DC HOMELAND SECURITY COMMISSION 2018 ANNUAL REPORT

SAFEGUARDING CYBERSPACE IN THE NATION'S CAPITAL

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

About the Commission

The District of Columbia (District) Homeland Security Commission (HSC or Commission) was established by the Homeland Security, Risk Reduction and Preparedness Amendment Act of 2006. The HSC makes recommendations for improvements in security and preparedness in the District. Specifically, the Commission gathers and evaluates information on the status of homeland security in the District, measuring progress and gaps in homeland security preparedness, recommending security improvement priorities in consultation with major public and private entities and advising the District government on the homeland security program. Each year, the HSC provides an annual report to the Mayor and District of Columbia Council. Each member's background and expertise is listed below. For more information about the Commission, please visit the Commission's website at: https://hsema.dc.gov/page/homeland-security-commission.

♦

David F. Heyman (Chair): The Honorable David F. Heyman is a nationally recognized homeland security expert, thought leader, and former systems software engineer with nearly three decades of experience working globally at the intersection of technology, innovation, and national security. He has served in senior positions at the White House, the U.S. Department of Energy, and as the Assistant Secretary for Policy at the U.S. Department of Homeland Security (DHS), where he led the development of the nation's first congressionally-mandated national homeland security strategy. Previously, after 9/11, Mr. Heyman was Founding Director of the Homeland Security Program at the Center for Strategic and International Studies (CSIS) and an adjunct professor at Georgetown University's School of Foreign Service. Mr. Heyman started his career and worked for nearly a decade, as a computer systems software engineer and eventually head of international operations for a firm specializing in industrial automation, robotics, and supply-chain management. He is currently the CEO and founder of Smart City Works, a new class of business accelerator established to build and launch next generation IoT infrastructure companies that improve the security, resilience, and livability of cities.

Dr. Meloyde R. Batten-Mickens: Dr. Meloyde R. Batten-Mickens currently serves as the Director of Facilities Operations at Prince George's Community College. She has more than twenty years of progressive experience in planning emergency management programs including public safety, people management, communication strategies, and organizational leadership. She is a credentialed Certified Emergency Manager by the International Association of Emergency Managers and serves on the Federal Emergency Management Agency's National Advisory Council (FEMA-NAC) Integrated Public Alert and Warning System (IPAWS) Sub-Committee and previously served on the FEMA-NAC Preparedness and Protection Sub-Committee. Dr. Mickens was also the lead program director for public safety and emergency management at Gallaudet University and Simmons College, where she executed Emergency Management Accreditation Program (EMAP) standards and principles to develop and strengthen the institutions' emergency management councils, crisis leadership teams, public safety operations, and facility infrastructure. As a member of the Emergency Management Institute's Executive Academy, her cohort co-authored the article, "Development of Metrics for Personal Preparedness," to highlight the criticality of creating a metric mechanism to demonstrate if emergency preparedness initiatives are actually creating a prepared nation. Dr. Mickens' volunteers regularly with the local community and faith-based organizations, coordinating and providing disaster preparedness briefings. As a member of Delta Sigma Theta Sorority

Incorporated's National Emergency Response Task Force, she is an active participant on the White House-sponsored National Youth Preparedness and FEMA's America's Prepare-A-Thon national initiatives.

Brad Belzak: Mr. Brad Belzak is a national security executive with 16 years of U.S. Federal, state and local government and international business experience living and operating in over 70 countries. Currently, Mr. Belzak works for a global consulting firm advising Fortune 500 and public sector clients on insider threats, resiliency, and other risk management issues. Previously, he served as a Political appointee at DHS, as Senior Advisor within the Office of Intelligence and Analysis. Prior to that, he worked as a consultant supplying companies with homeland security and emergency management capacity building. While at Deloitte, he advised senior leaders in the Middle East on homeland security best practices. Prior to his time in the private sector, Mr. Belzak spent eight years working for the U.S. Government in both the Executive and Legislative branches. He was then at DHS as a Senior Policy Adviser to leadership, Deputy Chief of Staff and First Responder during Hurricane Katrina recovery operations and an Intelligence Analyst on detail to the Federal Bureau of Investigation. Mr. Belzak has a Masters of Science in Security and Resiliency from Northeastern University and a Bachelor of Arts in Political Science and International Relations from Elon University.

Philip McNamara: Mr. Philip McNamara is an accomplished Government Affairs, Advocacy and Political Executive. He has over eight years of experience with DHS as a part of the senior leadership team where he concluded his service as the Assistant Secretary for Intergovernmental Affairs / Partnerships & Engagement. At DHS, he served a major leadership role during the incident responses from the H1N1 pandemic, to the Deepwater Horizon oil spill, to Hurricanes Irene, Sandy and Matthew, to the Boston Marathon Bombing, and many others. As a team-oriented manager, Mr. McNamara coordinates with senior level officials to make timely decisions on complex issues. He specializes in relationship building and working with individuals of diverse perspectives to reach common ground. Phil is currently the director of government relations at The Pew Charitable Trusts. In this role, he oversees the work of government relations to assist in designing and executing strategies to fulfill the policy goals of many of Pew's projects. Mr. McNamara and the staff he manages work closely with program and operations units to build and sustain effective relationships with elected officials and policymakers at all levels of government that advance Pew's advocacy goals.

Acknowledgements

This report benefited from the assistance and guidance of the District of Columbia's Homeland Security and Emergency Preparedness Agency (HSEMA), and, in particular, Sarah Case-Herron, Jason Rubinstein, and Anthony Crispino. We thank them for their advice and support in running the Commission, its meetings, and for research and technical assistance in preparing this report. The Commission would also like to express our appreciation to HSEMA's Office of Public Affairs for assistance in formatting and preparing for publication the final report.

Additionally, the authors acknowledge the time and expertise provided by subject matter experts, government officials, and representatives from the private sector. In particular, Commissioners would like to thank the following individuals for their time and insights, in helping to level set current municipal practice in cybersecurity: Tony Sager and Thomas Duffy (Center for Internet Security); Suneel Cherukuri (DC's Office of the Chief Technology Officer); and Dr. Christopher Rodriguez (HSEMA).

The authors of this report would also like to thank former Commissioner Susan Reinertson for her dedicated service to the Commission and for her contributions to this report. Reinertson served two terms on the District of Columbia's Homeland Security Commission, completing her service in August 2018.

Lastly, in December 2018, the Commission welcomed new Commissioners Brian Baker, Edward Pearson, and Joanna Turner. Their terms will commence as the report goes to press.

NOTE: *The opinions expressed in this report are solely those of the Commissioners. None of the individuals or organizations listed in the Acknowledgements or in the Appendices have any responsibility for the content of the report, nor do they necessarily endorse its findings or recommendations.*

Table of Contents

Executive Summary

Over the past decade, societal pressures, to include rapid urbanization, failing infrastructures, climate change, and fiscal constraints, have placed significant demands on cities to provide services that can do more, save more, but cost less. As a result, municipalities across the globe, including the District of Columbia, have turned to the adoption of smart digital technologies, integrated sensors, controls, and cloud computing enhanced by data analytics to provide intelligence and automation that can make cities smarter, more efficient, sustainable, and resilient. Moving into the 21st century, building smart cities has become a strategic imperative and an operational necessity of municipalities across the nation.

However, the interconnectivity between the physical and digital worlds has also introduced new and substantial security risks. In recent years, we have witnessed cyberattacks on city systems and infrastructure increasing in frequency and scale. Threat actors now have the expertise and cyber tools necessary to take down government networks, damage critical infrastructure and services and shut down businesses and systems. For those infrastructures with critical interdependencies with other sectors—and for the electric grid in particular—such attacks can have cascading effects causing major economic and societal disruptions, affecting hundreds of thousands of people in cities, and costing hundreds of millions, if not billions of dollars in losses and remediation.

> Building smart cities has become a strategic imperative and operational necessity of municipalities in the 21st century; and digital life, indispensable to modern life.

The District has not been immune from such attacks, either. A ransomware attack in 2017 shut down approximately 70 percent of the Metropolitan Police Department's (MPD) surveillance cameras eight days before the presidential inauguration[1]. Further, in the Summer of 2018, multiple coordinated email phishing attacks from overseas and domestic sources targeted over 30,000 District employees.

While cyber threats are not unique to the District, the City possesses distinct characteristics as the seat of the federal government which may amplify the risk of cyberattacks. Specifically, the District is home to many of the world's largest multilateral organizations, such as the World Bank and International Monetary Fund, as well as to embassies and diplomats from nearly every country in the world. The implication is clear: with so many of our nation's assets potentially at risk, the District has a unique responsibility to maintain a cybersecurity posture that is best-in-class.

> Threat actors now have the expertise and cyber tools necessary to take down government networks, damage critical infrastructure and services, and shut down businesses and systems.

It is against this backdrop and because of the preeminent nature of the District as the nation's capital that District's Homeland Security Commission chose to review the District's cybersecurity posture as its 2017-18 Annual Report topic. Over the course of the past year, Commissioners interviewed security, information technology, policy, and infrastructure experts from across the District government and the private sector. The purpose of

[1] "Ransomware Shuts Down 70 Percent of Washington Surveillance Cameras", eWeek, February 2017. Available online at, http://www.eweek.com/security/ransomware-shuts-down-70-percent-of-washington-surveillance-cameras.

this study was to assess the District's cybersecurity posture, with an aim of making recommendations on how to improve District government policies, plans and procedures for safeguarding the jurisdiction against cyber threats.

To ensure consistent yet organic conversations, the Commission focused on the following key areas: Governance of Cybersecurity, Intelligence & Information Sharing; Preparedness and Incident Response, and Policy & Resources (*See* **Figure 1, Commission Study Areas**).

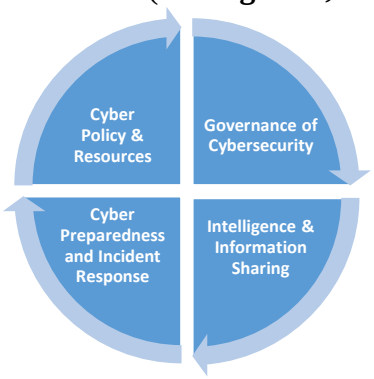

Figure 1 – Commission Study Areas

As an initial matter, the Commission gathered evidence of progress across the District government in establishing technical cybersecurity capabilities and associated security infrastructure, as well as in creating key leadership positions to protect the District's information technology networks against cyber threats. However, despite that progress, the principal finding of the Commission is that the District continues to lack well-established coordination and collaboration processes within the government and across the National Capital Region (NCR) to safeguard the District's cyberspace. In particular, the Commission finds that the District has yet to define clear roles, responsibilities, and associated authorities for its constituent agencies and positions responsible for cybersecurity. The Commission further identified significant opportunities for cybersecurity workforce development, improved intelligence and information-sharing, national capital regional coordination, and for improving coordination of public disclosure of cyber threats and attacks to the public.[2]

The principal finding of the Commission was that the District continues to lack well-established coordination and collaboration processes within the government and across the National Capital Region to safeguard the District's cyberspace.

Considering its findings, the Commission makes the following recommendations:

1. **Establish a Cyber Governance Structure**. Adopt a formal cyber governance structure with clear roles, responsibilities, and processes to enable continued progress and prevent future bureaucratic lapses.
2. **Empower the Chief Information Security Officer (CISO) and HSEMA**. Fully authorize OCTO and the CISO to develop, deploy and enforce, in partnership with HSEMA, and in coordination with other governmental entities, cyber policy and procedures across all entities under as the District's internet domain or system.

[2] *See* Appendix A, "Summary of Commission Findings" for a more detailed description.

3. **Institute Cyber Policy, Law, and Practice**. Institutionalize a standard practice for consideration of safeguarding cyberspace in development of new policy, law, regulation, programs, or procurement actions.
4. **Establish a Cybersecurity Center in the District's Fusion Center**. In concert with OCTO, and in close coordination with that agency's Security Operation Center (SOC), HSEMA should establish a cybersecurity fusion capability under the NCR Threat Intelligence Consortium (NTIC) for cyber threat monitoring and information sharing.
5. **Ensure Public Cybersecurity Disclosures**. Develop and implement a policy and practice for public cybersecurity disclosures to notify the public of potential cyber risks, maintain public confidence and potentially protect against unforeseen additional consequences.
6. **Establish OCTO's SOC as a Regional Resource**. The SOC should serve as a hub for technical support to District government agencies and for collaboration with District partners.
7. **Develop Stafford Act for Cyber**. The District should advance the development and implementation of a framework and standard practice for ensuring that federal emergency and disaster relief can be provided to states or the District, when a state or the District's resources are inadequate or overwhelmed during a cyber incident or attack.
8. **Establish and Employ a Municipal Reference Model for Cyber**. The District may or may not retain one of the nation's best postures for cybersecurity, but there's no easy way today of knowing. There is no agreed upon municipal reference model; no mechanism for measuring status, progress, gaps, or trends.
9. **Prioritize Workforce Cyber competency**. To mitigate an ever-changing threat environment, the District should continue to prioritize recruiting and retaining best-in-class cybersecurity workforce and developing training programs for District government personnel.
10. **Stand-up a Task Force for Recommendations on Enhancing the District's Cybersecurity Investments, Budgets, and Resources**. District government officials interviewed for this study universally raised concerns regarding adequacy of budget resources for cybersecurity programs and activities.

In the end, the Commission came to a single most important conclusion: the District must timely advance a framework and corresponding programs for transforming its 20th century bureaucracy into a modern digital society – a *cyberdom*[3] – where residents and visitors can both rely on and enjoy a digitally secure city. If the District aggressively works to achieve this vision and to implement the recommendations of this report, we believe it will greatly improve not just municipal security for Washington, D.C., but given the District's stature as the nation's capital, our nation's security as well.

The District must timely advance a framework and corresponding programs for transforming its 20th century bureaucracy into a modern digital society where residents and visitors can both rely on and enjoy a digitally secure city.

[3] 'Cyberdom' refers to a jurisdiction – country, state, district, or territory – whereby business, governance, and daily life are enhanced by digital services and operations.

Purpose of Report

To review the cybersecurity posture of the District of Columbia with an aim of making recommendations on how to improve District government policies, plans and procedures for safeguarding the District against cyber threats.

Authorities

This report has been developed pursuant to the District of Columbia's Homeland Security, Risk Reduction, and Preparedness Amendment Act of 2006, which directs the District's Homeland Security Commission to report on an annual basis to the Mayor and Council on the work of the Commission and areas of the Homeland Security Program in need of improvement, and to make such report available to the public.[4]

Background

The role of information and communication technologies (ICT) in society has, over time, become more and more integrated into our daily lives. Digitalization of the physical world—the process of bringing aspects of business, of government, and of our home and social lives 'online' through internet-enabled devices and applications now offers new and exciting ways to improve how we live, work, and organize ourselves. It also, however, introduces significant vulnerabilities to potential cyberattacks.

Smarter Cities and the Internet of Things (IoT)

Over the past decade, societal pressures, including rapid urbanization, failing infrastructures, climate change, and fiscal constraints have placed significant demands on cities to provide services that can do more, save more, but cost less. As a result, municipalities across the globe have turned to the adoption of smart digital technologies—integrated sensors, controls, and cloud computing, enhanced by data analytics—to provide intelligence and automation to make cities smarter, more efficient, sustainable, and resilient. Building smart cities, thus, has become a strategic imperative and operational necessity of municipalities in the 21st century.

Not surprisingly, more and more aspects of our lives—from transportation to the electric grid to water systems, health services, education, commerce, and government services—have indeed gone digital. So much so, that today, most of what we do is mediated through, touches upon, or is supported by some cyber connection. This trend is increasing. The smart city market is expected to exceed $1.7 trillion over the next 20 years.[5]

[4] The Homeland Security Risk, Reduction, and Preparedness Amendment of 2006, District of Columbia Code §7-2201.02 and §7-2201.03.
[5] PricewaterHouseCoopers. *Smart Cities: Five Smart Steps to Cybersecurity*. Available at https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/smart-cities.html

Digital life, in effect, has become indispensable to modern life. The interconnectivity between the physical and digital worlds, however, has also introduced new and substantial security risks. With every device that comes online—phones, access points, routers, sensors, industrial controls, IoT devices, cars, traffic signals, robots, etc.—the associated infrastructure and data from the physical world becomes open to and vulnerable to cyberattacks.

As such, digitization has created both promise and peril to cities. On the one hand, the increased connectivity makes cities smarter, allows for reduced energy consumption, optimizes water usage, and creates more efficient transportation systems, among other benefits. It also enables healthier living environments and enhanced public safety as well as improvements to myriad other government or community services.

On the other hand, digital connectivity is a two-way street: it simultaneously brings new capabilities online, but also opens the door for malicious actors to exploit and threaten critical infrastructure and vital services. Connectivity enables criminals and others to steal or ransom sensitive data and/or hack and harm key public and private sector operations through malware, data manipulation, denial of service, and other forms of cyberattacks.

The Cyberattack Landscape

Today, we see quite clearly that cyber risk is no longer theoretical. Cyberattacks on city systems and infrastructure have been increasing yearly in frequency and scale. We have witnessed just in the past three years that threat actors now have the expertise and tools necessary to take down government networks, damage critical infrastructure and services, shut down businesses and systems, and cause significant outages, delays, and destruction, affecting hundreds of thousands of people in cities, and costing billions of dollars.[6]

In 2018 alone, state and local governments across the United States reported a significant uptick in cyberattacks. For example, the Colorado Department of Transportation suffered a ransomware attack in February on back-office systems that cost nearly $1.5 million to recover. Also in February, Allentown, Pennsylvania experienced a malware attack on its finance and police departments, costing an estimated $1 million to recover. In March, online services for the city of Atlanta were disrupted for days after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. The city had to spend approximately $2.6 million to recover from the attack. Also in March, Baltimore's 911 dispatch system was taken down for 17

[6] See for example: Ukraine power grid, where attackers compromised 30 **power substations**, leaving 230,000 people without electricity (December 2015); attackers changed the levels of chemicals used to treat water at an unnamed **water treatment** facility, and compromised data of 2.5 million utility customers (March 2016); a distributed-denial-of-service (DDoS) attack on Sweden's **transportation systems** shut down and delayed trains, affecting thousands of passengers (October 2017); North Korean hackers were found to have targeted US electric companies in a spear-phishing campaign meant to probe utilities' defenses (October 2017); a ransomware attack deleted 30 million files from Sacramento's regional **transit system** (November 2017); and Schneider Electric Company was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. (December 2017). For additional information, see Center for Strategic and International Studies. *Significant Cyber Incidents Since 2006*. Available at https://csis-prod.s3.amazonaws.com/s3fs-public/181101_Significant_Cyber_Events_List.pdf?hsZtm10X2Ery9_CD.a2FYbE6ti..tQuu .

hours after a ransomware attack, forcing the city to revert to manual dispatching of emergency services.

The District's Experience

Similarly, the District of Columbia has also been victim to cyberattacks and attempts. In January 2017, for example, just days before the Presidential inauguration, a ransomware attack shut down 70 percent of the Metropolitan Police Department's (MPD) surveillance cameras. From January 12 to January 15, 2017, 123 of the 187 cameras of the department's closed-circuit TV cameras were unable to record. It took the District government four days to fully restore all the cameras and ensure there was no effect on the security plan for the 2017 Presidential Inauguration, which was designated by the U.S. Department of Homeland Security (DHS) as a National Special Security Event.

More recently, in July 2018, the District government received multiple and perhaps coordinated email phishing attacks from overseas and domestic sources, which were sent to over 30,000 employees across the District government. Officials reported no evidence of information being compromised as a result of the attacks and they were successfully defended against.[7]

Washington D.C. Uniquely at Risk

While cyber threats are not unique to the District, the jurisdiction possesses distinct characteristics that may amplify cyber risk to the city.

First, as the seat of the federal government, the District is the home of cabinet secretaries, members of Congress, the Supreme Court, and associated senior officials and employees. These characteristics may make the District and its infrastructure a more attractive target for malicious actors and enemies of the United States, while also potentially amplifying the disruptive impact of an attack. One merely needs to consider the impact of past non-cyber disruptions across the District to understand this phenomenon; such as, when snowstorms and hurricanes have caused the federal government to shut down when roads become impassible.

Second, the District is home to many of the world's largest multilateral organizations, as well as embassies from nearly every country in the world. As such, attacks on the region's infrastructure could have a ripple effect internationally, garnering greater attention and a larger audience than most other U.S. cities.

Third, the District, as the nation's capital and home of international organizations and diplomats, is also one of the most-visited cities in the U.S. by international visitors. What makes this relevant to cyber is that when people visit the District, or even when they merely seek to learn about the District prior to traveling, they invariably access District government websites, servers, and Internet Technology (IT) infrastructure. This is true for even the simplest of activities, such as looking up how to get from the airport to downtown on the Metro. As such, the District's cyberspace is also amongst the world's most internationally traversed cyber terrain too.

[7] "D.C. government targeted by overseas hacking attempt; referred matter to feds", Washington Post. July 28, 2018. Available online at, https://www.washingtonpost.com/local/dc-politics/dc-government-targeted-by-overseas-hacking-attempt-referred-matter-to-feds/2018/07/28/0246948e-91eb-11e8-8322-b5482bf5e0f5_story.html?utm_term=.12fb08fe6e76 .

"…with much potentially at risk, the District has a unique responsibility to maintain a cybersecurity posture that is best-in-class."

The implication here is clear: with much potentially at risk, the District has a unique responsibility to maintain a cybersecurity posture that is best-in-class.

It is against this backdrop and because of the preeminent nature of the District as the nation's capital, that Commissioners chose to review the District of Columbia's cybersecurity posture for its 2017-18 annual report. Cybersecurity is no doubt among the highest, if not, the highest, homeland security risk to the District, its residents, businesses and visitors. This report, thus, provides a review of the District's cybersecurity posture and makes recommendations regarding policies, plans and procedures to help safeguard the District against cyber threats today and in the future.

METHODOLOGY

Over the course of the past year, the Commission reviewed various aspects of the District's cybersecurity landscape. Key areas included:

- How the government organizes itself to protect government data, infrastructure, and services;
- How information and intelligence is shared across the District;
- The relationships among entities responsible for identifying and mitigating threats;
- Preparedness, incident response, and recovery from cyberattacks; and
- Policies and resources associated with the cybersecurity mission.

The Commission's review was limited in scope. The review was not a technical audit, but rather, was policy focused, examining three principal lines of inquiry.

First, the Commission reviewed the previous 2013 Commission study and assessed the District's progress toward implementing those recommendations.

Second, the Commission sought to establish a baseline for assessing the District's cybersecurity posture vis-a-vis cyber best practices and recommendations. The Multi-State Information Sharing and Analysis Center (MS-ISAC)[8] has a mission to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery. Given the District's membership in the MS-ISAC, the Commission engaged the MS-ISAC as a reference point in understanding and reviewing how the District might measure up to current standards and best practices.

Third, the Commission interviewed key staff from several of the District's agencies, departments, and key private sector partners responsible for cybersecurity, critical infrastructure, and emergency preparedness and response. It's worth noting that not all government entities are subject to the administrative authority of the Mayor. The Commission made every effort to interview representatives from both government entities subject to the administrative authority of the Mayor (e.g., the District of Columbia Office of Unified Communications, the District of Columbia Homeland Security and Emergency Management Agency, the Office of the Chief

[8] For details, see Center for Internet Security, Multi-State Information Sharing and Analysis Center. Available at: https://www.cisecurity.org/ms-isac/.

Technology Officer) as well as independent agencies and private sector partners outside of the Mayor's administrative authority, such as those responsible for the District's critical infrastructure or that the government relies on to deliver critical services or programs on behalf of the District of Columbia (e.g., the District of Columbia Board of Elections, Exelon Corporation, and DC Water).

For each interview, the Commission focused on several key questions, as follows:

- **Governance of Cybersecurity.** In general, from your perspective, who is in charge of the District's cybersecurity? What are the roles and responsibilities of the agency in charge? What are *your* organization's roles and responsibilities with respect to securing cyberspace in the District of Columbia? What is your organization's relationship with the organization in charge of cybersecurity? What do you believe to be the roles and responsibilities of other District agencies or departments in terms of *protecting* the District's cyberspace? What do you believe to be the roles and responsibilities of other District agencies or departments in terms of *responding to and recovering* from cyber threats and attacks?

- **Intelligence & Information Sharing.** In general, how do you and *your* organization stay current on cyber threats? How do you stay current on best practices and/or technologies for safeguarding cyberspace? In particular, who do you turn to for threat intelligence and for associated information on cyber threats? Who do you share your threat intelligence or information with? How do you make decisions with respect to communicating threat information or information on cyberattacks to the public?

- **Preparedness and Incident Response.** How do you and *your* organization prepare and train for responding to cyberattacks? What is or should be the role of HSEMA in preparing for and training for responding to cyberattacks? How do you know you and your organization are well-positioned to address current and emerging cyber threats?

- **Policy & Resources.** Do you and *your* organization have an adequate legal framework to accomplish the work you are responsible for with regard to safeguarding cyberspace? What additional authorities or policies could help better support efforts to safeguard cyberspace? Do you and your organization have adequate resources—technology or people—to appropriately safeguard IT infrastructure and accomplish the work you are responsible for with regard to safeguarding cyberspace? What additional policies or resources could help better support efforts to safeguard cyberspace?

In total, the Commission held 15 fact-finding meetings and/or discussions, including: 6 quarterly meetings and nine interviews from September 2017 through November 2018. See **Appendix C** for full list of Commission engagements and meetings.

Key Findings

SECTION 1: Previous Commission Report Implementation Progress

The table below summarizes the District's progress toward implementing each of the District of Columbia's 2013 Homeland Security Annual Report recommendations.

	2013 Commission Report GENERAL RECOMMENDATIONS	**Implemented as of October 2018**
1)	**Issue a Cybersecurity Directive:** • Establish CISO for entire District • Create governance structure to oversee cyber risk with key internal and external stakeholders. • Enumerate cybersecurity roles/responsibilities of each agency. • Establish cybersecurity adjudication process for city-wide disagreements over how to protect networks. • Create DC taskforce to perform cybersecurity risk assessment.	• Issued "Mayor's Order 2017-115" designating creation of: ✓ Chief Data Officer (CDO) ✓ Data Policy ✓ Chief Information Security Officer (CISO) ✓ Established committees of agency information security officers and of agency data officers to support CISO and CDO in efforts to protect IT systems and data • NO formal delineation of cybersecurity roles/ responsibilities • NO formal City-wide adjudication process formed • NO taskforce established for risk assessment
2)	**Appoint Chief Information Officer, reporting directly to the Mayor**	• Created CISO reporting to CTO in OCTO
3)	**Develop Contingency Response Plan for Catastrophic Cyberattack on the District's Electrical Power**	• No Plan has been developed.
4)	**Establish Risk Governance Framework to Analyze Risks**	• A number of general risk assessment exercises currently exist, though not specifically for cyber threats. In 2016, HSEMA worked on a Community Risk Assessment as a tool for informing preparedness planning that considered cyber threats as part of the overall assessment.

SECTION 2: 2018 Commission Key Findings

While the Commission observed progress across the government in establishing technical capabilities and associated infrastructure to protect the District's information technology networks against cyber threats, the principal finding of the Commission was that the District continues to lack well-established coordination and collaboration processes within the government and across the NCR to safeguard the District's cyberspace. The Commission believes this is largely a result of the government not yet developing, through policy or legislation, a comprehensive governance model with clearly defined roles, responsibilities, and authority to oversee and implement cybersecurity across the District. Additional findings regarding governance, information sharing, preparedness, incident response, and resources flow from this critical deficiency and are detailed below.

GOVERNANCE OF CYBERSECURITY

1. **No formal cyber policy framework.** Despite previous Commission recommendations in 2013 to issue a cybersecurity directive, no citywide directive, legislation, or policy framework has been issued formalizing the District's cybersecurity governance model. District government staff interviewed by the Commission and responsible for cybersecurity in the District's executive agencies offered that an overarching directive or legislation would indeed help agencies better identify and prioritize operational requirements, institutionalize agency-specific roles and responsibilities, establish clear governance structures, and better guide resource allocation to help thwart and mitigate cyber threats.

2. **Key leadership elements to oversee District's cyber policies and administration established.** Despite the lack of a formal cybersecurity framework described above, the District has taken steps to codify some policies and key leadership positions. In 2017, as part of Mayor's *Order 2017-115*,[9] the District:
    a. Created a *Chief Data Officer* position, reporting to the Chief Technology Officer (CTO) with responsibility over the District's data governance processes;
    b. Put forth a *Data Policy* to safeguard citywide data from harm; and
    c. Created the position of *Chief Information Security Officer* (CISO) to be responsible for all matters pertaining to information security, and with explicit responsibility to establish an information security program, for the District government.

3. **Key elements of the District's cyber governance body are established, but connective tissue grow more by informal processes than through institutions**. Mayor's Order 2017-115 also set forth the establishment of two committees to govern IT and data security across the District: a committee of Agency Information Security Officers (AISOs), and a committee of Agency Data Officers (ADOs). The AISOs are chaired by the CISO and are in charge of developing and propagating best management practices, security plans, risk assessments, and associated other actions to further IT security districtwide. The ADOs are chaired by the CDO, and, with reference to cybersecurity, are in charge of protecting against inappropriate disclosure of personal information and misuse of data for activities such as identity theft or other significant concerns. The ADOs have met fifteen times since 2017 and the AISOs have

[9] District of Columbia Municipal Regulations and District of Columbia Register, 2017-115: District of Columbia Data Policy, April 2017, available at: https://octo.dc.gov/page/district-columbia-data-policy

met twice since they were established, pursuant to the District of Columbia Data Policy in 2017.

Even so, overall management and administration of the District's cybersecurity apparatus appears to be growing more through informal versus formal processes. Agencies across the District appear to emphasize informal professional networks, over the established AISOs/ ADOs committee-based governance model, as a basis for sharing information or best practices, or to address agency-specific cybersecurity needs. Specifically, agencies often turn to pre-existing personal or professional relationships—from other agencies, from colleagues in the Federal government or from other cities or the private sector—for support in addressing agency-specific needs or problems.

4. **Despite creation of key positions, the District's cybersecurity leadership lacks authority for instituting District-wide cybersecurity.** D.C. Code § 1-1402 assigns responsibility over the District government's information technology and telecommunications (IT) systems, including the IT systems of independent agencies, to the Office of the Chief Technology Officer (OCTO). Legislation establishing OCTO vests it with authority to develop and enforce policy directives and standards regarding information technology and telecommunications systems throughout the District government. Further, it delineates specific associated functions, including: procurement, information management, support to District services, and digital inclusion. It is, however, silent on cyber or IT security.

   As a remedy to this, Mayor's Order 2017-115 created a CISO, reporting to the District's Chief Technology Officer, and responsible for all matters pertaining to the District's information security. While this Order provides authority to the CISO to oversee security "across all District agencies, departments, offices, and other divisions," it only *encourages* "voluntary compliance" for government entities ***not*** subject to the Mayor's administrative authority. In other words, the CISO lacks authority to compel or require government entities outside the Mayor's direct authority to adhere to and implement the District's information security programs and practices. Such entities include, for example, the D.C. Board of Elections, and the Council of the District of Columbia. The consequences of this shortcoming are that independent agencies may adopt practices and protocols different than those recommended by the CISO.

5. **A clear cybersecurity role for HSEMA has not been formally established**. In the post 9-11 era, emergency management agencies (EMAs) were created (or re-created) to plan for, protect against, and respond to *terrorist* threats. A decade later, these organizations shifted to more of an *all*-hazards approach, to include cybersecurity, among other threats. Even so, planning for and protecting against cyber threats has rarely been a higher priority than for floods, disasters, terrorism, or pandemics and other bio-threats, until recently. As such, the cybersecurity role for municipal EMAs has yet to be well-established. This is the case with HSEMA as well.

   While statutory requirements for HSEMA direct it to lead District-wide efforts to prepare for, prevent, protect against, respond to, mitigate and recover from all threats and hazards, including cyber threats, and though the District's Prevention and Protection Plan does include some roles and responsibilities for HSEMA related to cyber in the Critical Infrastructure and Cybersecurity Annexes, currently, no formal doctrine, policy, or directive

exists clearly defining HSEMA's role (and associated responsibilities) in preparing for, warning the public about, and/or responding to cyberattacks.

Further, with Mayor's *Order 2017-115*, OCTO now operates a 24/7 cybersecurity operations center that: monitors the District's cybersecurity posture across the network and all systems; detects and leads OCTO's response to security incidents and escalates and reports on events and changes to the security baseline. This new entity—and its various roles—raise questions regarding the relationship between OCTO's cybersecurity responsibilities and HSEMA's *de facto* statutory responsibilities and leaves open a risk of resources being insufficiently budgeted for or employed, processes being duplicative, or key responsibilities not assumed.

6. **Much more work needs to be done to coordinate, prepare for, and ensure effective response to cyberattacks at the regional level, across the (NCR).** Local governments no longer have the luxury of being islands unto themselves. To the contrary, as urbanization pushes municipalities into larger integrated regions and mega-regions, and digitization integrates infrastructures and services—transportation, energy, water, telecommunications, and others—cities more and more rely on infrastructure and services beyond historic city boundaries. The District is already part of a deeply integrated region known as the 'National Capital Region." It is comprised of multiple jurisdictions, including:

   - the District of Columbia;
   - In Maryland, Montgomery and Prince George's counties; and
   - In Virginia, Arlington, Fairfax, Loudon, and Prince William counties, and
   - Each of their associated infrastructures, as well as emergency management systems, public safety and law enforcement organizations.

   There are three established regional bodies that have recently taken an interest in NCR cybersecurity coordination:

   - The NCR's Critical Infrastructure Protection Work Group (CIP WG), which has previously helped to coordinate regional critical infrastructure issues;
   - The Metropolitan Washington Council of Governments (MWCOG), a non-profit association established to provide networks among state and local governments in the NCR, and has started looking at its role in protecting the NCR from cyberattacks;[10] and,
   - A monthly regional CISO meeting that also serves as a forum for regional cybersecurity discussions.

   The Commission noted—as identified by these groups—existing shortcomings in regional cybersecurity preparedness due to lack of coordination, to include: differences in public-messaging; government-to-government communications; funding priorities; and resource availability; as well as regional planning for response to and recovery from cyberattacks.

INTELLIGENCE AND INFORMATION SHARING

[10] See meeting Metropolitan Washington Council of Governments meeting notes from National Capital Region Emergency Preparedness Council (EPC) meeting, May 10, 2017.

7. **Opportunities exist for strengthening threat information sharing and coordination**. Agencies were asked: "how do you stay ahead of cyber threats?" and, "what are your sources of intelligence?" Only governmental agencies subject to the administrative authority of the Mayor were directly connected to OCTO and HSEMA, which houses the District's Fusion Center, the NCR Threat Intelligence Consortium. These agencies regularly received pushed security updates. The District's independent agencies and others not subject to the administrative authority of the Mayor had less formal, little, or no relationship with OCTO. Regardless, even those directly connected to OCTO and HSEMA, supplemented OCTO's threat and security intelligence with information from other institutions, to include, for example, from: MS-ISAC; contracts with private sector threat warning and analysis firms; and/ or informal professional networks, to include government colleagues at the Federal Bureau of Investigations (FBI), U.S. Secret Service (USSS), DHS, or other state or municipal agencies. In practice, this means that at any one time, agencies across the District may not have a common view of threats, or for that matter, may maintain differing perspectives on threat priorities and security needs. Furthermore, agencies operating outside of the Mayor's direct administrative authority, and private sector critical infrastructure partners, were less likely to be integrated into OCTO's information-sharing and coordination orbit. As such, opportunities exist—and agencies relayed to the Commission, that organizations seek—to improve cybersecurity through greater coordination with and perhaps integration into OCTO's and HSEMA's threat information and intelligence sharing activities.

8. **Opportunities exist for strengthening coordination of disclosure of cyber threats and attacks to the public**. EMAs have, as one of their principal responsibilities, a mission of providing information and warning about threats to the public. HSEMA plays a key role in disseminating the District's public safety information, alerts and warnings. On a day to day basis, the HSEMA sends out emergency alerts to the public with critical information on public safety incidents and associated preparedness, safety and alert information. During emergencies and special events, HSEMA also assists the Mayor in coordination of the District's crisis communications. These responsibilities have been well-tested and in place for well over a decade, principally for severe weather conditions, disasters, national security events, terrorist threats, and other major events impacting quality of life. They have been less tested and not as well-established for cyber threats and cyberattacks. To the contrary, the Commission found that no government organization interviewed, including HSEMA, had a specific cyber-related public affairs plan in place to inform the public that they have faced a cyberattack. From a public perspective, this was evident in January 2017, when the District suffered its ransomware attack on the Metropolitan Police Department's surveillance cameras and District residents learned about the attack only after the government fixed the problem.

PREPAREDNESS AND INCIDENT RESPONSE

9. **The District—and other cities across the U.S.—lack a municipal reference model for assessing a city's cybersecurity posture or level of preparedness, or to measure the city's cybersecurity posture over time**. Commissioners struggled with the lack of a model or existing process to assess the District's cybersecurity posture. The question for District government leadership and those responsible for oversight is what constitutes baseline cybersecurity for a municipality and how does the District measure up? Further, how should each agency, department, or affiliated organization measure up to that baseline? How should each agency, department, or affiliated organizations monitor its own cybersecurity posture

over time? And how can the District with all its constituent agencies, divisions, and departments track and measure its cybersecurity posture as a whole, over time?

What the Commission found is that with respect to cybersecurity, there exists a range of viewpoints, and, in some cases, products regarding cybersecurity best-practices from the private sector, non-governmental organizations (e.g., the Center for Internet Security, the MS-ISAC and the National Governor's Association), and other governmental bodies (e.g., DHS, NIST).[11] Much of these recommendations are technical in nature. What Commissioners learned, however, is that there is not a single agreed upon and holistic "municipal reference model" for local governments to turn to regarding what constitutes a minimal viable security posture for a city, let alone best practice.

For example, many believe that metrics—like tracking the frequency and speed in which a city can patch bugs, remove malware, or detect intrusions—are important indicators of cybersecurity. But what about whether a city has a CISO in place, a regional response plan, or contracts in place for expanding technical support in times of attack? What about training programs and exercises? How many exercises, what type, and with what frequency constitute a best practice?

The consequence of this shortcoming is that local governments across the U.S.—the District included—are left to develop from the ground up what they each independently believe to be best practice, typically with advice from vendors, non-government organizations, or other governments or colleagues. None of these are comparable, cities are evaluated in a vacuum, and the nation as a whole is left less secure as a result.

10. **There are no established mechanisms in the District—or none formalized—for obtaining additional assistance in cases when a cyberattack overwhelms current capabilities.** Commissioners asked agencies, "where do you go for assistance if you are overwhelmed during a cyberattack?" And "to what extent do you have resources, relationships, and/ or contracts already in place to provide support in an attack that overwhelms your current capacity to thwart or mitigate an attack?" These questions may be particularly relevant in cases where agencies must respond to a distributed denial of service attack (DDOS), or in taking down an advanced persistent threat, or addressing other complex, intensive threats where an agency may need additional technical support or resources.

    Agencies directly under the Mayor's administrative authority rely on OCTO to provide cybersecurity resources before and during an attack. Other agencies or departments receive support from OCTO on a case-by-case basis. These entities may also have additional private sector contracts in place for further 'reach-back' technical support, as well. Agencies may also reach out to federal partners—DHS, FBI, or MS-ISAC, for example—for advice and

[11] For example, see best practices from Center for Internet Security (available at: https://www.cisecurity.org/cybersecurity-best-practices/); from the National Governor's Association (available at: https://www.nga.org/bestpractices/divisions/hsps/statecyber/); from the National Institute of Standards and Technology (available at: https://www.nist.gov/cyberframework); and from US Cert (available at: https://www.us-cert.gov/ccubedvp).

support, depending on whether they have pre-existing relationships with individuals in these organizations. In total, though, no formal or agreed upon mechanism is in place across the District for obtaining additional assistance in cases when a cyberattack overwhelms current capabilities.

11. **Some mechanisms exist for ensuring continuity of vital services and critical infrastructure in the District, but it is unclear how they may be utilized if needed to protect against cyberattacks.** Industries that provide vital services to District residents—hospitals, water, transport, power—have long-established business continuity plans to address historic threats such as natural disasters and terrorist attacks. The District government, similarly, has established mechanisms, to include within existing procurement and contract vehicles, for ensuring continuity of operations to support agencies in times of emergency. Opportunities exist, however, for greater districtwide and regional coordination to ensure sufficient resources would be available in instances when cyberattacks occur that are multi-agency or multiple-jurisdictional in nature.

POLICY AND RESOURCES

12. **Looking over the horizon, agencies are concerned that increased connectivity due to smart devices and infrastructure, may lead to increased risk to the District.** The District has and contemplates numerous smart city initiatives, to include: Pennsylvania Avenue 2040 (PA 2040), D.C. Gigabit Community Initiative, Smarter Waste Management, and looking at requiring new buses and trains to be 'online', with more connected communications and dashboards. With these and other initiatives, the District plans to connect more of its infrastructure to the internet, and, consequently, to potentially expose District residents to additional cyber risk. Commissioners found, however, that these so-called 'smart' initiatives do not routinely or uniformly make as a requirement, the appropriate security that may be needed to mitigate against potential additional cyber risk. Nor are there requirements for similar security at the regional level.

13. **Recruiting and retaining top talent could end up being a decisive factor in the District's cybersecurity posture**. Government – at all levels – has, in general, struggled to attract and retain top tech talent. It comes as no surprise, therefore, that this trend persists in such a technical field as cybersecurity. Lack of financial and staff resources remains a key concern for departments, agencies, and affiliated organizations seeking to improve security programs. Recruiting and retaining people to senior leadership executive positions (CISO, OCTO in particular) has been a challenge for the District.[12]

14. **Understanding and prioritizing risk across the District remains an unfulfilled priority.** The 2013 Homeland Security Commission report recommended that the District government create a taskforce to perform cybersecurity risk assessment. That recommendation has yet to be implemented at a time when more and more of the District's services and infrastructure are becoming digitized. The Commission believes more needs to be done by the District in

[12] John MacMichael, first District of Columbia appointed CISO, resigned from his position in January 2018. Thereafter, Suneel Cherukuri was named Acting CISO and then was named CISO on November 13, 2018, ten months after MacMichael's resignation. The District's Chief Technology Officer Archana Vemulapalli stepped down from her role effective January 5, 2018. Barney Krucoff was chosen by Mayor Bowser as Interim Chief Technology Officer in January 2018 and is currently serving in that role.

terms of inventorying risk, classifying risk, prioritizing risk, and providing a process or framework for managing and mitigating that risk.

COMMISSION RECOMMENDATIONS

For inhabitants of the District of Columbia, daily life, economic vitality, and security depend on a stable, safe, and resilient cyberspace. In fact, cybersecurity is the foundation of smart cities of tomorrow. But, as the District, like so many other cities, adopts digital technologies to reduce costs, improve operations, and address climate change, among other priorities, it also potentially opens the door to malicious actors and nation-states seeking to disrupt, destroy, or threaten the District's critical infrastructure and services.

These cyber threats unfortunately are not constrained by political, administrative, or jurisdictional boundaries. They readily travel regionally, globally and virally at the speed of light. Today, "smart city" projects are gaining appropriate momentum across the District and the country, but attention needs to be paid to properly architecting these from a cybersecurity and emergency preparedness perspective. Often these new innovation initiatives fall outside of the traditional IT department and under the domain of departments without a cybersecurity acumen. Similarly, the shift to smart infrastructures, and digitized city services and operations has taken root oftentimes without consideration to continuity of city operations or preparedness for catastrophes involving cyberattacks.

Thus, as cities digitize, they must also fundamentally change their way of doing business. Cybersecurity and preparedness for cyberattacks must become core government functions on par with accounting and public affairs—responsibilities that pervade every aspect of government. CISOs and their teams must shift their culture and mindset from stand-alone security operations, to integrated partners of broader emergency management teams, while HSEMA and its team must prepare for cyber-related incidents as they would snow emergencies or terrorist attacks.

Following a year's study of the District's cybersecurity posture, the Commission has come to a single most important conclusion: the District must timely advance a framework and corresponding programs for transforming its 20th century bureaucracy into a modern digital society – a *cyberdom*[13] – where residents and visitors can both rely on and enjoy a digitally secure city.

The following specific recommendations provide a roadmap for achieving such an effort. They will not be accomplished overnight, but time is also not on our side. Society is becoming fully digital; while cyberattacks more pervasive and consequential. Recent attacks on municipalities are only the opening act of what will likely become a persistent and potentially highly consequential threat. If the District aggressively implements this agenda, however, we believe it will greatly improve not just municipal security for the District, but, given the District's stature as the nation's capital, our nation's security as well.

GOVERNANCE OF CYBERSECURITY

[13] By 'cyberdom' we mean a jurisdiction – country, state, district, or territory – where business, governance, and daily life are enhanced by digital services and operations.

1. **Establish a Cyber Governance Structure.** *Adopt a formal cyber governance structure with clear roles, responsibilities, and processes to enable continued progress and prevent future bureaucratic lapses*. Such a structure should focus on establishing clear roles and responsibilities for OCTO/CISO and HSEMA, in particular, and include, among other priorities, the following:

    - Establish, under the District's Fusion Center or another similar body, an additional cyber capability (and associated membership) for coordinating training, education, technical assistance and outreach activities related to cybersecurity.

    - Improve NCR coordination. While cities have been spared thus far with potentially catastrophic cascading impacts of cyberattacks, recent events reflect an ever more sophisticated risk environment with increasingly severe consequences to cities and their associated infrastructure. The District must be prepared for such inevitability when cyber incidents, like floods, transcend local political boundaries, requiring multi-jurisdictional and regional response. As such, the Commission recommends the District expand cyber coordination and incident planning across the NCR, improve information sharing between the District government and life-line critical infrastructure private sector partners, and establish a common NCR operating picture and mutual-incident support capability for cyber. This capability would most likely reside in the District's Fusion Center and SOC (See "Intelligence and Information Sharing" #4 and #6, below) and should be supported by associated additional resources.

    - Establish a dedicated cyber focus within existing District risk assessments to ensure regular risk prioritization efforts that will inform leaders of priority concerns both in terms of cyber risk, but also cyber risks relative to all other risks.

2. **Empower CISO and HSEMA.** *Fully authorize OCTO and the CISO to develop, deploy and enforce, in partnership with HSEMA, and in coordination with other governmental entities, cybersecurity policy and procedures across all entities under the District's internet domain or system*. Legislation is required to clarify that the roles, responsibilities and authorities of OCTO and HSEMA apply broadly to District government and non-governmental entities, including sectors of critical infrastructure, as well as other entities within the NCR. Such clarification should include, but not be limited to authorities:

    - To ensure timely information-sharing, including authority to coordinate District government and non-governmental entities, establish information sharing relationships, and enter into information sharing agreements; and to timely receive, analyze, and disseminate information about cybersecurity risks and incidents;

    - To proactively develop and implement cyber protection, including authority to provide guidance, assessments, incident preparedness and response support, and other technical assistance upon request;

    - To foster infrastructure resilience, including authority to receive, through mutual assistance agreements or other arrangements, guidance, assessments, incident response support, and other technical assistance upon request; and

- To build and maintain a best-in-class workforce, including authority to establish cybersecurity positions, appoint personnel, fix rates of pay and promulgate implementing regulations in consultation with the District's Director of Human Resources; as well as to develop, coordinate, and implement apprenticeship, internship, training, and other related workforce recruitment, retention, and workforce cyber hygiene and advancement programs.

3. **Institute Cyber Policy, Law, and Practice.** *Institutionalize a standard practice for consideration of safeguarding cyberspace in development of new policy, law, regulation, programs, or procurement actions*. Much as privacy, environment, and budget impact analyses are requirements for developing new policies, programs, and regulations, cybersecurity, because ICT now pervades nearly all that we do, should similarly become a routine consideration. As a matter of course, therefore, the Commission recommends that the development of policy, legislation, and regulation, as well as new programs or procurement actions should include, baked into the process, a mandatory review of all such actions to fully assess their impact on safeguarding districtwide cyberspace, with an eye towards seeking opportunities to enhance districtwide cybersecurity.

INTELLIGENCE AND INFORMATION SHARING

4. **Establish a Cybersecurity Center within the District Fusion Center.** *In concert with OCTO and in close coordination with the Security Operation Center, HSEMA should establish a cybersecurity fusion capability under the NCR Threat Intelligence Consortium (NTIC) for cyber threat monitoring and information sharing*. The primary emphasis of this work would be just outside the firewall, to the wider region and world, to provide information to private industry, the public, and others. This would be a new function for HSEMA and associated additional resources to undertake this initiative should also be appropriated.

5. **Ensure Public Cybersecurity Disclosures**. *Develop and implement a policy and practice for Public Cybersecurity Disclosures to notify the public of potential cyber risks, maintain public confidence and potentially protect against unforeseen additional consequences***.** When a state or local government falls victim to successful cyberattacks or experiences other cybersecurity incidents that may incur substantial costs, they may well suffer other negative consequences such as increased cybersecurity protection costs, or loss of public trust or confidence due to unauthorized access or appropriation of sensitive personal data, among other risks. Establishing a framework for public disclosures, to include both timely and annual reporting, can help mitigate these risks.

PREPAREDNESS AND INCIDENT RESPONSE

6. **Establish OCTO's SOC as a regional hub** for technical support to District government agencies and for collaboration with District partners. The SOC currently is responsible for monitoring, detecting, analyzing, remediating, and reporting on cyber events and incidents impacting the technical infrastructure of the District of Columbia. Even so, the District's cybersecurity posture is only as strong as the integrity of the sum of its parts, which includes regional and private sector partners. Regional collaboration is vital to the District's security, as there are a variety of owners and operators of critical infrastructure, and other

governmental entities, that need to be communicating on a regular basis and involved in regional emergency response plans. These regional players should be invited to participate in and help support OCTO's security operations.

To better reduce the risk of systemic cybersecurity and communications challenges, the SOC must establish itself as a regional cybersecurity hub for information, technical expertise, 24/7 situational awareness, security collaboration and incident response. This could be done in partnership with the MS-ISAC, which routinely works with state, local, federal, private sector and international organizations, as well as with Fusion Centers, and the DHS National Cybersecurity and Communications Integration Center. Lines of effort would include collaborating regionally to:

- Promote actions to improve the risk posture across the District and its constituent local/ regional organizations and infrastructure;
- Support a common operational picture of the NCR cyber risk landscape; and,
- Defend District networks and respond to significant incidents. As this effort would expand and enhance current SOC capabilities, associated additional resources to undertake this initiative should also be appropriated.

7. **Develop Stafford Act for Cyber**. The Stafford Act authorizes the president to declare a "major disaster" or "emergency" in response to an incident or threatened incident that overwhelms the response capability of state governments. In 2018, the Governor of Colorado declared the first "cyber" state of emergency that enabled the deployment of federal resources and eligibility for federal aid. Working with the National Governor's Association, the State of Colorado, the International Association of Emergency Managers (IAEM), and the Joint DOD-DHS Cyber Protection and Defense Steering Group, the District should advance the development and implementation of a framework and standard practice for ensuring that federal emergency and disaster relief can be provided to states or the District, when a state or the District's resources are inadequate or overwhelmed during a cyber incident or attack.

POLICIES AND RESOURCES

8. **Establish and Employ a Municipal Reference Model for Cyber**. The District may or may not retain one of the nation's best postures for cybersecurity, but there's no easy way today of knowing. There is no agreed upon municipal reference model; no mechanism for measuring status, progress, gaps, or trends. Consequently, there is no way of comparing the District to its former self or to compare it to other similar municipalities. This is a shortcoming, not just of the District, but for all local governments seeking to provide assurances to city residents that their digital infrastructure and associated programs and services are secure. This reduces visibility to city managers responsible for overseeing cybersecurity and transparency to those who would seek to audit municipal programs and progress.

   As such, the Commission's strong recommendation is that the District should lead, in collaboration with the private sector, academia, and other municipalities, the development and adoption of a municipal reference model to enable and institutionalize regular cybersecurity posture reviews and audits. This framework would allow for the Mayor to set a baseline and more consistently measure over time municipal gaps, capabilities and trends;

compare municipal departments and agencies with each other and their peers; as well as understand the District's cybersecurity posture alongside other comparable municipalities. This model should include metrics on security (e.g., how many attempts to hack worker's email accounts or websites; viruses detected and deleted by antivirus software; spyware detected and deleted by antivirus software; patches performed; etc.); but also, metrics on governance, resources, information sharing, training, and preparedness.

9. **Prioritize Workforce Cyber competency**. To mitigate an ever-changing threat environment, the District should continue to prioritize one, recruiting and retaining best-in-class cybersecurity workforce, and two, instituting government-wide training programs for District government personnel, to include the following:

    - Appoint the District's top cybersecurity officials—the Chief Information Security and Chief Technology Officers are key positions that have been vacant (or filled with 'Acting' officials) for nearly a year[14].

    - Review and improve how the District acquires key homeland security talent. The Mayor's Office of Talent and Appointments (MOTA) assists the Mayor by making recommendations for outstanding community leaders to serve. Throughout the year-long course of this Commission's cybersecurity study, the CISO and the CTO remained vacant. Leaving key positions unfilled increases the District's security risk, and reflects either a lack of priority, lack of incentives to recruit and retain key talent, or shortcomings in the appointment process. It should be immediately addressed.

    - Establish a formal cybersecurity training program for the District's cybersecurity professionals with regular and continuous education as a professional performance requirement. As part of this effort, District agencies should take advantage of existing programs such as the Federal Virtual Training Environment (FedVTE), which is a free online, on-demand cybersecurity training system available at no charge for state and local government personnel and veterans.

    - Continue to grow the District's cybersecurity training programs for non-cybersecurity professionals, and incorporate them into onboarding and annual training programs, as well as, potentially, performance reviews.

    - Create internship, apprenticeship, and similar pipeline workforce recruitment programs, with colleges and universities, and others in the public and private sector, to augment and build a sustainable cybersecurity workforce. As an example, the District is eligible for and could participate in the federal *Scholarship for Service Program*, managed by the National Science Foundation that awards undergraduate students scholarships of up to 100 percent of their education expenses, for up to two years of service to the government (e.g., District government).

[14] NOTE: on Tuesday, November 13, 2018, as this Commission report was going into publication, OCTO released a statement naming Suneel Cherukuri as the new CISO replacing previous CISO, John MacMichael. See: https://octo.dc.gov/release/dc-names-new-chief-information-security-officer-ciso.

10. **Stand-up a Task Force for Recommendations on Enhancing the District's Cybersecurity Investments, Budgets, and Resources**. District government officials interviewed for this study widely discussed concerns regarding adequacy of budget resources for cybersecurity programs and activities. While the Commission was not in a position to assess these concerns on the merits or carry out a detailed review of the District's cyber budgets, there is no doubt such a study should be undertaken, particularly in concert with the establishment of a Districtwide Cybersecurity Framework and Governance Model, and associated programs as recommended in this report. Further, given the likelihood that additional resources may well be required, and given real fiscal constraints, the Commission recommends standing-up a task force to provide recommendations on novel models for enhancing the District's Cybersecurity Investments, Budgets, and Resources, to include, for example, consideration of cybersecurity investment incentive tax credits, and other potential new funding sources.

APPENDICES

APPENDIX A
Summary of Commission Findings

Table 1. Summary of Key Findings

1. No formal cyber policy framework.	2. Key leadership elements to oversee District's cyber policies and administration established.	3. Key elements of DC's cyber governance body established.
4. Despite recent initiatives, DC's cybersecurity leadership lacks authority for instituting districtwide cybersecurity.	5. Overall management and administration of the District's cybersecurity is growing organically, not necessarily via policy or plans.	6. A clear cybersecurity role for HSEMA has not been formally established.
7. Much more work needs to be done to coordinate, prepare for, and ensure effective response to cyberattacks at the regional level, across the National Capital Region (NCR).	8. Opportunities exist for strengthening threat information sharing coordination.	9. Opportunities exist for strengthening coordination of disclosure of cyber threats and attacks to the public.
10. The District and other cities across the U.S. lack a municipal reference model for assessing a city's cybersecurity posture or level of preparedness, or to measure the city's cybersecurity posture over time.	11. There are no established mechanisms in District or none formalized for obtaining additional assistance in cases when a cyberattack overwhelms current capabilities.	12. Some established mechanisms exist for ensuring continuity of vital services and critical infrastructure, but uncertain how they are being leveraged for protecting against cyberattacks.
13. Looking over the horizon, agencies are concerned that increased connectivity due to smart devices and infrastructure, may lead to increased risk to the District.	14. Recruiting and retaining top talent could end up being a decisive factor in the District's cybersecurity posture.	15. Understanding and prioritizing risk across the District remains an unfulfilled priority.

APPENDIX B

Summary of Commission Recommendations

1. Establish a Cyber Governance Structure.
2. Empower CISO and HSEMA.
3. Institute Cyber @ Policy, Law, and Practice.
4. Establish a Cybersecurity Center within the D.C. Fusion Center.
5. Ensure Public Cybersecurity Disclosures.
6. Institutionalize OCTO's SOC as a regional hub for technical support to D.C. governmental entities and for collaboration with District partners.
7. Develop Stafford Act for Cyber.
8. Establish and Employ a Municipal Reference Model for Cyber.
9. Prioritize Workforce Cyber competency.
10. Stand-up a Task Force for Recommendations on Enhancing the District's Cybersecurity Investments, Budgets, and Resources.

APPENDIX C
Key Commission and Stakeholder Meetings

The following table outlines the dates of each of the Commission's Quarterly Meetings and stakeholder briefings that were held to facilitate the development this report:

Meeting	Date
Homeland Security Commission Quarterly Meeting	September 15, 2017
Homeland Security Commission Quarterly Meeting	December 8, 2017
MS-ISAC Briefing	January 29, 2018
DC Water Briefing	February 9, 2018
DC Board of Elections Briefing	February 21, 2018
Office of the Chief Financial Officer Briefing	March 21, 2018
DC Homeland Security & Emergency Management Agency Briefing	March 23, 2018
Homeland Security Commission Quarterly Meeting	April 20, 2018
Exelon Corporation Briefing	April 23, 2018
Office of Unified Communications Briefing	June 13, 2018
Homeland Security Commission Quarterly Meeting	June 21, 2018
Washington Metropolitan Area Transit Authority Briefing	July 12, 2018
Office of the Chief Technology Officer Briefing	July 27, 2018
Homeland Security Commission Quarterly Meeting	August 20, 2018
Homeland Security Commission Quarterly Meeting	November 16, 2018