



**District of Columbia**  
**Homeland Security Commission**  
**2013 Annual Report**

## Letter from the Homeland Security Commission

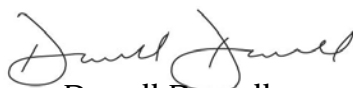
We are pleased to present the first District of Columbia Homeland Security Commission Annual Report.

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.

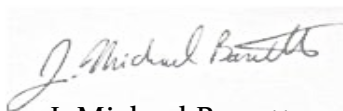
With such a broad statutory agenda confronting it, the Commission decided that it could most effectively contribute by focusing on a single topic, rather than undertaking a cursory overview of the many subjects within its purview. This report outlines our general findings on the state of cybersecurity 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.

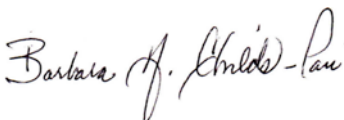
### The District of Columbia Homeland Security Commission



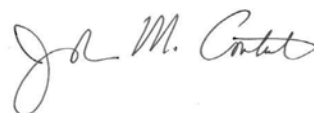
Darrell Darnell  
Chairman



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

Recommendations .....9

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 2006<sup>1</sup> 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.<sup>2</sup>

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

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

<sup>2</sup> 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.<sup>3</sup>

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.

---

<sup>3</sup> 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.**

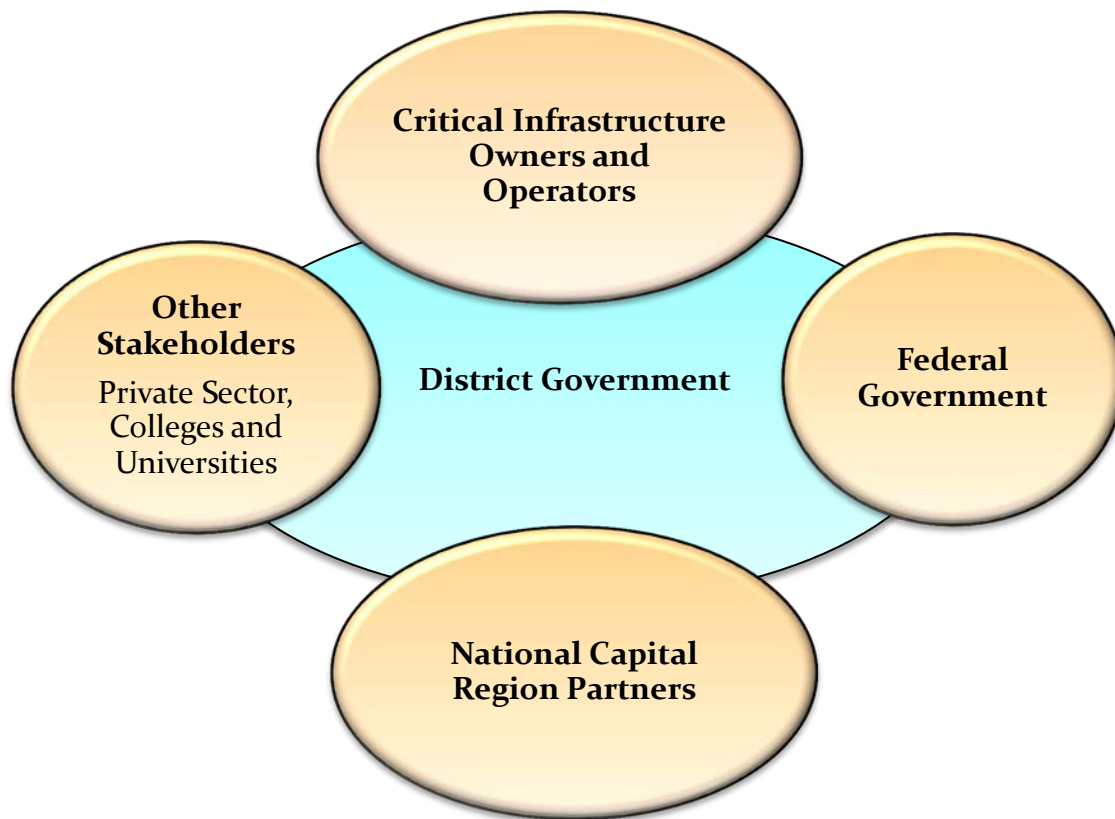
While much effort is being expended by hardworking and qualified personnel, the Commission found that there is a lack of communication between District agencies when trying to identify, manage, and address cyber threats. Several agency officials expressed to the Commission that they were unsure of either 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.<sup>4</sup> State CISOs view a lack of funding and skilled staff as top barriers to improving cybersecurity capabilities.<sup>5</sup> 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.

---

<sup>4</sup> 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](http://www.fema.gov/media-library-data/20130726-1916-25045-0015/npr2013_final.pdf), (accessed on September 25, 2013).

<sup>5</sup> *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 structure<sup>6</sup> 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.

---

<sup>6</sup> 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.<sup>7</sup> 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

<sup>7</sup> 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](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.

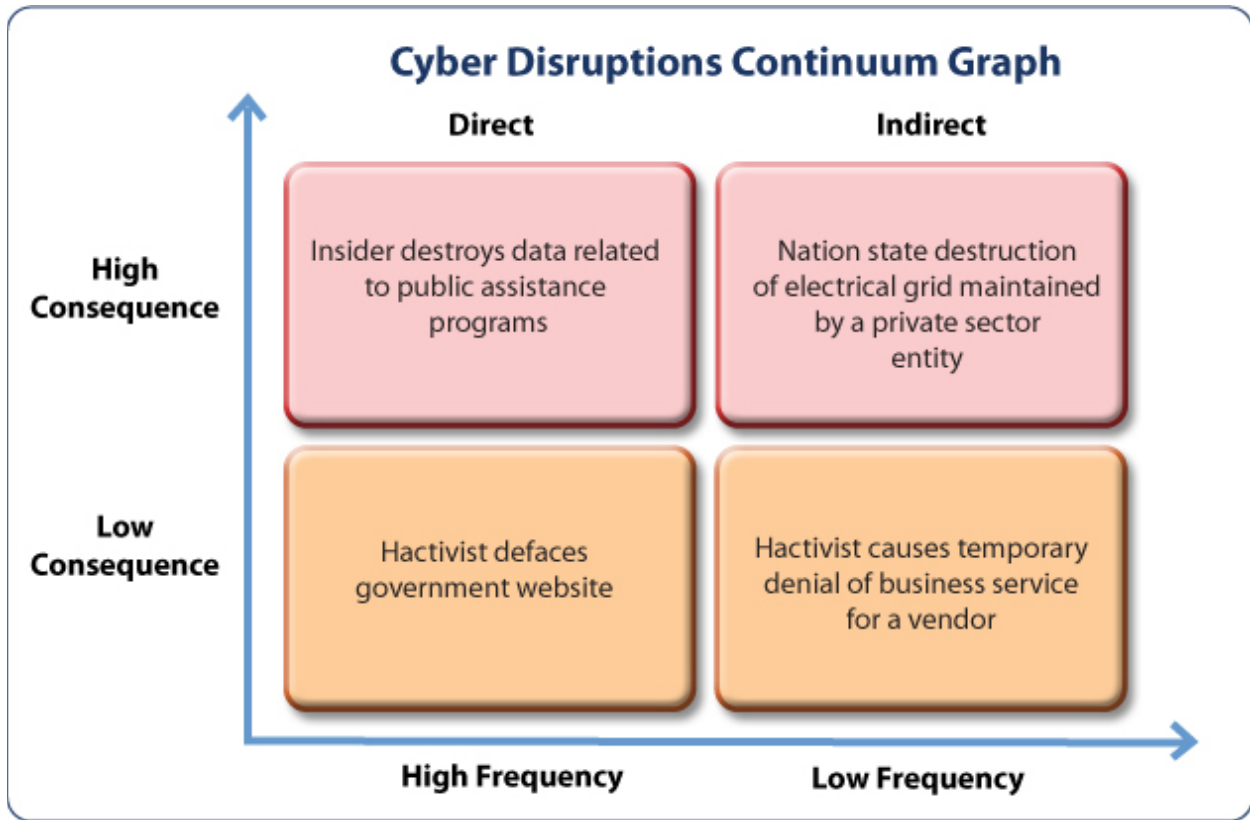
#### **4. Establish a risk governance framework to analyze and identify risks.**

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:

<b>Private Sector Management</b>	<b>Middle Ground</b>	<b>Government Management</b>
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.<sup>8</sup>

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.*

<sup>8</sup> 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),<sup>9</sup> 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

---

<sup>9</sup> CERT is a registered trademark owned by Carnegie Mellon University, available at: [http://www.cert.org/csirts/cert\\_authorized.html](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](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](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](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](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](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](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](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).