Department of Homeland Security Cybersecurity Support to Nonfederal Levels of Government: State, Local, Tribal, and Territorial Government Entities

March 26, 2019

Fiscal Year 2018 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director of the Cybersecurity and Infrastructure Security Agency

March 26, 2019

I am pleased to present the following report, "Department of Homeland Security Cybersecurity Support to Nonfederal Levels of Government: State, Local, Tribal, and Territorial Government Entities," which has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency.

This report details the overall effectiveness and outreach in improving cybersecurity resources, capacity, and performance at nonfederal levels of government, including state, local, tribal, and territorial government entities. This report has been compiled pursuant to the language set forth in the Joint Explanatory Statement accompanying the Fiscal Year 2018 Department of Homeland Security Appropriations Act (P.L. 115-141).

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jon Tester
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (202) 282-8260 or to CISA's Office of the Chief Financial Officer at (703) 235-2111.

Sincerely,

Christopher C. Krebs
Director

Department of Homeland Security Cybersecurity Support to State, Local, Tribal, and Territorial Government Entities

Table of Contents

I. Legislative Language

This report has been prepared pursuant to the requirements set forth in the Joint Explanatory Statement accompanying the Fiscal Year (FY) 2018 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-141). The Joint Explanatory Statement includes the following provision:

> Not later than 120 days after the date of enactment of this act, NPPD and FEMA shall brief the Committees on the types of grant assistance, technical assistance, and formal ongoing engagement available to SLTT government entities, including law enforcement agencies, for the purpose of protecting their cyber networks. Within 240 days of the date of enactment of this Act, NPPD shall provide an assessment to the Committees of the overall effectiveness of this assistance and outreach in improving cybersecurity capacity and performance at non-federal levels of government. The Department may provide technical assistance and support to SLTT entities related to the purchase of commercial software capable of protecting the integrity of government information and networks against intrusions.

Section 2202(a)(2) of the Homeland Security Act, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 (P.L. 115-278), states that "Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department." As such, the Joint Explanatory Statement's reference to the National Protection and Programs Directorate (NPPD) as well as all other statutory references to NPPD contained in this document apply to the Cybersecurity and Infrastructure Security Agency (CISA).

II. Background

This report is a response to P.L. 115-141, which compels CISA and the Federal Emergency Management Agency (FEMA) to provide the House and Senate Appropriations Subcommittees on Homeland Security information about the types of grant assistance, technical assistance, and formal ongoing engagements available to state, local, tribal, and territorial (SLTT) government entities for the purpose of protecting their cyber networks.

Nationwide Cybersecurity Review

The Nationwide Cybersecurity Review (NCSR) is an annual self-assessment designed to measure the gaps and capabilities of SLTT governments' cybersecurity programs. Based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, this annual assessment is funded by DHS and facilitated by the Multi-State Information Sharing and Analysis Center (MS-ISAC). Using the results of the NCSR, DHS delivers a biennial summary report to Congress providing a broad picture of cybersecurity maturity across SLTT governments. Additional information can be found online at: https://www.cisecurity.org/ms-isac/services/ncsr/.

CISA

CISA coordinates many of DHS's cybersecurity engagements with SLTT government entities. Through developed relationships, as well as direct, indirect, and self-service engagement, DHS provides SLTT communities with the ability to further advance their cybersecurity risk management.

CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24/7 operational and technical support, incident response, and analysis of cybersecurity risks, as well as exercise and planning programs. The NCCIC is the central hub of cybersecurity and communications integration for the Federal Government, SLTT government entities, the intelligence community, law enforcement, the private sector, and international entities. The NCCIC applies unique analytic perspectives, ensuring shared situational awareness and orchestrating synchronized response efforts while protecting the constitutional and privacy rights of Americans. The NCCIC's role is to lead the protection of Federal civilian agencies in cyberspace, as well as to provide support and expertise to SLTT government and critical infrastructure owners and operators.

CISA streamlines strategic outreach to government and industry stakeholders, including SLTT governments. Through stakeholder engagement, CISA sustains strategic SLTT and critical infrastructure relationships to implement persistent cyber risk management, as well as to perform outreach and education activities related to DHS cyber capabilities.

These strategic relationships allow DHS experts to work collaboratively with SLTT governments and industry stakeholders in order to improve cyber resilience in critical areas. While the majority of CISA's efforts focus on long-term and systemic protection and prevention, CISA's

efforts also help to position stakeholders to act decisively with little-to-no notice during a cyber incident.

FEMA

FEMA's Homeland Security Grant Program (HSGP) provides funding to SLTT governments to prevent, protect against, mitigate, respond to, and recover from potential terrorist attacks and other hazards. The HSGP plays an important role in the implementation of the National Preparedness System (NPS) by supporting the building, sustainment, and delivery of core capabilities essential to maintaining a secure and resilient Nation. Funds can be used for preparation, organization, equipment purchase, training sessions, exercises, management, and administration across all core capabilities and mission areas.

Overarching Approach to Increasing SLTT Cybersecurity

DHS's strategy is to raise the level of cybersecurity across a broad range of stakeholders nationally, including SLTT governments. Through the development of relationships with SLTT agencies around the country, government entities such as the SLTT Government Coordinating Council (GCC) and SLTT associations, DHS gathers accurate requirements, measures net risk reduction, and provides comparative analysis.

This process enables two outcomes. The first outcome is the implementation of governance, standards, policies, and procedures that raise the national baseline level of cyber capabilities. One example of this includes developing models for statewide incident response plans that fully account for Federal and SLTT roles and responsibilities. The second outcome is support services made available to SLTT governments. DHS applies a layered approach of direct, indirect, and self-service support to improve national cybersecurity posture tangibly.

III. Cybersecurity Support to SLTT Government Entities

DHS provides a number cybersecurity support services in distinct categories for its SLTT stakeholder base: Cybersecurity Assessments and Incident Response; Information Sharing and Awareness; Training, Education, and Resources; Detect and Prevent; MS-ISAC; and FEMA Grants.

A. Cybersecurity Assessments and Incident Response

Cybersecurity assessments are conducted to acquire an accurate understanding of what organizations are attempting to protect, the inherent and residual cybersecurity risk, and the maturity of the overarching security program and its underlying controls, as well as comparative analysis. Upon request by the entity, DHS provides a range of assessments that provide SLTT governments with strategic, operational, and technical perspectives to improve cybersecurity. These assessments build awareness of cyber and communications vulnerabilities, threats, incidents, impacts, and mitigations. The assessments that DHS offers to SLTT entities are voluntary, nonbinding, and no-cost.

Strategic assessments such as the Cyber Infrastructure Survey (CIS), the Cyber Resilience Review (CRR), and the Risk and Vulnerability Assessment (RVA) allow entities to assess their cybersecurity posture. These assessments provide a comparative analysis via an interactive dashboard that allows SLTT governments to plan for and mitigate impacts during an incident. This approach increases cybersecurity awareness and overall preparedness within SLTT communities.

Operational DHS programs and capabilities support SLTT governments. For example, Hunt and Incident Response Teams (HIRT) are available to assist SLTT governments during a cyber incident. Other technical services offered to SLTT governments include the Advanced Malware Analysis Center and routine vulnerability scanning.

Cyber Infrastructure Survey

The CIS is a strategic, no-cost, and voluntary survey that evaluates the effectiveness of an SLTT government's organizational security controls, cybersecurity preparedness, and overall resilience. Conducted by Cybersecurity Advisors (CSA), the CIS is an assessment of essential cybersecurity practices that are in place for critical services. The CIS is a structured, interview-based assessment focused on more than 80 cybersecurity controls grouped under 5 key surveyed topics. This facilitated assessment is conducted through an informal interview—typically 2.5 to 4 hours—with up to 2 cybersecurity personnel from the entity. Following the assessment, DHS provides participants with the ability to review and interact with the findings via a user-friendly and data-rich dashboard through a secure, online portal. The CIS dashboard allows entities to visualize results and provides a comparative analysis against other SLTT organizations. The CSA program conducted 47 CISs with SLTT government entities during FY 2018, including 20 CISs conducted specifically on elections infrastructure. *(Aligns to the May 2018 DHS*

Cybersecurity Strategy, Goal 1 Assess Evolving Cybersecurity Risks Objective 1.1 Maintain Strategic Awareness of Trends in National and Systemic Cybersecurity). [1]

Cyber Resilience Review

Another strategic cybersecurity assessment offered by DHS is the CRR. The CRR is a no-cost and voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors and SLTT governments. The goal of the CRR is to measure key cybersecurity capabilities in order to provide meaningful indicators of an entity's ability to manage cyber risk to critical services during normal operations, times of operational stress, and crisis. To ensure the protection and sustainment of an entity's critical services, the CRR seeks to understand the entity's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors in 10 domains: Asset Management, Controls Management, Configuration and Change Management, Vulnerability Management, Incident Management, Service Continuity Management, Risk Management, External Dependency Management, Training and Awareness, and Situational Awareness. Through the CRR, an organization will develop an understanding of its ability to manage cyber risk during normal operations and in the event of an incident. During FY 2018, the CSA program conducted 62 CRR assessments with SLTT government entities across the Nation, including 24 CRR assessments specifically for elections infrastructure. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 1 Assess Evolving Cybersecurity Risks Objective 1.1 Maintain Strategic Awareness of Trends in National and Systemic Cybersecurity).*

National Cybersecurity Assessments and Technical Services

CISA offers vulnerability scanning and penetration testing via the National Cybersecurity Assessments and Technical Services (NCATS) team. The NCATS team conducted multiple RVAs in FY 2018. An RVA is a no-cost offering that combines national threat and vulnerability information with data collected through onsite assessments in order to provide stakeholders with actionable recommendations prioritized by risk. Engagements are designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment can include scenario-based network penetration testing, Web application testing, social engineering, wireless testing, configuration reviews of servers and databases, and evaluation of an organization's detection and response capabilities. The NCATS team conducted 36 RVAs of election sector SLTT organizations in FY 2018. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 1 Assess Evolving Cybersecurity Risks Objective 1.1 Maintain Strategic Awareness of Trends in National and Systemic Cybersecurity).*

[1] For a copy of the May 2018 DHS Cybersecurity Strategy, see: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

National Cybersecurity and Communications Integration Center

The NCCIC operates 24 hours a day every single day of the year, and is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat information, and coordinating incident response and mitigation activities. The NCCIC uses information from across the globe and operational capabilities to defend Federal networks, assist the private sector with defending its own networks, and share situational awareness about the cyber and communications risk landscape. The NCCIC shares classified and unclassified information through trusted and operational relationships with a broad range of stakeholders. The NCCIC conducts assessment, cyber hunt and incident response, network monitoring, threat and malware analysis, and open-source research. During FY 2018, the NCCIC provided situational awareness and coordinated operational activities to assist SLTT governments. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 5 Respond Effectively to Cyber Incidents Objective 5.1 Increase Voluntary Incident Reporting and Victim Notification to Facilitate the Provision of Response Assistance and Objective 5.2 Expand Asset Response Capabilities to Mitigate and Manage Cyber Incidents).*

Cybersecurity Support for Special Events: Super Bowl LIII

In FY 2018, the NCCIC closely engaged with the City of Atlanta, Georgia in preparation for Super Bowl LIII. DHS serves as the co-chair to the Atlanta's Communications Infrastructure Subcommittee to ensure that there is sufficient capacity and coverage of communications at the venue sites. Additionally, in FYs 2018 and 2019, DHS coordinated closely with both the National Football League and Atlanta for cyber vulnerability assessments and tabletop exercises. A cyber tabletop exercise occurred on September 21, 2018, which included numerous Federal and SLTT government entities and private-sector members.

Hunt and Incident Response Team

CISA offers hunt and incident response capabilities through HIRTs. A HIRT provides mitigation and recovery services through 24/7 intrusion analysis post-incident. DHS utilizes state-of-the-art hunting capabilities to identify advanced adversary presence proactively in a network that evades traditional security controls. Skilled personnel are dispatched when a cyber incident occurs to assist in malicious actor identification, technical analysis, containment, mitigation guidance, and post-incident recovery.

HIRTs have provided incident response and coordination activities successfully for cyber incidents in SLTT governments. During FY 2018, HIRTs conducted 20 hunt engagements for SLTT entities to identify malicious activity on systems and networks, including 17 for election cybersecurity. These engagements include 4 proactive hunt engagements and response to one SLTT incident involving suspected intrusion by foreign actors. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 5 Respond Effectively to Cyber Incidents Objective 5.1 Increase Voluntary Incident Reporting and Victim Notification to Facilitate the Provision of Response Assistance and Objective 5.2 Expand Asset Response Capabilities to Mitigate and Manage Cyber Incidents).*

National Communications Coordination

The NCCIC is the lead for Emergency Support Function #2 (ESF-2) - Communications. ESF-2 supports the restoration of communications infrastructure, facilitates recovery of systems and applications from cyber incidents, and coordinates Federal communications support to response efforts. ESF-2 also provides information and communications technology support to SLTT government entities and first responders when their systems have been affected. Following the devastating hurricane season of 2017, the NCCIC coordinated the restoration and repair of telecommunications infrastructure. The NCCIC also coordinated the protection and sustainment of cyber and information technology resources of affected SLTT government entities in Texas, Florida, and Puerto Rico. The ESF-2 Communications Training and Exercise team restarted the Annual Spring Exercise, which occurred in April 2018. The ESF-2 Webinar Series offered SLTT emergency communications operators and first responders distance learning and collaboration opportunities regarding incident response protocols. Responding to hurricane disasters in Puerto Rico, the SHAred RESources (SHARES) program, administered through the NCCIC, helped the Puerto Rico National Guard personnel to get their high frequency (HF) radios working for emergency communication coordination. The SHARES program was able to send email communications by HF when conventional Internet and communications infrastructures were not working properly in Puerto Rico. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 5 Respond Effectively to Cyber Incidents Objective 5.1 Increase Voluntary Incident Reporting and Victim Notification to Facilitate the Provision of Response Assistance and Objective 5.2 Expand Asset Response Capabilities to Mitigate and Manage Cyber Incidents).*

Advanced Malware Analysis Center

DHS provides dynamic analyses of malicious code in the event of an SLTT government discovering and reporting malicious code via the Advanced Malware Analysis Center. The Center is a standalone and closed computer network system used for analyzing computer network vulnerabilities and threats as well as for enabling the NCCIC to collect, analyze, and exchange malware information 24/7. Stakeholders submit malware samples via an online website and receive a technical document outlining the results of the analysis. Experts then detail recommendations for malware removal and recovery activities. This service can be performed as part of incident response, should the incident require it. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 5 Respond Effectively to Cyber Incidents Objective 5.1 Increase Voluntary Incident Reporting and Victim Notification to Facilitate the Provision of Response Assistance and Objective 5.2 Expand Asset Response Capabilities to Mitigate and Manage Cyber Incidents).*

Vulnerability Scanning and Assessments

CISA supported vulnerability scanning and assessments (known as Cyber Hygiene scanning) of Internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities. CISA also provides onsite support to SLTT governments by assisting them with performing a security self-assessment of their enterprise and control

system networks. During FY 2018, the program delivered 31,847 scanning reports to more than 700 system owners, including 247 SLTT government entities and 133 of these entities specifically for elections infrastructure. The program has put a renewed focus on increasing coverage of elections infrastructure for SLTT government entities. For example, in FY 2018, the Governor of Ohio issued a mandate for 88 counties to sign up for DHS Cyber Hygiene and Phishing Campaign Assessments to help secure election infrastructure. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 1 Assess Evolving Cybersecurity Risks Objective 1.1 Maintain strategic awareness of trends in national and systemic cybersecurity).*

B. Information Sharing and Awareness

Automated Indicator Sharing

CISA offers the automated indicator sharing (AIS) capability, which enables the exchange of cyber threat indicators between the Federal Government, SLTT government entities, and the private sector at machine speed. Threat indicators are information such as malicious IP addresses or the sender's address of a phishing email. AIS is part of a DHS effort to create a cyber ecosystem in which as soon as a stakeholder observes an attempted compromise, the cyber threat indicator of the compromise will be shared in real time with all stakeholders, thereby protecting everyone from that particular threat. AIS shared 3.6 million indicators in FY 2018. AIS's capability currently consists of 22 SLTT government entities that are direct participants, while 20 Information Sharing and Analysis Organizations as well as Information Sharing Analysis Center participants act as effective force multipliers for SLTT stakeholders. In total, there are 4,200 indirect participants in the program receiving threat feed data from 234 direct participants. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 3 Protect Critical Infrastructure Objective 3.2 Expand and Improve Sharing of Cyber Threat Indicators, Defensive Measures, and Other Cybersecurity Information).*

Homeland Security Information Network

DHS offers the Homeland Security Information Network (HSIN), which provides a platform that allows for increased collaboration and information sharing across communities. The portal provides to stakeholders the ability to share threat analysis and products within trusted communities of interest. For instance, the National Cyber Situational Awareness Room (NCSAR) is a forum for the SLTT/elections community, fusion centers, and Federal partners to participate in real-time as well as to secure information sharing and collaboration on issues

HSIN NCSAR Support to Election Infrastructure
The Election Infrastructure-Information Sharing and Analysis Center (EI-ISAC) operates the National Cyber Situational Awareness Room for EI-ISAC members in jurisdictions holding a primary or general election. The room is open several days in advance of or following an election. The room provides a centralized information sharing platform for the elections community and Federal partners regarding cybersecurity threats to election infrastructure. Invitations to the room are limited to EI-ISAC members in states holding an election that day, as well as Federal partners.

impacting elections. Vetted individuals with an HSIN account have access to the NCSAR as participants.

C. Training, Education, and Exercises

Cybersecurity Education and Training Assistance Program

DHS manages the Cybersecurity Education and Training Assistance Program (CETAP), which provides grant funding to promote cybersecurity education. The grantee, the National Integrated Cyber Education Research Center, supports a coordinated effort to increase knowledge of cybersecurity careers and to engage students and teachers in cybersecurity education. As of November 2018, more than 13,500 kindergarten through twelfth-grade (K-12) teachers have accessed the DHS-sponsored cyber education curricula, affecting more than 2.1 million students. K-12 educators access curricula through a learning management system that provides easy access to course materials (student workbooks, teacher and master notes, lesson plans, assessments, and other supplemental materials) free of charge. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 6 Strengthen the Security and Reliability of the Cyber Ecosystem Objective 6.4 Improve Recruitment, Education, Training, and Retention to Develop a World-class Cyber Workforce).*

Crosscutting Support - CSA Program

The DHS CSA program provides regionally located personnel who engage state and local governments to offer immediate and sustained assistance to prepare for and protect from cyber threats. The CSA program offers cybersecurity assistance on a voluntary and no-cost basis to critical infrastructure organizations, including SLTT governments.

During FY 2018, the CSA program established 8 new partnerships with SLTT water and wastewater stakeholders in Massachusetts and New Hampshire. These recent new partnerships were due in part to the relationship with regional U.S. Environmental Protection Agency (EPA) partners emphasizing the importance of cyber resilience through cybersecurity workshops. The CSA program participated in several tabletop exercises with regional water and wastewater owners and operators over the course of FY 2018. This newly established DHS/EPA partnership has made DHS cybersecurity resources available to a customer set that previously was not taking advantage of these programs to reduce overall cyber risk.

Another specific accomplishment of the CSA program in FY 2018 included providing direct onsite support to the special elections held by New Jersey, Utah, and Virginia. This direct onsite support resulted in close coordination between the state-level election chief information officers (CIO) and the NCCIC during the course of the election. This close coordination allowed the state CIOs to request information directly from the NCCIC via the CSAs while still being able to focus on supporting the election information technology (IT) infrastructure of their respective states. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 3 Protect Critical Infrastructure).*

Federal Virtual Training Environment

DHS offers the Federal Virtual Training Environment (FedVTE), which provides free cybersecurity training, available to all U.S. Federal and SLTT government employees, Federal contractors with the permission of their Federal sponsor, and U.S. active duty military and veterans. FedVTE contains more than 60 courses, providing online, on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness. Courses range from beginner to advanced levels and training is accessible from any Internet-enabled computer or mobile device. At the end of FY 2018, 250,000+ total users were registered on FedVTE, including 1,000+ SLTT-specific users and 38,000 military and veteran-specific users. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 6 Strengthen the Security and Reliability of the Cyber Ecosystem Objective 6.4 Improve Recruitment, Education, Training, and Retention to Develop a World-class Cyber Workforce).*

National Cyber Exercises and Planning Program

CISA's National Cyber Exercises and Planning Program (NCEPP) provides cyber exercise planning workshops and seminars, as well as conducts tabletop, full-scale, and functional exercises for organizations. These exercises enable organizations to rehearse their response to staged incidents, allowing organizations to develop "muscle memory" and identify areas that may need to be improved in order to prepare for a real-world situation. NCEPP's goals are to strengthen U.S. national cybersecurity resilience through cyber exercise planning and execution, advance exercise stakeholder relationships and cooperation, and expand opportunities for engagement.

NCEPP supports continued improvement in national cyber preparedness and resilience through designing, developing, and conducting cyber exercises and cyber plans for Federal and SLTT government entities, international stakeholders, and critical infrastructure-sector stakeholders. The program also renewed focus on supporting SLTT elections cybersecurity. As a result, the program conducted 14 election cybersecurity exercises, including a 3-day National Level Virtual Exercise and 13 focused exercises, including 6 in New York, 3 nationally, and 1 each for Rhode Island, South Carolina, Kentucky, Colorado, and the National Association of Counties membership. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 5 Respond Effectively to Cyber Incidents Objective 5.3 Increase Cooperation Between Incident Responders to Ensure Complementary Threat Response and Asset Response Efforts).*

Cyber Storm VI
Cyber Storm, DHS's biennial exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind.

During FY 2018, the Cyber Storm VI National Level exercise included significant SLTT participation. The focus was on the critical manufacturing and transportation sectors, with participation from the information communications and technology sectors; law enforcement, defense, and intelligence agencies; state and local governments; and international partners.

National Initiative for Cybersecurity Careers and Studies Catalog

The National Initiative for Cybersecurity Careers and Studies (NICCS) Catalog serves as the central location where cybersecurity professionals can find more than 4,000 cybersecurity-related courses both online and in-person from more than 160 providers across the Nation. NICCS provides research and training information through a catalog of cyber training programs that can be filtered by location, preferred delivery method, specialty area, or proficiency level. NICCS also provides information about science, technology, engineering, and math programs, along with cyber-related degree programs and cyber competitions and events. Courses help participants to increase their expertise, earn a certification, or even transition into a new career.

All of the courses are aligned to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which is the foundation for increasing the size and capability of the U.S. cybersecurity workforce and serves as the blueprint to categorize, organize, and describe cybersecurity work. The NICE Cybersecurity Workforce Framework provides educators, students, employers, employees, training providers, and policymakers with a systematic and consistent way to organize how we think and talk about cybersecurity work and to understand requirements of the cybersecurity workforce.

During FY 2018, the NICCS website received major redesigns and enhancements to improve user experience. This redesign includes a new tool allowing human capital managers to build position descriptions using the NICE Cybersecurity Workforce Framework, resulting in 1,988,577 unique page views—a 98.15-percent increase in views from FY 2017. One specific example is the addition of a keyword search utility to the NICE Cybersecurity Workforce Framework, which greatly enhances the accessibility and functionality of the NICCS website for our SLTT users. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 6 Strengthen the Security and Reliability of the Cyber Ecosystem Objective 6.4 Improve Recruitment, Education, Training, and Retention to Develop a World-class Cyber Workforce).*

STOP. THINK. CONNECT. ™ Toolkit

DHS leads the STOP. THINK. CONNECT. ™ (STC) Campaign, which is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The STC Campaign encourages Americans to view Internet safety as a shared responsibility at home, in the workplace, and in our communities. The STC Campaign provides access to resources that give Americans the tools that they need to make more informed decisions when using the Internet.

A key component of the campaign is the STC Toolkit, which provides resources and materials to help promote cybersecurity awareness. The toolkit includes education materials for a variety of audiences, from K-12 students to older Americans to small business owners. During FY 2018, 74 new Campaign Partners joined the STC Campaign:

- 23 Academic Alliance: nonprofit colleges and universities
- 36 Cyber Awareness Coalition: Federal agencies and SLTT governments, including 26 new SLTT partners
- 15 National Network: nonprofit organizations

The STC Campaign held monthly Partner Calls during FY 2018, with more than 1,100 participants, or an average of 91 participants each month. The STC Campaign focused on driving Web traffic to the toolkit and other resources, resulting in the STC Campaign landing page receiving 30.35 percent of all DHS.gov unique page views during FY 2018, which totaled to 49,138 unique page views. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 6 Strengthen the Security and Reliability of the Cyber Ecosystem Objective 6.4 Improve Recruitment, Education, Training, and Retention to Develop a World-class Cyber Workforce).*

National Computer Forensic Institute (NCFI)

The National Computer Forensics Institute (NCFI), located in Hoover, Alabama, is the Nation's only federally funded training center dedicated to instructing SLTT officials in digital evidence recovery and cybercrime investigations. NCFI was opened in 2008 in collaboration with the U.S. Secret Service (USSS), DHS, and the State of Alabama with a mandate to provide state and local law enforcement as well as legal and judicial professionals with a free, comprehensive education on current cybercrime trends, investigative methods, and prosecutorial challenges. With congressional support, NCFI has trained and equipped thousands of state and local police investigators, prosecutors and judges from all 50 states and 3 U.S. Territories. These NCFI graduates represent more than 2,500 agencies nationwide. SLTT agencies benefit from a tuition-free education. In addition, all travel, hotel, and per diem costs are covered by NCFI. Furthermore, students receive the same equipment and software as the Special Agents trained by USSS; a considerable benefit as this equipment and software allows both the local officer and the Federal agent to operate on common systems. Graduates of NCFI return to their respective agencies and apply their newly acquired skills and equipment training to investigating computer-based crimes. Additionally, these graduates are offered the chance to participate in USSS's Electronic Crimes Task Force (ECTF) Program. State and local ECTF members work alongside other Federal agencies to combat the systemic flood of cyber-related crimes through recovering digital evidence for investigation and prosecution. These ECTF members serve as force multipliers by complementing task force participants' skills and equipment.

D. Detect and Prevent

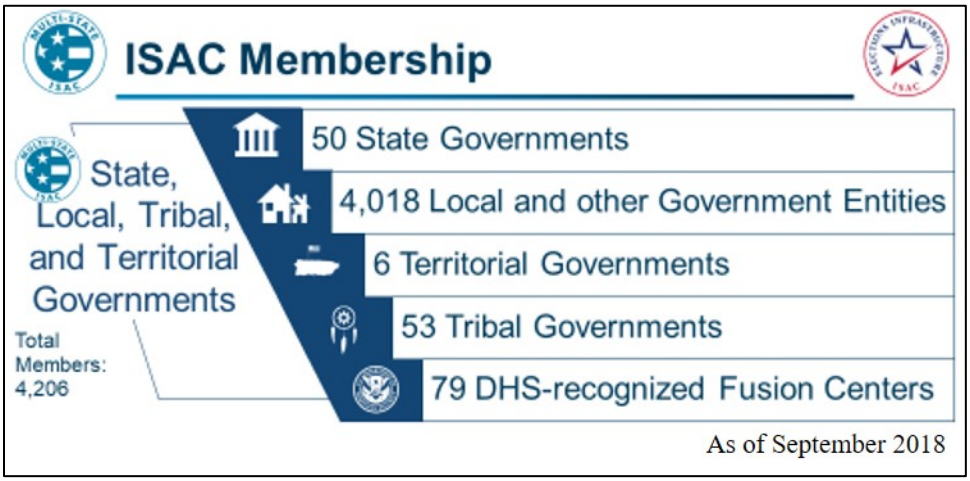
Enhanced Cybersecurity Services

The Enhanced Cybersecurity Services (ECS) program of DHS is an intrusion prevention capability that is available to U.S.-based entities and SLTT governments. DHS partners with service providers that build and maintain systems capable of protecting ECS customer networks against unauthorized access, exploitation, and data exfiltration. ECS follows a managed security service (MSS) model whereby DHS shares sensitive and classified cyber threat information with accredited ECS service providers that then use that information to protect their customers. ECS is meant to augment, not replace, an ECS customer's existing cybersecurity capability. The two ECS service offerings are DNS Sinkholing and Email Filtering. The current accredited service providers include AT&T, CenturyLink, and Verizon. During FY 2018, engagements between the ECS program and SLTT organizations increased following a briefing ECS program leaders provided to participants at the MS-ISAC Annual Meeting in April 2018. As a result, the

program began protecting its first SLTT government entity in FY 2018. There continue to be engagements between SLTT entities and DHS about how ECS can help to augment their network protections.

E. Multi-State Information Sharing and Analysis Center

The MS-ISAC is funded by DHS through a cooperative agreement to provide cyber capabilities and collaborate with SLTT governments on cybersecurity risks and incidents. As of September 2018, MS-ISAC membership exceeded 4,200 organizations—nearly a 300-percent increase from FY 2017—and includes all 50 states.



MS-ISAC takes a layered approached to support SLTT governments, including from general awareness to event notification. During FY 2018, MS-ISAC issued 150 cybersecurity advisories and *Daily Tips* (an emailed publication), as well as hosted 6 bimonthly national webinars. The webinars covered a broad range of topics, including:

- Foundations of an Application Security Program - Cryptocurrencies: the Current Landscape;
- General Data Protection Regulation Compliance: Why should I be Concerned?;
- Excellence in Essentials: Managing Complexity through Foundational Controls;
- Smart Cities; Cybersecurity, and the Intersection of Internet-of-things; and
- National Cybersecurity Awareness Month 2017.

The MS-ISAC also provides timely notification. The following table details the number of event notifications throughout FY 2018:

Notification Type	FY 2017	FY 2018	% Change
Defacement	690	420	-39%
Darknet	656	861	31%
Albert	37,932	57,611	52%
MSS	1,203	4,717	292%
Account Compromise	5,617	4,081	-27%

Spamhaus	8,912	12,490	40%
Vulnerability Management Program	1,082	17,781	1,543%
Total	**56,092**	**97,961**	**75%**

Nationwide Cybersecurity Review

Since 2011, NCSR has provided a no-cost cybersecurity self-assessment that measures gaps and capabilities of SLTT government entities. NCSR is based largely on the NIST Cybersecurity Framework. During FY 2018, MS-ISAC analyzed the survey results and published the 2017 Summary Report. The results of the 2017 NCSR are based on participation from 476 SLTT entities broken down into 45 states, 129 locales (representing 39 states), 5 tribes, and 297 state agencies. NCSR provides insight on the level of maturity and risk awareness of the SLTT's information security programs from year to year. Using the results of this Summary Report, DHS and MS-ISAC will continue to work on improving the overall cybersecurity maturity of the SLTT community with its stakeholders. *(Aligns to the May 2018 DHS Cybersecurity Strategy, Goal 3 Protect Critical Infrastructure Objective 3.2 Expand and Improve Sharing of Cyber Threat Indicators, Defensive Measures, and Other Cybersecurity Information).*

2017 NCSR Key Findings

The following were identified in the 2017 NCSR. DHS is working with SLTT communities to address each gap and build upon success.

1. With the exception of the tribal peer group, the SLTT community continues to exhibit growth in its cybersecurity maturity.

2. Despite continued growth, the SLTT community still has not reached the minimum recommended maturity of "Implementation in Process."

3. The state peer group reached the recommended minimum maturity level of "Implementation in Process" with an average score of 5.01 in the Respond Function.

4. The local peer group, although maturing at a faster rate, continues to lag behind the state peer group in its overall maturity level.

5. It is forecasted that the state peer group will meet the recommended minimum maturity across all of the functions in 2023 and the local peer group in 2024.

6. In analyzing the 2015, 2016, and 2017 data, on average 79 percent of top-level decision-makers are receiving periodic reports on the status of information risks, controls, and/or security from within their organizations.

7. The SLTT community has identified the same top five security concerns over the past three years:
   - Increasing sophistication of threats;
   - Lack of sufficient funding;
   - Emerging technologies;
   - Lack of documented processes; and,
   - Inadequate availability of cybersecurity professionals.

F. FEMA HSGP - Cybersecurity Elements

The NSP builds, sustains, and delivers core capabilities needed to achieve the goal of a more secure and resilient Nation. The development and sustainment of these core capabilities requires the combined effort of the whole community at multiple levels of government. To that end, the FY 2018 HSGP provides funds to support SLTT government efforts to prevent terrorism and other catastrophic events, and to prepare the Nation for the threats and hazards that pose the greatest risk to the security of the U.S.

- **State Homeland Security Program (SHSP):** The SHSP supports SLTT preparedness activities that address high-priority preparedness gaps across all core capabilities that support terrorism preparedness. Cybersecurity is an allowable expense, although not the central focus of SHSP.
- **Urban Area Security Initiative (UASI):** The UASI program assists high-threat and high-density urban areas in efforts to build, sustain, and deliver the capabilities necessary to prevent, protect against, mitigate, respond to, and recover from acts of terrorism. Cybersecurity is an allowable expense, although not the central focus of UASI.
- **Operation Stonegarden (OPSG):** The OPSG program supports enhanced cooperation and coordination among U.S. Customs and Border Protection and Federal and SLTT law enforcement agencies. The OPSG program provides funding to support joint efforts to secure U.S. borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders. Cybersecurity is an allowable expense, although not the central focus of OPSG.

Priorities

The 2017 National Preparedness Report (NPR) identified the following subset of core capabilities as national areas for improvement:

- Cybersecurity;
- Infrastructure Systems;
- Economic Recovery;
- Housing;
- Supply Chain Integrity and Security;
- Natural and Cultural Resources; and,
- Risk Management for Protection Programs and Activities.

Since 2012, states and territories have consistently reported cybersecurity as their least proficient of the core capabilities. In the years between the 2012 and 2017 NPR, almost an equal number of states and territories improved (13) and declined (16) in cybersecurity proficiency, indicating that cybersecurity proficiency still lacks consistency across the Nation. In developing applications for the FY 2018 HSGP, recipients considered funding projects that address core capability gaps, including cybersecurity, within the NPR national areas for improvement to the extent that they relate to terrorism preparedness.

For purposes of SHSP and UASI, FEMA requires states, territories, and urban areas to complete a Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness

Review (SPR) (formerly known as the State Preparedness Report), as well as prioritize grant funding to support closing capability gaps or sustaining capabilities identified in this process. Cybersecurity threats are included in this process.

Consistent with that approach, DHS also included the following new cybersecurity-related requirements in the FY 2018 HSGP:

I. Involve cyber threat and risk management expertise in the grant planning and allocation process;
II. Ensure at least one investment is in support of the state's, territory's, or urban area's cybersecurity efforts;
III. Separately submit the cyber justification that seeks to mitigate a capability gap identified in a cyber assessment; and,
IV. Make available no-cost DHS resources in grant guidance, including no-cost cyber assessments.

Initial Cybersecurity Findings from FY 2018 HSGP

Despite the FY 2018 DHS requirement for states and UASI programs to make stand-alone cyber investments with their preparedness grant dollars, FEMA's initial analysis indicates that overall investment did not increase significantly, and is consistent with previous year investments. Applicants from all 50 states, the District of Columbia, and U.S. territories submitted a total of 91 investment justifications, which covered 223 projects. Cyber-focused investments totaled approximately $36 million, but this figure could fluctuate as CISA continues its analysis and finds cyber-focused projects in other parts of a state and/or UASI programs' complete FY 2018 grant submittal.

Out of the $36 million total in investments, $22 million went toward more tactical cyber initiatives like closed emergency network infrastructure, identity management/access control, encryption software, and firewall enhancements. $14 million went toward strategic initiatives, such as workforce training for Internet and network safety, replacing outdated and inadequate IT infrastructure, developing incident response plans, and funding for cybersecurity-focused positions to manage the cyber program.

Though analysis is ongoing, SLTT cyber investments utilizing HSGP funds still rank below the investments for traditional, physical threats despite the fact that states and territories have rated cybersecurity as the least proficient core capability and the one in greatest danger of decline. SLTT entities make significant investments into cybersecurity using nonfederal funds; however, DHS will continue to utilize the HSGP—and the other forms of support detailed in this report—to guide SLTT agency investment in cybersecurity.

IV. Conclusion

DHS works with SLTT stakeholders to raise the overall level of cybersecurity by assessing risks to SLTT communities, reducing vulnerabilities, preventing and disrupting criminal activity, and, when necessary, responding to cyber incidents. Working with FEMA, CISA is focused on increasing the use of DHS's no-cost services, increasing information and data sharing and analysis, and further clarifying both Federal and SLTT roles and responsibilities during incident response.

Resources such as the NCSR—which saw a record number of respondents—allow CISA to evaluate cybersecurity risks constantly and to prioritize its support to SLTT stakeholders better. By prioritizing based on risk, CISA is able to focus on the most effective methods to reduce risks. CISA will continue to employ a layered approach, leveraging direct, indirect, and self-service models.

CISA and FEMA are working together to formalize the process for how the agencies jointly consider the data points that support the determination of DHS cyber grant priorities. These data points include DHS leadership priorities, threat and risk environment, analysis of the THIRA/SPR, stakeholder input across both CISA and FEMA, and information collected across Cyber Division programs, analysis, and technical efforts. As part of the FY 2019 planning process, CISA and FEMA hope to leverage the FY 2019 President's Budget submission of $522 million for a grant program to address emerging threats and risks, known as the National Priorities Security Grant Program. DHS sent a letter to House and Senate leadership on September 13, 2018, asking for the establishment of this program by amending the Homeland Security Act of 2002. With DHS and White House support, DHS plans to work with the SLTT and cyber elements across DHS to shape the goals and objectives of this grant program around cyber initiatives to fund the continued under-investment in cyber capability across SLTT communities.

Lastly, while CISA works to limit the number of cybersecurity incidents, CISA also must be prepared to respond to incidents when they occur. As such, FEMA and CISA have worked closely to refine incident response procedures, via working with SLTT stakeholders as well as with other interagency partners, to ensure that all relevant parties understand their incident response roles and capacities in the event they are required.

DHS's cybersecurity support to SLTT government entities provides a mechanism to work together as a Nation to build, sustain, and improve our capability in order to prepare for, protect against, respond to, recover from, and mitigate all hazards. These programs are intended to inform SLTT government entities of cybersecurity best practices.

Appendix: Abbreviations

Abbreviation:	Definition:
AIS	Automated Indicator Sharing
CETAP	Cybersecurity Education and Training Assistance Program
CIO	Chief Information Officer
CIS	Cyber Infrastructure Survey
CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cybersecurity Advisors
CRR	Cyber Resilience Review
DHS	Department of Homeland Security
ECS	Enhanced Cybersecurity Services
ECTF	Electronic Crimes Task Force
EII	Election Infrastructure Information
EI-ISAC	Election Infrastructure-Information Sharing and Analysis Center
EPA	U.S. Environmental Protection Agency
FedVTE	Federal Virtual Training Environment
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GCC	Government Coordination Council
HF	High Frequency
HIRT	Hunt and Incident Response Team
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
IT	Information Technology
K-12	Kindergarten through twelfth-grade
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSS	Managed Security Service
NCATS	National Cybersecurity Assessment and Technical Services
NCCIC	National Cybersecurity and Communications Integration Center
NCEPP	National Cyber Exercises and Planning Program
NCFI	National Computer Forensic Institute
NCSAR	National Cyber Situations Awareness Room
NCSR	Nationwide Cybersecurity Review
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NPR	National Preparedness Report
NPS	National Preparedness System
OPSG	Operation Stonegarden
RVA	Risk and Vulnerability Assessment
SHARES	SHAred RESources

SHSP	State Homeland Security Program
SLTT	State, Local, Tribal, and Territorial
SPR	Stakeholder Preparedness Review
STC	STOP. THINK. CONNECT.™
THIRA	Threat and Hazard Identification and Risk Assessment
UASI	Urban Area Security Initiative
USSS	U.S. Secret Service