Testimony of Thomas Duffy
Senior VP of Operations and Security Services & Chair of the MS-ISAC
Center for Internet Security
Hearing on Cybersecurity Challenges for State and Local governments: Assessing How the Federal Government Can Help
Subcommittee on Cybersecurity, Infrastructure Protection and Innovation of the House Committee on Homeland Security
United States House of Representatives
310 Cannon House Office Building
Washington, DC
Tuesday, June 25, 2019
2:00 p.m. ET

Chairman Thompson, Chair Richmond, Ranking Member Katko, and members of the Subcommittee, thank you for inviting me today to this hearing. My name is Thomas Duffy and I serve as the Senior Vice President of Operations and Security Services at the Center for Internet Security, a global nonprofit focused on improving cybersecurity for public and private organizations. I also serve as the Chair of the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial governments as well as all 79 Fusion Centers.

I have spent my career in service to state and local governments, including the past 15 years with the MS-ISAC. I appreciate the opportunity today to share our thoughts on the current state of cybersecurity in state and local governments, focusing on how the federal government can help. I look forward to offering ideas on how we can collectively build on the progress being made to secure the state and local government cyber infrastructure.

In short, I will: (1) introduce you to the current level of cyber maturity in and local governments (2) the major challenges faced by and local governments and (3) recommendations on how the federal government can help.

About Center for Internet Security and the MS-ISAC

The Center for Internet Security's (CIS') was established in 2000 as a nonprofit organization and its primary vision is to lead the global community to secure our connected world through the identification, development, validation, information sharing, and sustainment of best practice solutions for cyber defense. CIS was instrumental in establishing the first guidelines for security hardening of commercial IT systems at a time when there was little security standards, best practices, or leadership.

The MS-ISAC was formed in 2004 under the auspices of the state of New York, and transitioned to CIS in 2010. The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) was formed in 2018, in response to the need to have a dedicated focus on protecting our nations election infrastructure.

Today, CIS works with the global security community using collaborative deliberation processes to define security best practices for use by government and private-sector entities. The approximately 200 professionals at CIS provide cyber expertise in three main program areas: (1) the Multi-State and more recently the Elections Infrastructure Information Sharing and Analysis Center, the MS-ISAC and EI-ISAC respectively; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

MS-ISAC[1]. In 2010, the U.S. Department of Homeland Security (DHS), under the then-National Protection and Programs Directorate (NPPD), partnered with CIS to host the MS-ISAC, which has been designated by DHS as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial) governments as well as all 79 Fusion Centers nationwide. MS-ISAC members include all 56 states and territories and more than 5,000 other state and local government entities. MS-ISAC's 24x7 cybersecurity operations center provides: (1) cyber threat intelligence that enables MS-ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) IP and domain monitoring (4) incident response support; and (5) various educational programs and other services. Furthermore, MS-ISAC provides around-the-clock network monitoring services with our so-called 'Albert' network monitoring sensors for many state and local government networks, analyzing over one trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2018, MS-ISAC analyzed, assessed, and reported on over 56,000 instances of malicious activity to over 6,000 MS-ISAC members.

EI-ISAC[2]. In 2018 CIS was tasked by DHS to stand up an information sharing and analysis center focused on the Nation's elections infrastructure. Leveraging the resources of the MS-ISAC, CIS established the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC is now fully operational with all 50 states participating and over 1,700 total members, including elections vendors. The EI-ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials. During the 2018 primaries and mid-term elections the EI-ISAC hosted the National Cyber Situational Awareness Room, an on-line collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats. More than 600 elections officials participated in these forums. Moreover, the MS-ISAC was processing data from

[1] : Find out more information about the MS-ISAC here: https://msisac.cisecurity.org/. List of MS-ISAC services here: https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf

[2] A list of EI-ISAC services can be found here: https://www.cisecurity.org/ei-isac/ei-isac-services/

135 Albert sensors monitoring the networks, which supported on-line elections functions such as voter registration and election night reporting. The Albert sensors processed 10 petabytes of data during 2018, resulting in over three thousand actionable notifications to elections offices.

CIS Benchmarks. CIS is also the world's largest producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Security Benchmarks (also known as "configuration guides" or "security checklists") provide highly detailed security setting recommendations for a large number of commercial IT products, such as operating systems, data base management systems, virtual private cloud environments, and for most of the major vendors network appliances. These benchmarks are vital for any credible security program. The CIS Security Benchmarks are developed though a collaborative effort of public and private sector security experts. Over 200 consensus-based Security Benchmarks have been developed and are available in PDF format free to the general public on the CIS or NIST web site. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called 'hardened images' that are based on the benchmarks that we are deploying in the Amazon, Google, and Microsoft cloud environments. These hardened images help ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS hardened images are used worldwide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Security Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan
- DHS Continuous Diagnostic Mitigation Program
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)
- CIS Critical Security Controls

CIS Controls[3]. In 2015, CIS became the home of the CIS Critical Security Controls, previously known as the SANS Top 20, the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene and essential cyber defense ground truth. They are developed by an international consensus process and are available free on the CIS web site. The Critical Security Controls or just the CIS Controls have been assessed as preventing up to 90% of

[3] Find out more information about the CIS Controls and download them for free here: https://www.cisecurity.org/critical-controls.cfm

pervasive and high risks cyber-attacks[4]. The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order—achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program[5].

The MS-ISAC, and more recently the EI-ISAC, are operated pursuant to a Cooperative Agreement with Department of Homeland Security. Members include all 50 states, all 50 state election directors, almost 6,000 local governments, 88 tribal governments , all 5 U.S. territories and the District of Columbia. Local government members represent over 80% of the U.S. population.

Cybersecurity Challenges Faced by State and Local Governments

Cyber protections at all levels of government are critical, and central to the fiduciary responsibility to protect the data that is entrusted to government by our citizens and businesses. Local governments connect to state governments, state governments connect to the federal government. All levels of government have a shared responsibility for safeguarding information. Data on citizens is tracked from cradle to grave, from the issuance of your birth certificate, to the filing your death certificate.

Regarding the question "has the cybersecurity posture of and local governments improved?" – the answer is yes. There are, however, other related and equally important questions that should be asked. If the question is "have and local governments kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected?", the answer is probably not. If the question is "are state and local governments prepared to build, maintain and evolve their cybersecurity programs commensurate with the risks that they will face in the future?", the answer is again, probably not. Both state and local governments continue to make news for ransomware, cybercrime and other cybersecurity-related issues every week.

The cyber threat landscape continues to evolve faster than our preparedness activities and protective measures, and the number of entry points to our systems continues to grow at an accelerated rate. We are constantly playing a game of catch up. There is no silver bullet to solve the problem. Software providers continue to issue patches for system vulnerabilities daily! Keeping up with this is an enormous challenge for all organizations, large and small.

---

[4] Up to 91% of all security breaches can be auto-detected when release, change and configuration management controls are implemented. IT Process Institute: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf

[5] NIST Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls)

The MS-ISAC conducts an annual cybersecurity maturity assessment, called the Nationwide Cybersecurity Review (NCSR), of state and local governments. The NCSR, based on the NIST Cybersecurity Framework, is a self-assessment tool developed by CIS in concert with state and local cybersecurity professionals.

What have we learned from the annual NCSR over the past few years?

The assessment uses a scale of 1-7 to measure cybersecurity maturity, and establishes a score of 5 as the minimum-security level organizations should strive for. The state average in 2018, was 4.7, with 44% states achieving the baseline of 5. The local government average is 3.4, with only 18% achieving the baseline minimum of 5. There have been improvements over time, with the states improving by 5% over the past 3 years and local governments improving by 17%. States on average report higher maturity scores than local governments. While improvements have been noted, there is much that still needs to be done, especially at the local government level.

One constant finding of the NCSR has been the top five security concerns, which remain unchanged for the past 5 years, the only difference being that the order of priority has changed every year. The top five concerns in 2018 were:

1. **Lack of sufficient funding** State and local governments struggle with balancing operational needs to improve their IT infrastructure and providing adequate cyber defense simultaneously. Threat actors continually attacking state and local governments with ransomware and breaching their legacy defense mechanisms to steal private data, causing an increase need to provide incident response, improve IT network defense, and reprioritize budgets to implement security best practices and security controls that often require major operating system and proprietary software migrations. The cybersecurity budget must to compete with other programs, such as education, infrastructure like roads and bridges, health care and law enforcement, for funding. The value of security investments is not obvious to public. Public officials don't run on a platform of "I am going to upgrade our IT infrastructure!". It is only after it is too late, that they realize a missed opportunity to prevent a major compromise, that requires a major investment in cybersecurity.

2. **Increasing sophistication of threats** It is no secret that threat actors, threat groups, and/or advanced persisted threats funded by nation states to carry out cyber espionage are increasing. Sophisticated malware like Emotet, which "reinvents" itself weekly to avoid detection by traditional defenses, is a good example of the bad guys making cyber defense a 24x7x365 job. In addition, threat actors are using realistic and effective spear phishing and phishing campaigns to gain access to state and local government systems and end-users' workstations and mobile devices.

3. **Lack of documented processes** Mature organizations have formally documented policies, standards and procedures. Implementation is tested, verified and reviewed regularly to ensure continued effectiveness. This not found

in most state and local governments. Many processes in managing government systems remain ad hoc. This is well documented in the NCSR. The priorities are to "keep the lights on", respond to emergencies, managing new projects, roll out new technologies, etc. One of the enhancements planned for 2019 in the NCSR is to included links to policies and standards where this is identified as a need in the NCSR submission. However, resources will be required to implement the policies and standards and ensure they are tested, verified and reviewed regularly.

4. **Emerging technologies** The future is now. Major urban areas are in the progress of building 5G communications infrastructures to support the rapidly growing need for connectivity to support autonomous vehicles, data streaming services, consumer electronics and smart devices. IoT devices are now finding their way into daily government operations. HVAC systems are now connected to the internet as are medical devices. Drone technology is being deployed across all levels of government. Each of these technologies require organizations to expand the scope of protective measures that need to be implemented, tested and verified regularly. They also introduce new opportunities for attackers to exploit networks looking for vulnerabilities or lapses in security. Status quo will not protect your network. The defenses need to continually evolve. We must proactively put in place security measures that effectively defend against current and future cyber threat attacks.

5. **Inadequate supply of security professionals** The NCSR clearly highlights what is a national problem – the shortage of skilled cybersecurity professionals. This impact of this lack of talent is even more impactful for state and local governments entities due to lower pay. State and local governments are at a major disadvantage in recruiting cybersecurity professionals. Vacant positions mean some critical work may not be accomplished.

Each year, the DHS issues a National Preparedness Report on the challenges that all organizations, public and private, face in preparedness. It includes a capabilities assessment in thirty-two core areas reported by every state. The 2018 report noted:

1. Cyber threats are a rapidly evolving threat, joining nation-state threats and terrorism as an area of significant public concern.
2. Since 2012, states and territories have consistently reported cybersecurity as their least proficient capability."

Just this past weekend CISA reported on "a recent rise in cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies." Improving our cyber security posture will take time. We must act now.

Recommended Actions for the Federal Government

Addressing these challenges requires resources as well as state and national strategies. We need to: increase the pool of cybersecurity professionals, plan for investments in our IT infrastructure, and ensure that security is built into products and services.

What can the federal government do to assist state and local governments?

DHS has been very supportive in addressing the increasing challenges of state and local governments posed by expanding cyber threats, including funding of the Multi-State ISAC and Election Infrastructure ISAC, allowing state and local governments to participate in the Federal Virtual Training Environment (FedVTE), allowing state and local governments to participate the Scholarship for Service Program sponsored by the National Science Foundation. It has also developed the National Cybersecurity and Technical Services program that provides network scanning and penetration testing among its many service offerings. It has been very active in improving the security of our nation's election infrastructure and developing and sponsoring local, state and national cyber exercises. A national level election exercise sponsored by DHS last week.

There are two areas that I would recommend consideration be given to additional federal cyber support to the state and local community.

First, DHS should establish a dedicated state and local government cybersecurity grant program. When the initial Homeland Security Grant programs were created, the cybersecurity threat was not what it is today. Most of the funds were dedicated to anti-terrorism efforts, as was appropriate. Over time the grant funds have decreased, while cyber threat has expanded exponentially and the terrorism threat still exists. Thus, a smaller pool of funding is available for a large pool of threats. More money is going to sustain activities, leaving less money for new initiatives. If a cyber grant program is established, priority should be given, or funds set aside, to programs that support state and local partnerships. Leveraging the combined resources of state and local governments will serve as force multiplier. There are several great examples of state and local partnerships including the Wisconsin Cyber Response Team that was organized by the state to recruit local government staff to be regional cyber incident responders for local governments. Local government staff that met minimum qualifications were chosen to be part of the regional teams and received advance training by the state, that led to led to incident response certifications. The regional teams have responded to over thirty incidents since its inception.

Second, the federal government should adopt a "single audit" approach when auditing state programs for compliance with the security guidelines of the cognizant federal agencies. In 1984, the Single Audit Act was passed. The Act refers to a "single audit" because it consolidated multiple audits of non-federal agencies required for each award into a single audit. The stated purpose was to promote sound financial management of government funds by non-federal organizations, promote uniform guidelines for audits, and reduce the burden on nonprofits by promoting efficient and effective use of audit resources. It proved to be a cost-effective method audit of non-federal entities. One audit is conducted in lieu of multiple audits of individual programs and single audit

standard is applied. The same should apply to the security audits of state programs by federal agencies.

The following are some of the federal agencies that audit state systems: Centers for Medicare & Medicaid Services, Internal Revenue Service, Social Security Administration, Department of Agriculture, and Department of Health and Human Services. Although the compliance\audit requirements are often based on NIST SP 800-53, they vary in the amount of time required by the state to meet the requirements. For example, some federal agencies send an on-site audit team to the state to review security controls while other federal agencies rely on the completion of a written questionnaire. Regardless, there are multiple audits being conducted that duplicate each other, and place a drain on scarce state resources dedicated to protecting state systems. Let these resources be freed up to develop and implement new cyber protective measures. The "single audit" concept would create savings for both the federal and state governments, savings that could be re-invested to enhance their cybersecurity posture.

Closing

Defending our Nation from rapidly advancing cyber threats has become a critical, yet incredibly difficult task. The overwhelming vulnerability inherent in the "Internet of everything" caught us off guard, forcing most organizations into reactive mode, and the asymmetry of cyberwarfare ensures that the good guys are always at a disadvantage. All this while we increasingly rely on a safe, secure and trustworthy internet to do everything from ordering groceries to ordering drone strikes.

And while state and local governments have made progress in key areas, so have our adversaries. The dizzying array of cybersecurity requirements has made it difficult to develop effective programs, a lack of funding stalls progress and a lack of capable talent compounds the negative impacts of ransomware and other attacks. We must do better.

Our success or failure will be determined by our ability to have all levels of government work together to evade, counter or neutralize the endless risks that state and local governments state face. Each of these efforts require resources – time, money and energy – that are currently in short supply. If we are to make the progress required of us in meeting our collective missions, we must work together.

Attachments A: Biography of Thomas Duffy

Thomas F. Duffy
Senior VP of Operations and Security Services
Chair of the MS-ISAC
Center for Internet Security, Inc.

Tom is the Senior Vice President, Operations and Security, and the Chair of the Multi-State Information Sharing and Analysis Center, at the Center for Internet Security (CIS). He is responsible for managing all aspects of the CIS Security Operations and Security Services including services provided by the MS-ISAC. The MS-ISAC has been designated by DHS as the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal governments. He provides leadership in developing program, organizational and financial strategies. He also oversees the operation of the CIS 24-hour cybersecurity watch and warning operations center, which provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. Mr. Duffy works closely with the U.S. Department of Homeland Security (DHS), including its National Cybersecurity and Communication Integrations Center, as well as with state, local, tribal and territorial officials across the country.

Prior to joining CIS, Tom worked for New York State in a variety of senior level positions including as a member of the Governors' Task Force on Information Resource Management, Executive Deputy Commissioner at the Office for Technology and Deputy Director at the Office of Cybersecurity and Critical Infrastructure Coordination. In these roles he was part of the centralization of information technology programs for state agencies, the establishment of the Office for Information Technology and the creation of a statewide cybersecurity program.