition to the establishment of a District-wide CISO, the Commission also recommends that the currently vacant CISO position within OCTO be filled.

3. Develop a contingency plan for a potential scenario involving a catastrophic loss of electrical power to the District.

The District should develop a contingency plan for responding to a potential scenario in which, due to a cyber attack, the City experiences a catastrophic loss of electrical power for a period lasting a minimum of seven days.

Cyber attacks against electrical grid systems are increasing in frequency and sophistication, and the D.C. grid maintained and operated by Pepco is no exception. There are plausible cyber disruption scenarios in which the local grid could be disrupted for a period of time lasting longer than seven days. While these high-consequence scenarios are very unlikely to occur, and would result only from a cascading series of

⁷ Thomas MacLellan, Division Director Homeland Security and Public Safety Division, National Governors Association, Act and Adjust: A Call to Action for Governors for Cybersecurity, September 2013, page 2, available at:

http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf. (accessed on October 1, 2013).

unlikely events, their probability is not zero. Because the consequences of such a scenario to the District and to its population would be so severe, the Commission recommends that City develop a formal contingency plan for such an eventuality.

Pepco is taking a variety of leading steps to minimize the possibility of experiencing operationally disruptive cyber attacks and the company has a very strong cyber risk management program. However, perfect prevention of high-consequence attacks is not possible, even at great cost; therefore, the District needs to take steps to ensure its resilience in the case of such a scenario.

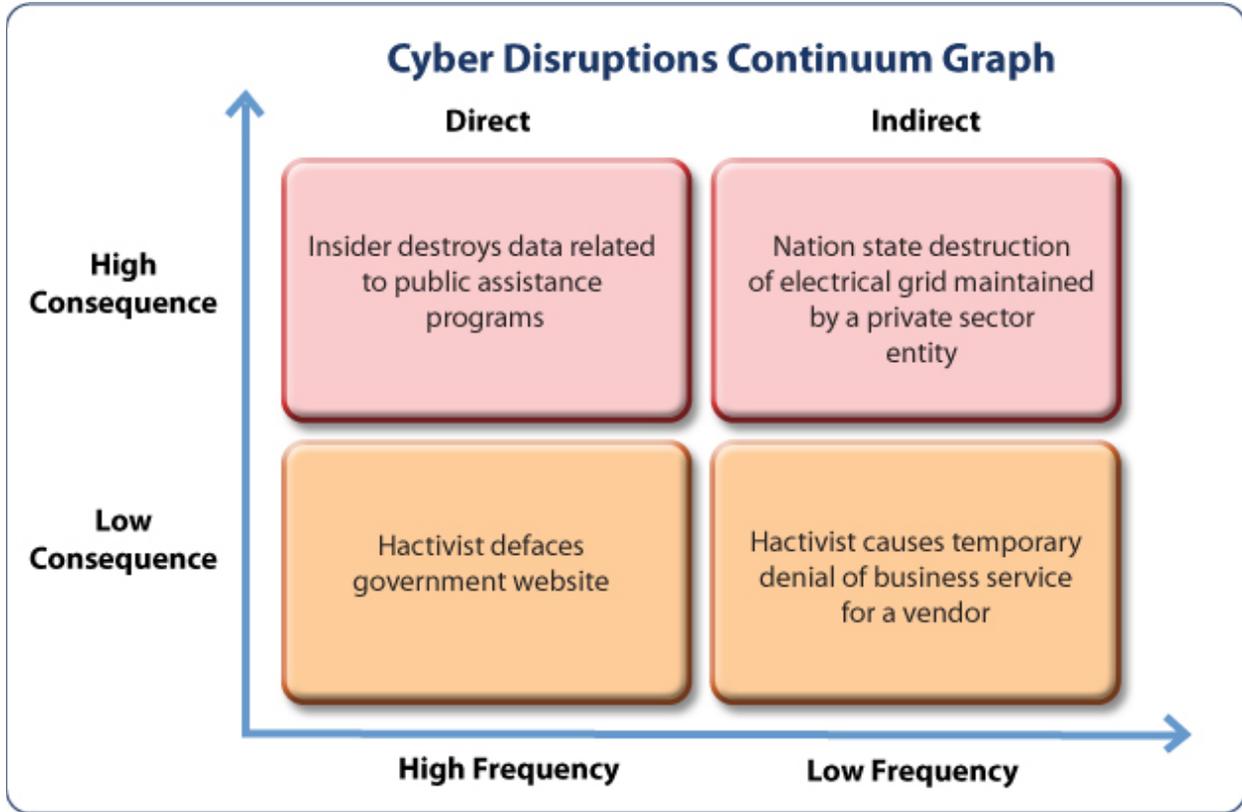
4. Establish a risk governance framework to analyze and identify risks.

The District of Columbia should establish and implement a risk governance framework to conduct risk assessments that identify and examine potential cyber risks to its systems and infrastructure as well as to prioritize actions and resources necessary to address those risks. The risk framework should acknowledge the interdependencies, relationships, and responsibilities between all District agencies involved in managing a cyber incident. The Commission recommends a five-step process outlined below.

Step 1: Identifying and Analyzing Risks:

This first step should involve identifying and recognizing known risks and vulnerabilities, similar to the current Hazard Identification Risk Assessment (HIRA) developed by District of Columbia Homeland Security and Emergency Management Agency (HSEMA) that analyzes human-caused as well as natural hazards impacting the District.

When conducting the risk assessment, it can be useful to consider that cyber (and other) disruptions exist on a continuum. The graph below outlines this continuum. Those disruptions characterized as “high frequency and low consequence” are at one end of the continuum; those characterized as “low frequency and high consequence” exist at the other. It is the higher consequence event with which we are most concerned. While an agency or jurisdiction should prepare for all types, the Commission is more concerned with higher consequence events that would have more widespread impact across multiple District agencies.



Step 2: Identify Functions Performed

The cyber HIRA should describe the function that each agency performs and the potential hazards that could impact those functions. Agencies need to identify the functions they perform in order to understand the relationships that agency has with other entities. For example, HSEMA performs public notification as just one of its functions. In order to fulfill that function, they must maintain connections to the media, the Mayor’s Office of Communications, as well as direct channels of communications with the public.

- Criteria for assessing cyber risks**
- Life threatening
 - Immediacy of the situation
 - Scale of the situation (local, regional, national significance)
 - Lack of a work around/redundancies
 - Impact on the mission of the District or Federal government
 - Potential threats to economy and commerce

Step 3: Develop Several Scenarios

In evaluating risks, it is often useful to use “*scenario based planning*” to ground the effort in real life incidents. In this case, several scenarios could be developed that have cyber ramifications in order to identify the various “*stressors*” that would be brought to bear on District of Columbia Government and its various organizational units. These stressors would be useful in identifying the risks faced by the District agencies and their systems and how those stressors will impact *essential functions*.

For example, a cyber attack on the City’s communications systems to the public would challenge what systems? Sub-systems? What dependencies would this tax? What interdependencies would this illuminate? These impacts on the agency would be related to how connected the agency was to the scenario ranging from physically connected to virtually connected.

Notably, as with other areas of significant persistent risk, in the cyber domain, it is often difficult to assign responsibility for managing risks due to differences in near-term or long-term points of view and the fact that critical infrastructure is owned or operated largely by private companies, whose primary responsibility is to remain profitable. In terms of addressing risks it is possible to categorize these risks against critical infrastructure in three ways:

Private Sector Management	Middle Ground	Government Management
Risks that may/may not threaten the viability of a business but pose no meaningful public threat	Risks that involve BOTH the private and public sectors, making it difficult to assign leadership for managing the risk	Risks that clearly pose a public/national threat for which governmental institutions play a large role

It is further possible to categorize these either risks as “direct” or “indirect” – as they relate to a given stakeholder. For example, the District of Columbia faces indirect risk from cyber attacks against the local electric grid, because it is entirely reliant upon Pepco to manage these risks directly. In contrast, the difficulties the Office of the Chief Technology Officer faces resulting from attempted hacks on its computer systems would be a direct risk from a District perspective.

Given the continuum of cyber risks facing the District of Columbia, some should clearly be managed by OCTO – for example, insider attacks against the District’s education services. Private critical infrastructure owners/operators should clearly have a role in managing other risks – *e.g.*, insider cyber attacks against the local electrical grid.

Step 4: Evaluate the Impact on Functions

Threats emanating from the cyber domain can create significant and persistent risks that cascade across some or all of the other critical infrastructure sectors. This, in turn, can have a dramatic impact upon the functions of the government, impeding its ability to provide necessary services as well as to facilitate normal public, private, and commercial activities.

Techniques for Managing Risk

- *Avoidance* (eliminate by withdrawing from or not becoming involved with a risk)
- *Reduction* (minimize by changing processes or increasing diversity of supply, etc.)
- *Sharing* (transfer by outsourcing or insuring against the risk)
- *Retention* (accept by budgeting for appropriately)

District agencies should evaluate the impact to functions by assessing the agency’s ability to bring *capabilities* to bear to mitigate those impacts. If the cyber attack on the City’s communications had the impact of interrupting power to the system, but the City had backup power generation, then a determination might be made that the City could successfully address that threat.

In order to minimize the functional impacts of such events, the Commission recommends the CISO and appropriate authorities within each District agency work together to address those risks that, based on the above described analysis, are categorized either as ones the *government should clearly manage* or constitute the most critical ones that lie *in the middle ground*.

Step 5: Prioritize Actions

Finally, for those impacts that cannot be readily or satisfactorily mitigated, agencies will need to prioritize actions to address that stressor. This involves determining the capability that is needed and how the agency will go about obtaining that capability.

District agencies can apply the five-step process described above to understand the nature of the cyber threats they face, identify agency functions, develop scenarios

impacting those functions, evaluate potential capability shortfalls, and prioritize action steps to help to mitigate the risk.

Appendices

Appendix A: Commission and Stakeholder Meetings

The Commission is required to meet on a quarterly basis throughout the year to discuss, and evaluate the status of homeland security within the District. The Commission also met with a select group of District agencies and private sector stakeholders to examine their efforts in bolstering cybersecurity protections for the District. The following table outlines the dates and times of each Commission meeting and stakeholder briefing that was held during this year.

Meeting/Briefing	Date
Commission Meeting	February 8
Commission Meeting	April 17
Office of the Chief Technology Officer Briefing	April 17
OCTO Briefing	June 4
District of Columbia National Guard Briefing	June 11
Washington Metropolitan Area Transit Authority Briefing	June 26
Commission Meeting	July 31
District of Columbia Water and Sewer Authority Briefing	September 10
Commission Meeting	October 30
Metropolitan Police Department Briefing	October 31
Pepco Briefing	November 12

Appendix B: Agency Findings

Office of the Chief Technology Officer (OCTO)

OCTO is the central technology organization of the District of Columbia Government. OCTO develops, implements, and maintains the District's technology infrastructure and major enterprise applications; establishes and oversees technology policies and standards; provides technology services and support for District agencies; and develops technology solutions to improve services in all areas of District Government.

OCTO's cybersecurity practice is well known throughout the District of Columbia Government to be a combined effort of the Citywide Information Technology Security (CWITS) team; the new OCTO Cyber Security Operations and Command Center; and the Network Operations Center. The success of the cybersecurity program can be measured by: the availability of the District of Columbia's resources on the Internet to the public; maintaining data integrity; ensuring a secure internal computing environment; and ensuring the number of related cybersecurity incidents are detected, prevented, and remediated over a period of time.

Through the District's performance management program, OCTO has provided key performance metrics that support availability and up time of Internet resources and reduced unsuccessful malicious attacks targeted towards the District of Columbia's public-facing infrastructure technology applications. OCTO's infrastructure support groups work cohesively to detect and remediate incidents related to cyber exploits and viruses and minimize risk to business operations.

OCTO has reduced exposure to system and application risks through an efficient vulnerability assessment program with periodic assessments of its security capabilities. The vulnerability assessment program assesses security risks for end point systems, applications, and file servers.

Despite these successes, the practice of IT security remains a constant one, with continuous improvement taking place, along with additional plans for workforce awareness and alerts that are a part of the Security Operations plan. Quarterly assessments routinely reveal the presence of known system level vulnerabilities, which are reported to application and business owners. The failure to remediate vulnerabilities is due to the existence of legacy applications that cannot be upgraded as well as systems that have reached end-of-life support environments and both of these issues pose a significant risk to the enterprise. Security audits conducted by independent industry experts have revealed that the lack of an effective strategy to

build an efficient information security program incorporating all critical functions of a mature security framework is also an impediment in OCTO's long-term mission.⁸

In addition, a small cyber workforce has also impacted operations of OCTO's CWITS department. Currently the CWITS department has only 11 members consisting of a mix of District of Columbia employees and contractors. The ability to identify, hire and retain personnel needed to maintain and enhance the security environment across all information technology domains is a significant challenge because of competition from the Federal government and the private sector in hiring and retaining qualified personnel.

In the long-term, OCTO plans to establish multiple Security Operations and Command Centers (SOC) that will provide continuous monitoring of information technology events for the District of Columbia. Advancing threats are always considered to be major risks that need to be detected and controlled before they present a major threat to the security of the District government's information management systems. Currently CWITS personnel must continually assess the threat landscape as part of their operational function.

The establishment of multiple SOCs will alleviate that operational responsibility away from CWITS's core security functions. The SOC will also serve as a central location for collection and information sharing, and management and coordination of the District of Columbia's response to cyber threats and incidents. OCTO is currently working with external vendors to identify solutions for both staffing and building the necessary skill sets desired for the SOC.

CWITS provides enterprise-wide, managed and on-demand information security services for all District Government agencies and public partners who conduct daily business activities with the District Government. The primary objectives of CWITS are: ensure that the District of Columbia's IT assets, resources, organizational and personal data are secure by establishing and enforcing information security policies and procedures and work with District agencies and its vendors in this process.

⁸ The Commission requested a copy of these audits for further review but OCTO failed to provide the documents to the Commission.

In addition, OCTO plans to develop and maintain a strategic risk assessment program to measure agency and District of Columbia's compliance to information security policies and procedures, as well as other federal guidelines and regulations. OCTO is currently working on identifying solutions and engaging vendors in assessing toolsets to conduct assessments under the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FIMSA) compliance mandates.

OCTO is also preparing to focus on an enterprise awareness program for the District of Columbia workforce on information and cybersecurity in FY 2014. Finally, OCTO will continue development and implementation of a strong security infrastructure to detect, prevent, and remediate against existing and future unknown vulnerabilities and threats as well as implement cyber awareness programs to train and educate the workforce against evolving cyber threats.

Metropolitan Police Department (MPD)

The MPD is the primary law enforcement agency for the District of Columbia and has over 4,000 sworn and civilian members serving the District. It is the mission of the Metropolitan Police Department to safeguard the District of Columbia and protect its residents and visitors by providing the highest quality of police service with integrity, compassion, and a commitment to innovation that integrates people, technology and progressive business systems.

Potential cyber threats impacting MPD are jointly managed by MPD and the OCTO. If a cyber threat were to impact one of MPD's databases, both agencies would conduct a review of the incident, analyze where the breach occurred, and determine the best protective measures for the future.

In addition, MPD is concerned about the degree of coordination among District agencies to counter a potential cyber threat due to incidents in the past over the proper communication protocols and oversight of cybersecurity attacks impacting the District. MPD would like to see greater coordination and communication between District agencies to address cyber incidents impacting the District in the future.

Several District agencies, including MPD, are expected to house their primary technology operations, also known as data centers, in one location. MPD would like to have further discussions with District agencies and senior leadership regarding the location of the data centers to ensure this location adequately meets industry standards.

In the long term, MPD plans on increasing efforts to train staff and new cadets on cyber crimes and this will require a great deal of time and investment since this is a very specific

and technical area. MPD will continue increasing cybersecurity awareness and training for its staff in the future.

District of Columbia Water and Sewer Authority (DC Water)

DC Water is a multi-jurisdictional regional utility that provides distribution of treated drinking water to more than 600,000 residential, commercial, and governmental customers in the District of Columbia, and wastewater services to more than two million people in the National Capital Region. To distribute water and support the distribution system, DC Water operates more than 1,350 miles of pipes, four pumping stations, five reservoirs, three elevated water storage tanks, 37,100 valves and 9,340 public hydrants. To collect wastewater, DC Water operates 1,800 miles of sanitary and combined sewers, 22 flow-metering stations, nine off-site wastewater pumping stations, and 16 storm water pumping stations. Separate sanitary and storm sewers serve approximately two-thirds of the District of Columbia. In older portions of the system, such as the District's downtown area, combined sanitary and storm sewer systems are prevalent.

The focus of cybersecurity within the water distribution, wastewater collection and wastewater treatment systems, lies primarily in the potential for contamination and environmental impact as a result of a targeted cyber attack. For example, if an adversary were able to corrupt the control system for the water distribution system, the related water pressure, fire-flow capacity and water quality could become compromised. Wastewater collection is another area of concern, where a compromise to the control and pumping system may increase the potential for sewage overflow into the Potomac or Anacostia rivers or backup into customers' homes. A final area of concern is within the wastewater treatment process located at the Blue Plains plant. A compromise of this control system may lead to the environmental damage of the Potomac River. Each control system has a manual mitigation plan.

DC Water has two separate Supervisory Control and Data Acquisition (SCADA) systems: one for the Blue Plains Advanced Wastewater Treatment Plant and a second for water distribution and wastewater management. There is 24-7 monitoring by trained operators and hard overrides at the pumping stations. DC Water has specially configured encrypted laptops for configuring the system and maintains a white list of approved applications. SCADA networks are physically separated from the larger administrative network as an added level of security.

DC Water continuously monitors its SCADA environment with an eye toward risk mitigation. DC Water operates its own network and is not tied into OCTO's DC-NET,

which is a fiber optic-based metropolitan area network that provides high-speed transport of data, voice, video, and wireless telecommunications services for District agencies. DC Water is evaluating the benefits of joining DC-NET, which include access to long-range threat profiles of its systems from OCTO. Finally, DC Water would like to have a presence in the Security Operations and Command Center at OCTO.

Washington Metropolitan Area Transit Authority (WMATA)

WMATA is a tri-jurisdictional government agency that operates transit service in the Washington Metropolitan Area. WMATA operates the second largest heavy rail transit system, and the sixth largest bus network in the United States. In 2012, WMATA ridership included over 200 million people on its rail service and over 100 million on its bus service. In addition to ongoing operations, WMATA participates in regional transportation planning and is developing future expansions of its system. These projects include an extension of Metrorail to Dulles Airport and light rail in suburban Maryland.

From a transit sector perspective, WMATA is one of the most capable cybersecurity programs in the country since it has a large basket of tools at its disposal, ample leadership support, and has a strong strategic and tactical planning mindset. WMATA would like to focus on improving operations in relation to measuring and evaluating cybersecurity products and services. WMATA will be deploying or enhancing multiple cyber products and services from a cybersecurity standpoint in the FY 14 including: CERT-resiliency management model (RMM),⁹ authentication & authorization identity management, network access control, critical infrastructure secure architecture, secure application development, and data governance liability. The CERT-RMM is a capability model for managing and improving operational resilience developed by the Carnegie Mellon University and the usage of this model is in its infancy.

One of WMATA's top FY 14 projects is to establish a CERT-RMM roadmap that has near term goals of mapping business unit capabilities into defined communities of interest, conduct employee training in CERT-RMM, and conduct a self-assessment to identify levels of process maturity for each goal area. This project is expected to take two years for development and training of its initial assessment.

In addition, WMATA would like to see more integration between emergency management and the cyber community to prevent stovepipe communications and increase situational awareness during emergency events. WMATA would like to be

⁹ CERT is a registered trademark owned by Carnegie Mellon University, available at: http://www.cert.org/csirts/cert_authorized.html (accessed on October 24, 2013).

involved in future cyber exercises such as analyzing the role of voice communications within the region and also conduct a dependency analysis on those services from a cyber standpoint.

District of Columbia National Guard (DCNG)

The DCNG trains primarily for two types of missions: wartime and domestic. In its role as a domestic operations responder, the DCNG brings extensive training to the aid of the local community and its mission partners. The DCNG's operational methodologies extend to the cyber realm as well. The Joint Operations Center (JOC) is manned with leaders who are familiar with the capabilities possessed by the DCNG and can direct them to address a physical, cyber, or complex emergency environment potentially impacting the District.

The DCNG Computer Network Defense Team (CND-T) is well versed in both the Department of Defense and civilian computing environment standards. The DCNG is also thoroughly versed in the multitude of federal and state information security regulations that civilian agencies must maintain under compliance standards. This broad knowledge enables the DCNG to integrate into many incident response situations by providing additional support during potential threats or disasters.

The DCNG's current cyber program is still in its infancy and is in the process of being fully implemented, but the program has the equipment, capability, and capacity to monitor network traffic and provide situational awareness to its clients. The DCNG cyber capability is comprised of two specific teams: the Computer Network Defense Team (CND-T) and the Air force National Guard Joint Force Headquarters-DC (ANG JFHQ-DC) team. The DCNG supports a Joint Incident Site Communications Capability (JISCC) that allows for emergency communications to be deployed to an incident site on notice. The size of these units can easily encompass up to 30 or more individuals all performing cybersecurity specific functions during events such as the Presidential Inauguration.

In the long term, DCNG's strategic priorities include identifying possible gaps in technology, operations, and coordination as well as producing a training plan for FY14. DCNG capabilities are not very well integrated or coordinated with District agencies and consequently the DCNG wants to build stronger relationships with District agencies in order to focus more training towards essential tasks and skills needed for addressing emergencies and potential cyber incidents. The DCNG's would also like to provide assistance to the District during potential cyber threats or attacks in order to help the

City defend its networks and provide enhanced situational awareness for all partners responding to a cyber incident.

Pepco

Pepco is a subsidiary of Pepco Holding Inc. (PHI) and it is headquartered in the District of Columbia with a service territory of approximately 640 square miles, of which 65 square miles are in the District.

Pepco has taken a heterogeneous approach on cybersecurity to protect its electric system. Pepco's cybersecurity plan uses a "defense in depth" strategy and this strategy addresses prevention, detection, response and recovery. Some examples of these defenses include: cryptography and encryption; device authentication controls; tamper alerts; periodic penetration testing; intruder detection functionality; and a number of other protective mechanisms. Pepco also backups customer data to secondary location and plans for tertiary locations.

For network security, Pepco limits access so that employees only have access to the information and systems required to perform their role. It also has a complex network design and the Company has multiple networks that are segmented by multiple defense mechanisms—part of its defense in depth strategy. A network monitoring group is still in the process of implementation, but the Company has in place a middle network of individuals from the Emergency Management, Information Technology, and other departments that can relay information between various parties.

In addition, Pepco has created a cyber incident support team (IST) and it has been integrated into Pepco Holding Inc. (PHI's) Incident Command Structure (ICS) to manage emergency incidents. The Pepco IST typically convenes at its District headquarters building, but regional incident management teams are activated at command centers at their regional operating centers. The crisis information strategy team within their incident support team sets the strategy for media communications. For local stakeholders, the crisis information strategy team distributes timely and accurate information which includes media updates, conversations with government officials, and any social media information.

PJM is a regional transmission organization (RTO) that coordinates the movement of wholesale electricity in all or parts of 13 states and the District of Columbia. Pepco recognizes that in certain emergencies, portable generation for our customers may be needed. Although most customers make arrangements for backup power based on their

own needs, Pepco has assisted in certain situations but notes that deployment can take up to 72 hours, especially for locations that have not been prepared in advance. Pepco has access to spare transformers not only through its inventory, but through an industry wide program in the event of physical damage to a transformer. Pepco substations are designed with redundancy, so if a large substation transformer goes out of service, the substation will continue to provide service to all customers served by this station.

Over the long term, Pepco would like to continue engaging in external outreach with outside parties. The company works with industry working groups, state and local governments, and have met with the members from the national intelligence community to expand outreach efforts. Due to previous issues in the past regarding inadequate communications between Pepco and the District of Columbia Homeland Security and Emergency Management Agency (HSEMA) about prioritizing critical facilities restoration, there are now established communication policies between HSEMA's Executive Director and Pepco regarding the prioritization of facilities that should be up and running after a power outage. A formal list of District infrastructure and facilities has been developed that prioritizes which facilities require restoration if there is a power outage issue. Through its established Incident Command Structure (ICS), the Pepco representative in HSEMA's Emergency Operations Center (EOC) has a dedicated contact at Pepco's EOC during events in order to address issues associated with restoration priorities.

In addition, Pepco would like communication companies such as Verizon & Comcast to take more responsibility over complaints regarding downed wires during power outages. Pepco must respond to all customer complaints regarding wires on the ground- even if the wires are communications wires (not power lines) and are not Pepco's property, which impacts its efficiency and resources in restoring service. Pepco would like to see Verizon and Comcast become more involved in the restoration effort to better manage the wires that are downed during storms and events impacting the District.

Appendix C: Background information about the Commission

Mayor Vincent Gray officially appointed Commission members on February 8, 2013. The District of Columbia Homeland Security and Emergency Management Agency and the Deputy Mayor of Public Safety and Justice jointly vetted Commission members. Each member's background and expertise is listed below.

J. Michael Barrett: Mr. Barrett is a seasoned professional in both counterterrorism and risk assessment. Mr. Barrett is the CEO of Diligent Innovations, Inc., a consulting firm that advises clients on policy development, strategy, and business plan execution in the areas of defense and national security. He has served on the White House Security Council as the Senior Analyst for the Joint Chiefs of Staff and as a U.S. Navy Intelligence Officer for the Office of the Assistant Secretary of Defense.

Barbara Childs-Pair: Ms. Childs-Pair is an expert on security and transportation and has over three decades of experience in emergency management and homeland security, including as Director of HSEMA's predecessor agency, the District of Columbia Emergency Management Agency. She currently serves in the Office of Emergency Management for the Washington Metropolitan Area Transit Authority.

John M. Contestabile: Mr. Contestabile's expertise includes over thirty years of experience in the transportation sector addressing such areas as homeland security/emergency management, COOP, critical infrastructure protection and interoperable communications. Mr. Contestabile worked for the Maryland Department of Transportation in various senior-level positions coordinating with all the modal agencies in the Department [highway, transit, airport, maritime/port]. Mr. Contestabile now works at the Johns Hopkins University/Applied Physics Lab where he is working on projects with the Department of Homeland Security Science and Technology Directorate as well as the National Capital Region [NCR]. His NCR work is grant funded and is focused on developing a regional interoperable video-sharing program among transportation agencies, emergency operations centers, and fusion centers.

Andrew Cutts: Mr. Cutts serves as the Vice President for Critical Infrastructure Protection Programs for the Norwich University Applied Research Institutes. He is an expert in cyber security and is working to create a risk management tool that will allow financial institutions to determine their risk in various cyber disruption scenarios. Mr. Cutts also works to ensure that all homeland security planning includes seamless continuity of operations for technology systems.

Darrell Darnell: Mr. Darnell's expertise is risk assessment. Currently, Mr. Darnell is Senior Associate Vice President for Safety and Security at the George Washington University, where he directs the University's Police Department, Emergency Management personnel, and the Office of Health and Security. A retired Master Sergeant with the United States Air Force, Mr. Darnell has nearly a decade of experience at the U.S. Departments of Homeland Security and Justice. Before moving to the White House, he served as director of the District of Columbia Homeland Security and Emergency Management Agency, the Agency responsible for all-hazards emergency planning, preparation, response, and recovery for the District.

Glenn S. Gerstell: Mr. Gerstell is the managing partner of the Washington, D.C. office of Milbank, Tweed, Hadley & McCloy LLP, an international law firm headquartered in New York. By appointment of President Obama, Mr. Gerstell serves as a member of the National Infrastructure Advisory Council (NIAC), which is composed of 30 presidential appointees and advises the President and U.S. Department of Homeland Security on the strengths and weaknesses of the nation's infrastructure and its ability to withstand a terrorist attack or other national security threat. Previously, Mr. Gerstell served for two terms, by appointment of the Mayor of the District of Columbia, as the Chairman of the Board of Directors of the District of Columbia Water and Sewer Authority.

Daniel Kaniewski: Dr. Kaniewski is the Mission Area Director for Resilience and Emergency Preparedness/Response at the Homeland Security Studies and Analysis Institute. He is also an adjunct assistant professor at Georgetown University where he teaches in the School of Foreign Service and serves on the advisory board of the graduate program in Emergency and Disaster Management. Previously, Dr. Kaniewski was Assistant Vice President for Homeland Security and Deputy Director of the Homeland Security Policy Institute at George Washington University. He also spent three years on the White House staff as Special Assistant to the President for Homeland Security and Senior Director for Response Policy.

Appendix D: List of References

- 1) The Homeland Security Risk, Reduction, and Preparedness Amendment of 2006, District of Columbia Code §7-2201.02 and §7-2201.03.
- 2) The White House, National Security Strategy, May 2010, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, (accessed on September 25, 2013).
- 3) US Department of Homeland Security National Preparedness Report, March 2013, pgs 24-25, available at: http://www.fema.gov/media-library-data/20130726-1916-25045-0015/npr2013_final.pdf, (accessed on September 25, 2013).
- 4) Presidential Policy Directive 21- Critical Infrastructure Security and Resilience, February 2013, available at: <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (accessed on September 25, 2013).
- 5) District of Columbia Water Annual Report 2012 available at: http://www.DistrictofColumbiawater.com/news/publications/DistrictofColumbiawater_2012_annual.pdf, (accessed on September 25, 2013).
- 6) National Institute of Standards and Technology National Initiative for Cyber Security Education framework, available at: <http://csrc.nist.gov/nice/framework/> (accessed on September 25, 2013).
- 7) District of Columbia Water All-Hazards Initial Response Action Plan, September 2010.
- 8) District of Columbia Water Incident Response Quick Reference Guide, March 2011.
- 9) Interview with Jonathan Reeves (Emergency Response and Planning Coordinator), Nelson Sims (Security Analyst), and Ravi Kammila (SCADA Manager), District of Columbia Water (September 10, 2013).
- 10) Interview with Cathy Lanier (Chief of Police), Peter Newsham (Assistant Chief of Police), and Barry Gersten (Chief Information Officer), Metropolitan Police Department (October 31, 2013).
- 11) Washington Metropolitan Area Transit Authority PowerPoint presentation, Cybersecurity and Emergency Management, June 26, 2013.
- 12) Washington Metropolitan Area Transit Authority Fact Sheet, available at: http://www.wmata.com/about_metro/docs/metrofacts.pdf (accessed on October 21, 2013).
- 13) Interview with Adam Meyer (Chief, Office of Information Technology Security/Chief Information Security Officer) (June 26, 2013).

- 14) Interview with Tina M. Kopilchack (Director of Military Support), John M. Isom (Deputy Director of Intelligence), and John Galeotos (contractor), District of Columbia National Guard (June 11, 2013).
- 15) Office of the Chief Technology Officer PowerPoint presentation, District of Columbia- NET (May 2, 2013).
- 16) Office of the Chief Technology Officer Information Citywide Information Technology Security Service Catalog, September 2012.
- 17) Interview with Tegene Baharu (Deputy Chief Technology Officer of Infrastructure Services) and George Geo (District of Columbia -Net Federal Account Manager), Office of the Chief Technology Officer (May 2, 2013).
- 18) District of Columbia Homeland Security and Emergency Management Agency (HSEMA), District of Columbia Hazard Vulnerability Assessment, 2012, pgs 48-49.
- 19) Potomac Electric Power, Fact Sheet on the District of Columbia, available at: http://www.pepco.com/_res/documents/PepcoDCFactSheet.pdf, (accessed on October 1, 2013).
- 20) Thomas MacLellan, Division Director Homeland Security and Public Safety Division, National Governors Association, Act and Adjust: A Call to Action for Governors for Cybersecurity, September 2013, available at: http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf (accessed on October 1, 2013).
- 21) District of Columbia Homeland Security and Emergency Management Agency, available at <http://hsema.dc.gov/page/statewide-interoperability-coordinator-swic> (accessed on November 4, 2013).
- 22) Interview with Doug Meyer (Vice President and Chief Information Officer), Pete Pedersen (Emergency Management Manager), Caryn Bacon (Director Emergency Preparedness and Business Continuity), Michael Kuberski (Chief Information Security Officer), and Peter Meier (Vice President Legal Services), Pepco Holdings, Inc. (November 12, 2013).
- 23) Carnegie Mellon University, available at: http://www.cert.org/csirts/cert_authorized.html (accessed on October 24, 2013).
- 24) Federal Emergency Management Agency, FY 2013 Homeland Security Grant Program, <http://www.fema.gov/fy-2013-homeland-security-grant-program-hsgp-0#3> (accessed on December 1, 2013).