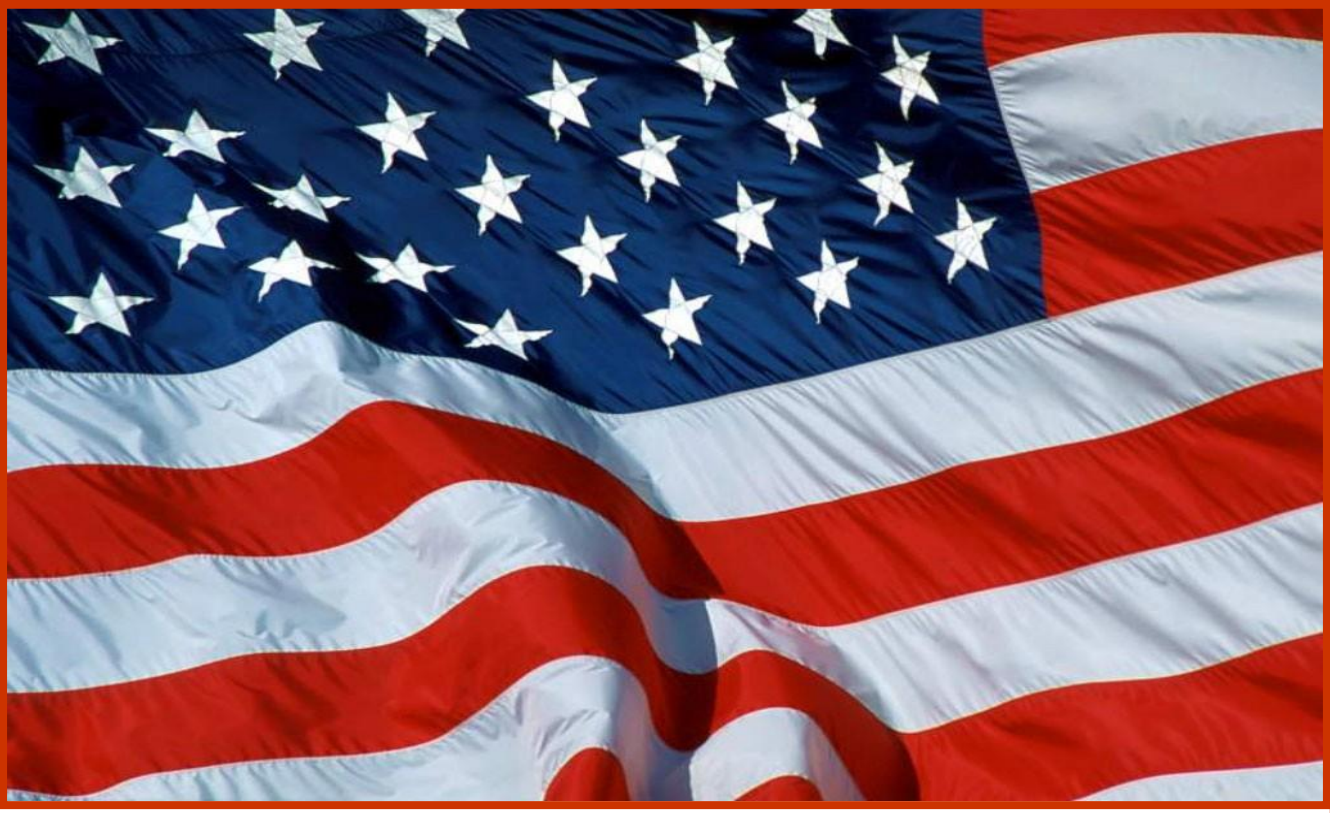

HOMELAND SECURITY ADVISORY COUNCIL

FINAL REPORT OF THE STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY SUBCOMMITTEE

November 14, 2019

This page is intentionally left blank.

This publication is presented on behalf of the Homeland Security Advisory Council, State, Local, Tribal, and Territorial Cybersecurity Subcommittee, under Co-Chairs Paul Goldenberg and Frank Cilluffo and Vice Chair Robert Rose, as the ***final report*** and recommendations to the Acting Secretary of the Department of Homeland Security, Kevin McAleenan.

<SIGNATURE OBTAINED FOR PDF COPY>

Paul Goldenberg (Co-Chair)

Frank Cilluffo (Co-Chair)

Robert Rose (Vice-Chair)

This page is intentionally left blank.

STATE, LOCAL, TRIBAL AND TERRITORIAL SUBCOMMITTEE MEMBERS

Paul Goldenberg (Chair) – President and CEO, Cardinal Point Strategies, LLC
Frank Cilluffo (Co-Chair) – Director, McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University
Robert Rose (Vice-Chair) – Founder and President, Robert N. Rose Consulting, LLC
Art Acevedo – Chief of Police, Houston, Texas
Steve Adegbite – Former Chief Security Officer, Cotiviti Corporation
Keith Alexander – Founder and CEO, IronNet Cybersecurity
Donald P. Dunbar – Major General, Wisconsin National Guard
Jeff Moss – CEO of DEF CON Communications, Inc.
Harold A. Schaitberger – General President, International Association of Firefighters

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Matt Hayden, Executive Director, Homeland Security Advisory Council
Mike Miron, Deputy Executive Director, Homeland Security Advisory Council
Evan Hughes, Associate Director, Homeland Security Advisory Council
Catherine Fraser, CBP Advisor, Homeland Security Advisory Council
Colleen Silva, Staff, Homeland Security Advisory Council
Sarahjane Call, Staff, Homeland Security Advisory Council
Kira Cincotta, Staff, Homeland Security Advisory Council
Cassie Popplewell, Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

EXECUTIVE SUMMARY

Our nation faces serious and evolving cyber threats. As cyber and physical systems become more interconnected, the digital attack surface is extending further into our daily lives, with the potential for malicious cyber actors to create dangerous, real-world effects. Federal, State, Local, Tribal, and Territorial (SLTT) entities must collaborate and coordinate extensively with critical infrastructure private sector owners, operators, and stakeholders to identify and address these cybersecurity challenges.

To strengthen the security and resilience of critical infrastructure, DHS maintains strong partnerships with non-federal public stakeholders and associations (e.g., the National Association of Counties and National Governors Associations). The Department provides appointed and elected SLTT government officials with information and resources to manage cyber risk, to include cybersecurity briefings, information on available resources, and partnership opportunities to help protect citizens online.

To assist DHS in forecasting both threats and opportunities, working with partners, and improving the ability of DHS components to execute mission-critical objectives, the Secretary chartered the State, Local, Tribal and Territorial Cybersecurity Subcommittee of the Homeland Security Advisory Council (HSAC) in the Fall of 2018.

The subcommittee's mandate included, but was not necessarily limited to, addressing the following questions:

1. How can DHS most efficiently and effectively, across all DHS components, support SLTT agencies and partners in pursuing cybersecurity and resilience of their IT infrastructure, to include incident response and recovery?
2. What programs, services, and outreach should DHS prioritize that would provide the greatest benefit to SLTT stakeholders in reducing risks to IT infrastructure?
3. How effective has the Homeland Security Grant Program been in addressing cybersecurity risks at the SLTT levels? How could the Homeland Security Grant Program, including associated grant guidance and technical assistance, be best structured to address cybersecurity risks?

States and localities perform many essential functions, are closest to the problems of citizens, and have unique knowledge about the priorities and economies of their jurisdictions. In cyberspace, they are essential members of the national defense fabric for their own individual well-being, and for sustainment of the nation.

The fight in cyberspace is particularly challenging because non-traditional participants are essential to national security; everyone must play a role, with national goals in mind.

If we expect states and localities to play effectively on the national team, however, we must give

them the tools, training, and capacity to do so. This report provides time-sensitive recommendations appropriate to maturing the SLTT ecosystem now and in the near future.

RECOMMENDATIONS OF THE INTERIM REPORT

Empower Cyber Mutual Assistance for SLTT Entities

DHS should:

- Provide for SLTT stakeholders a single point of contact for cyber response within a reasonable geographic distance of the relevant parties.
- Where reasonable caution points toward enhanced coordination, provide samples of agreements and provide for additional resources for cyber mutual aid that can be put in place.
- Together with States, design and test coordination and response plans, including those that include the SLTT National Guard unit.
- Define clear roles and responsibilities for outreach, communications, and information sharing, as well as for prioritizing and navigating an SLTT cyber alert system.
- Consolidate a set of requirements and path forward for constructing a civilian equivalent to the National Guard cyber-force.
- Establish nation-wide Cyber 211 or 911 programs to provide consistent reporting of cyber incidents around the country.
- Establish a National Cybersecurity Academy to train SLTT government employees.
- Build collaborative partnerships with NGOs focused on training, empowering and developing young people to engage with DHS, and other similar organizations. Provide grants and resources to such organizations to build cybersecurity education programs.

Create a Dedicated Grant Program for SLTT Cybersecurity

DHS should establish a dedicated grant program to support SLTT agencies. Examples of program characteristics should include:

- Baseline capability documents, and associated grant criteria, that will be developed and monitored primarily by the Cyber Security Division of DHS (formerly CS&C).
- Grant awards should be conditioned upon the completion and submission to the grants administering body of assessments, such as the National Cyber Security Review (NCSR) assessment facilitated by the Multi-State Information Sharing and Analysis Center. While states are understandably unwilling to reveal cybersecurity capabilities and posture to a broad audience, the grants committee needs this data to understand the baseline current state and inform investment strategies with targeted improvements.
- Grants structured to permit regional collaboration and coordination, as well as traditional SLTT capability enhancement.

- Grants support for planning, prioritization, information-sharing, and goal assessment aspects of capability development, as well as for the life cycle of key technology. SLTT grant applications will need to articulate how their use of funds addresses both their own needs and their ability to contribute to a national response.
- Receipt of funds will be conditional upon participation and data-sharing for national situational awareness and analytics.

Strengthen Regional Cohesion, Situational Awareness, and Preparedness

DHS should:

- Establish a robust and comprehensive technical assistance program to support cybersecurity capability development. This effort should include development of model policies, guideline documents, best practices, workshops, how-to guides and other resources for SLTT agencies of all levels of maturity.
- Design a consistent SLTT customer management system, re-organize the website for consistency and ease of use, better organize description of services, implement a marketing and communications strategy leveraging SLTT associations and partners, improve tailored education and training programs, and enhance incident response capabilities.
- Identify the characteristics of strong regions, what leads to these characteristics, and apply this knowledge to other regions to help increase their strength.
- Support regional planning and resilience as part of the grants program.

Enable Fusion Centers to Provide Greater Cyber Situational Awareness

DHS should:

- Work in partnership with the Intelligence Community to increase the availability of intelligence training for SLTT cyber analysts.
- Support the National Network of Fusion Centers Cyber Intelligence Network (CIN) community on HSIN by having the NCCIC provide overnight management. Most fusion centers are not operating 24/7 and providing this much needed coverage will greatly improve situational awareness.
- Define cyber requirements to augment existing, predominantly law enforcement, fusion center capabilities. Train and expand the PSA program to include Cyber as an available resource.
- Explore whether fusion centers can be used as SLTT Cyber Security Operations Centers in areas that do not have SOCs.
- Support and train to equip fusion centers in this way.
- Review/update/expand guidance documents such as Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major

Urban Area Fusion Centers.[1]

Equip State and Local Election Officials to Identify and Counter a Comprehensive Range of Threats

DHS should:

- Create and sustain a consolidated portrait of Threat across the entire threat surface, including informational arenas, so that key stakeholders from any part of the ecosystem can understand what the nation faces and the interconnected nature of technology, information, influence, and election outcomes.
- Empower and fund SLTT Election officials to identify and defend against threats to the election system.
- Identify the gaps in current mitigation strategy and provide support in ways that SLTT Election officials can use.

Manage the Risks Introduced by Smart Cities

DHS should:

- Assess current and planned deployments of Smart Cities throughout the United States.
- Define a path to create mechanisms for managing cyber/cyber-physical risk in Smart Cities.
- Evaluate risks to public safety and critical infrastructure function associated with these deployments and plans.
- Inventory known or suspected cybersecurity incidents in Smart Cities globally to act as a corpus of knowledge to help better inform Smart City planners, regulators, and insurers.

[1] See https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers.

This page is intentionally left blank.

STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY

1.1 Background and Context

State, Local, Tribal, and Territorial (SLTT) cyber capabilities lag the corresponding threat and DHS is uniquely suited to help. Doing so serves both the individual SLTT entities and the broader national interest.

The Secretary of DHS has tasked the Homeland Security Advisory Council with making recommendations for action by DHS to address this critical national challenge.

1.1.1 The Department of Homeland Security's (DHS) Role

The Department of Homeland Security (DHS) has an enabling, rather than regulatory, role in cybersecurity for the SLTT community. (This is akin to the Department's enabling role regarding Critical Infrastructure Protection.)

DHS has embraced its cyber role by convening the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC)2, supporting the community activities of the Multi-State ISAC (MS ISAC), recruiting and placing Cyber Security Advisors (CSAs) in most regions, and creating a body of products (available on the Homeland Security Information Network and in other more public zones) and self-assessments that can be used by SLTT stakeholders as well as Critical Infrastructure owners and operators.3

The MS-ISAC provides situational awareness through a steady stream of Indicators of Compromise (IoC) and threat alerts to all fifty states including thousands of localities. DHS provides assistance in coordinating incident response, vulnerability assessment and malicious code analysis upon request.4

The DHS Cyber Security Division[5], or CSD, has two important divisions related to SLTT Cyber: the National Cybersecurity and Communications Integration Center (NCCIC), which fulfills a range of outreach and information sharing needs, including national cyber incident response; and the

---

[2] Note that leadership for SLTT activities resides in different organizations for different purposes; some SLTT stakeholders find this confusing and ask for "a single POC for all SLTT activities." The SLTTGCC falls under the overarching Critical Infrastructure governance approach, in the Infrastructure Security Division of CISA; the MS-ISAC and Election ISAC are run by SECIR; FEMA handles incident response generally, but the NCCIC is the lead for national cyber response.

[3] An example of a commonly used tool is the Cyber Security Evaluation Tool, or CSET. It can be used by stakeholders in industrial control industries, with or without federal assistance. This kind of tool can be useful to both SLTT stakeholders and private industry, as applicable. See ics-cert.us-cert.gov

[4] See cisecurity.org for an overview of services offered by the MS-ISAC.

[5] Note: CSD may experience organizational and naming shifts as it refreshes operations pursuant to the renaming and refocusing taking place as a legacy of the now-defunct National Protection and Programs Directorate (NPPD) and the standup of the new Cybersecurity and Infrastructure Security Agency (CISA). Unit, branch, and organization names are current as of January 5, 2019.

Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) branch, which supports a wide range of cybersecurity activities across the SLTT communities. SECIR plays a unique role within DHS, acting as a partner to SLTT communities in promoting cybersecurity and helping bolster SLTT communities' cyber preparedness. SECIR's mission is to "initiate and sustain strategic critical infrastructure (CI) and…SLTT partnerships to develop approaches for longer cyber risk management," as well as to "engage SLTT and CI partners to implement comprehensive but specific cyber preparedness and protective activities, [and] perform outreach and education activities and advocate for DHS cyber capabilities."[6] In support of its mission, SECIR regularly engages its partners on cyber preparedness and protection activities and raises awareness about DHS cyber capabilities.

Outside of CSD, two other DHS components play significant roles on the cyber front with the SLTT enterprise:

- The Federal Emergency Management Agency (FEMA) – which has lead responsibility for responding to the physical aspects of national emergencies. Bear in mind that cyber events can result in physical consequences; and
- The Office of Intelligence and Analysis (I&A) – which is DHS' official intelligence lead and the management locus for state and local Fusion Centers.

Although other parts of DHS may be involved in cybersecurity of the SLTT community,[7] CSD, FEMA, and I&A are the most consistently engaged.

As much as the federal government has recognized the need for and pursued aid to the SLTT ecosystem, the threat continues to outpace progress. Increased resilience and coordination are called for in today's evolving threat environment: a bad actor may hit Washington state while preparing to target Richmond, VA, and under current conditions the SLTT ecosystem would not have a systematic way to be notified in advance. In acting to blunt the threat, moving forward, the United States must invest for the highest return, to the benefit of both SLTT and U.S. national security.

1.1.2 Cybersecurity Today in the SLTT Ecosystem

Every day, states, localities, tribes, and territories rely on networks and systems to ensure continuity of government and delivery of mission-critical services. These systems are at risk of disruption from cyberattacks by adversaries and from natural catastrophic events. Addressing these risks requires a mix of capabilities that includes government, civilian and commercial actors. States govern cybersecurity in a variety of ways, from more centralized to heavily decentralized;8 given the size of the state, the precedents around how government runs more

[6] See https://www.dhs.gov/cisa/stakeholder-engagement-and-cyber-infrastructure-resilience.

[7] Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI), for instance, are frequently involved in law enforcement activity related to cybersecurity. Law enforcement engagement, however, indicates that damage has already been incurred; whereas the primary focus of this document is strengthening SLTT so that incidents may be better prevented and managed.

[8] See https://www.dhs.gov/cisa/cybersecurity-governance for both individual analyses and cross-state comparisons of

generally, and the diversity of technical maturity levels, there is no single option that suits all states (or localities) equally.9

In addition to state-focused governance and operations, many local governments are seeking ways to leverage the digital environment to enhance service delivery to their citizens. This includes expanding local governments' presence and offerings on the Internet and/or integrating information and communications technology (ICT) into their approaches to service delivery. This increased reliance on cyber and communications systems may improve local government efficiencies in novel ways. However, an increased digital footprint, coupled with the rise in incidents of cyber threat actors targeting local governments, also heightens local governments' risk. The disruption of systems responsible for key service delivery and critical infrastructure functions can have dangerous local impacts. State and local governments need help to better understand the risks and coordinate with others to better enhance their cybersecurity posture to ensure the safety, security, and integrity of their IT and smart city projects.

If the federal government is the warp of the national fabric, states, localities, and Critical Infrastructure are the weft. Strong fabric requires strong thread, consistently woven, in both directions. Today, states need more. More assistance, more funds, more capacity, and more assistance during disruption.

This document details six key actions to enhance SLTT cybersecurity.

1.2 Six ways DHS can support states to improve SLTT capabilities

By identifying and leveraging zones of excellence within a range of functions and geographic constructs, DHS can raise the baseline for SLTT cybersecurity and enhance cybersecurity for the nation. DHS can support states by improvement in these six ways:

- **DHS can empower cyber mutual assistance for SLTT entities**. SLTT stakeholders can benefit from strong cyber mutual assistance agreements, plans, and exercises. Those with greater capabilities can help the less robust SLTT stakeholders.
- DHS can create a dedicated grant program for state cybersecurity, and support raising the defined baseline through bulk purchase vehicles for commonly used cyber essentials. The SLTT community can achieve a higher baseline of cybersecurity in a more efficient manner if they can readily access a pre-negotiated, cost-effective body of basic hygiene and other essential offerings.
- **DHS can strengthen regional resilience, situational awareness, and preparedness.** Disasters do not respect state lines: cyber compromise can halt

cyber governance.

[9] Some evidence in the National Cyber Security Review, described later in this report, appears to point toward a higher level of cybersecurity maturity in centralized governance environments. This is extremely preliminary and requires further investigation and analysis.

functionality[10] without heed for geography, and natural disasters tend to have regional impact. States and localities are stronger when they share awareness and resources, thereby fostering resilience beyond any individual legal jurisdiction.

- DHS can empower existing Fusion Centers to become centers of cyber situational awareness and Security Operations Centers (SOCs) for the SLTT ecosystem. While some states have sophisticated cyber programs, many still need a focal point for understanding and assessing the cyber threat.
- DHS can unify efforts to empower SLTT election officials more comprehensively and to protect the nation's election infrastructure.
- **DHS can lead the nation toward managing the risks introduced by Smart Cities.** Many cities are adopting smart technology without understanding and managing the risks that these new technologies present to public safety and critical infrastructure functions.

1.2.1 DHS Can Empower Cyber Mutual Assistance for SLTT Entities

SLTT stakeholders can benefit from strong cyber mutual assistance agreements, plans, and exercises. Mutual assistance is a longstanding construct in the physical world. When a hurricane or earthquake disrupts life in Florida or California, trained and equipped fleets of backup energy personnel and equipment complement efforts by FEMA and other government responders.

DHS has moved to provide as much assistance as resources permit: capability now housed within the Cybersecurity and Infrastructure Security Agency (CISA, formerly NPPD) supports a limited number of fly-away teams for incident response. However, the volume and magnitude of national cyber issues that impact SLTT entities continues to grow. Just as state and regional incidents in the physical world are dealt with by FEMA, states, and private surge arrangements for mutual aid so too should cyber challenges be handled effectively through a spectrum of arrangements. The most consequential cyber challenges require resources beyond the capacity of the federal government or that of a single state.

DHS can help the SLTT community create surge capacity by enabling and facilitating resource identification and awareness across multiple states and standardizing the ways to negotiate, document, operationalize, and test cyber mutual aid arrangements.

Several commentators have recommended reliance on the National Guard for surge capacity. The National Guard can, in certain circumstances, provide useful assistance. Some areas, such as the Boston region, have explored this option in exercises (Cyber Yankee, in this case).

Two issues are essential to address in conjunction with this option. First, not all National Guard

[10] Rather than focusing on networks, systems, or assets, much of the homeland security risk dialogue now focuses on essential functions. Essential functions are things like the provision of water, power, transportation, and healthcare to the population—all enabled today by connected digital systems.

units have relevant capabilities; the core assumption that they can help needs to be either validated or ruled invalid. Second, leveraging the National Guard could create a potentially crippling, unintended side effect: private sector personnel who are cyber professionals and simultaneously members of the National Guard may be detailed away from performing equally critical cyber response on the private sector side.[11] Communications networks, electricity, and other critical infrastructure functions must remain supported in order for SLTT networks to serve their intended functions. The intertwined nature of public and private cyber infrastructure and response capabilities requires further study; the National Guard alone can provide a portion of a solution, and the solution can be made robust through mutual aid and the creation of a parallel, civilian force.

In addition to providing considerations, examples, best practices and lessons learned to states seeking to fold National Guard units into surge capacity, DHS should consider building a civilian equivalent to the Guard.

Recommendations:

- Provide structured, supported forums and the communication mechanisms for SLTT stakeholders to identify single points of contact and resources for cyber response within reasonable geographic access of the relevant parties.
- Where reasonable caution points toward enhanced coordination, provide samples of agreements and provide for additional resources for cyber mutual aid that can be put in place.
- Inform/design, execute, test, and exercise these plans and agreements as requested by the participating states and/or localities.
- Define clear roles and responsibilities for outreach, communications, sharing information, prioritizing and navigating an SLTT cyber alert system.
- Consolidate a set of requirements and path forward for constructing a civilian equivalent to the National Guard cyber-force.
- Establish nation-wide Cyber 211 or 911 programs to provide consistent reporting of cyber incidents around the country.
- Establish a National Cybersecurity Academy to train SLTT government employees.
- Build collaborative partnerships with NGOs such as the National Police Athletic League and other similar organizations focused on training, empowering and developing young people to engage with DHS, and other similar organizations. Provide grants and resources to such organizations for the purpose of building cybersecurity education programs.

1.2.2 DHS Can Create a Dedicated Grant Program for State Cybersecurity, and Support Efforts to Raise the Defined Target Baselines through Bulk Purchase Vehicles for Commonly Used

[11] This potential risk requires careful de-confliction by the National Guard of available skills and the relative response value of maintaining day-job performance versus National Guard service. The issue was flagged by DHS several years ago for further study.

Cyber Essentials

The SLTT community can achieve a higher baseline of cybersecurity more efficiently if it can:

- Clearly identify the target(s) for cybersecurity improvement.
- Fund development of the target(s).
- Readily access pre-negotiated, cost-effective vehicles by which to acquire or ensure basic hygiene and other essential offerings.

According to some estimates, 80 percent of cyber incidents can be prevented through effective establishment and maintenance of basic hygiene. Basic hygiene includes measures such as the 20 Critical Controls.[12] The federal government is in the process of ensuring that all agencies

1. Have a methodical, consistent definition of high-value assets (HVAs), and
2. Have deployed the 20 Critical Controls, through the Continuous Diagnostics and Mitigation (CDM) program.

In the federal civilian CDM program, a single office takes responsibility for vetting products that provide the required capabilities and for creating contract vehicles so that all federal agencies can make purchases from an already approved list.

A baseline set of capabilities for states and localities could reasonably include the capabilities currently established as targets for federal agencies. Data feeds from states and localities, then, can aim at the most essential priorities (HVA) and can begin to inform dashboards of activity (CDM) for national situational awareness.

DHS can help the SLTT ecosystem raise baseline cybersecurity by pre-positioning bulk purchase contracts that SLTT stakeholders can leverage as they see fit, covering capabilities that everyone needs. These capabilities might reasonably include:

- Basic hygiene/20 Critical Controls
- Penetration testing and remediation assessment
- Incident response and resilience
- High-value asset assessment and related security planning

To complement the establishment of bulk vehicles, DHS needs to enable states to take advantage of these vehicles through dedicated grants. In general, states and localities do not have resources or a workforce that match those of the federal government. Even with resources and considerable access to skilled workers, the federal government faces continuing cybersecurity challenges. States and localities face these same challenges, made more daunting by the gap in funds.

FEMA has years of accumulated institutional knowledge in administering grant programs. Large grant programs, such as the Homeland Security Grant Program and the Urban Area Security

[12] See, for instance, NIST 800-53: https://nvd.nist.gov/800-53/Rev4. Things like software and hardware inventory, access control, and privilege management fall into this category.

Initiative, have served the SLTT ecosystem since the earliest days of DHS. Perhaps because cyber expertise resides elsewhere, or for other reasons, DHS grant programs to date have focused primarily on physical aspects of preparedness, protection, and resilience rather than the cyber aspects of same.[13]

Cybersecurity is a team sport; all players need core skills. One leverage opportunity exists in adapting a well-known approach to this new arena. When Fusion Centers (FCs) were initially established, grants were provided to SLTT stakeholders to build and enhance the baseline capabilities of FCs. Grant criteria were targeted to the development of specific capabilities that helped the SLTT stakeholders and were intended to enable them to contribute to national situational awareness, threat identification, and mitigation.

The MS-ISAC conducts an annual, voluntary survey across the SLTT ecosystem. This survey, the National Cyber Security Review (NCSR), shows an increase in incident response capability for states, but also shows consistent gaps in SLTT cybersecurity.14 To head toward measurable increases in cybersecurity for the SLTT ecosystem, the grants process should condition receipt of funds upon a form of measurement of success. The NCSR is an obvious option. Providing NCSR scores as part of the funding application and ensuring that post-grant reporting of NCSR scores is required as part of grant compliance, is one way to head toward gauging improvements.15

Capturing the key elements in this section, the HSAC should consider recommending the establishment of a dedicated grant program to support SLTT cybersecurity.16 Examples of program characteristics should include:

- Baseline capability documents, and associated grant criteria, to be developed and monitored primarily by the Cyber Security Division (formerly CS&C).
- Grant awards conditioned upon the completion and submission to the grants administering body of assessments, such as the National Cyber Security Review (NCSR) assessment facilitated by the Multistate ISAC. While states are understandably unwilling to reveal their cybersecurity capabilities and posture to a broad audience, the grants committee needs this data to baseline current state capabilities and inform investment strategies with targeted improvements.
- Grant support for planning, prioritization, information-sharing, and goal assessment aspects of capability development, as well as for key technology

[13] Given the convergence of cyber effects into the physical realm, such distinctions are becoming less viable. At present, however, many mental constructs and organizational designs perpetuate the division.
[14] See https://www.cisecurity.org/ms-isac/services/ncsr/.
[15] Self-assessment is neither independent nor verifiable; at this time, the expert community maintains enough concern that mandatory independent assessments are overly burdensome for the SLTT ecosystem and would significantly deter participation in grant applications.
[16] A more aggressive model is being explored in a pilot project with Defense Industrial Base companies and merits a close watch by DHS for potential use with SLTT stakeholders, as well. The DIB cloud pilot – a cloud offering that standardizes key security practices at a higher uniform level than is currently achieved – is in the design phase with the DoD CAPE community. An exploratory discussion between DHS and DoD is likely to be timely in fall 2019.

acquisition. SLTT grant applications will need to articulate how their use of funds addresses both their own needs and their ability to contribute to national capabilities.

- Receipt of funds conditional upon participation in and data-sharing for national situational awareness and analytics.
- Grants structured to permit regional collaboration and coordination, as well as traditional SLTT capability enhancement.
- One focus area for baseline capabilities could be the enhancement of Fusion Centers to serve as cyber coordination and fusion centers for the local stakeholders, as described in the Fusion Center discussion above.

1.2.3 DHS Can Strengthen Regional Cohesion, Situational Awareness, and Preparedness

Disasters unfold organically. The geographic impact of a cyber, physical, or cyber-physical catastrophe cascades across connected networks, water systems, transportation networks, electricity grid segments, and other regional constructs.

States and localities are stronger when they know of, and can rely upon, a fabric of shared situational awareness and resources that fosters resilience beyond any individual legal jurisdiction; and which is based upon the natural geography and relationships that sustain population centers.[17]

Both FEMA and CISA have regional subdivisions. FEMA staffs and prepares for disaster at the regional level; and CISA is beginning to take a similar approach. This is a result of DHS' recognition that a DC-based program, on its own, cannot generate national resilience. The United States is too large (and varied) for this, and effective application of national frameworks often requires a tailored and decentralized approach.

Just as some states are leaders among their peers, some regions are stronger than others. The Pacific Northwest Economic region (PNWER) developed organically across Washington, Oregon, parts of British Columbia, and elsewhere, to surface and address shared equities of the public and private sectors that are unique to the region.[18] Recognition that impacts from cyberattacks, economic crises, and natural disasters will create region-wide consequences led these stakeholders to develop this kind of shared-responsibility and planning model that can be usefully translated to other regions as well.

At this time, DHS' embedded cyber personnel and services for both states and regions are less richly resourced than personnel and services related to physical planning, preparedness, and response. Given the threats the United States faces, it is essential to homeland security that national leaders identify and support the widespread propagation of technical tools, joint planning, and best practices for situational awareness, preparedness, and resilience in both states and regions.[19] DHS should expand their cyber-focused field presence (Cybersecurity Advisors) and complement them with a robust and comprehensive technical assistance program to support cybersecurity capability development. This effort should include development of

---

[17] See, for instance, *Critical Infrastructure Resilience: A Regional and National Approach.* https://www.mitre.org/sites/default/files/publications/14-4047-critical-infrastructure-resilience-a-regional-and-national-approach.pdf. Existing regional outreach is described in DHS CISA's fact sheet, which can be found at https://www.dhs.gov/publication/ip-regional-service-delivery-model-fact-sheet.

[18] See http://www.pnwer.org/ for more information on this leader in regional approaches.

[19] Worth noting is the debate about the definition of "region." FEMA regions are standardized blocks of states that are relatively evenly distributed around the nation. This is one way to define a region. Regions that are organic because of geography, population centers, or shared critical infrastructure look different from a FEMA region: a region for managing water issues on the West coast, or a region for providing healthcare to the dense population in the Boston urban area, can be larger, smaller, more complex, or focused on specific core issues. Effective partnerships with SLTT stakeholders will involve acknowledging the differing, organic definitions of regions as SLTT perceives them.

model policies, guideline documents, best practices, workshops, how-to guides and other resources for SLTT agencies of all levels of maturity.

Recommendations:

- Identify the characteristics of strong regions, identify what leads to these characteristics, and help other regions organize and become stronger.[20]
- Support regional planning and resilience as part of the grants program.
- Establish a robust and comprehensive technical assistance program to support cybersecurity capability development. This effort should include development of model policies, guideline documents, best practices, workshops, how-to guides and other resources for SLTT agencies of all levels of maturity.
- Design a consistent SLTT customer management system, re-organize the website for consistency and ease of use, better organize description of services, implement a marketing and communications strategy leveraging SLTT associations and partners, improve tailored education and training programs, and enhance incident response capabilities.

1.2.4 DHS Can Empower Existing Fusion Centers to Provide Greater Cyber Situational Awareness for SLTT

Some states have sophisticated cyber programs, but many states still need a focal point for understanding, assessing, and countering the threat. SLTT Fusion Centers across the nation have provided invaluable homeland security and law enforcement services since their founding circa 2008. Today, there are 79 state and major urban area Fusion Centers (FCs) nationwide.

The first set of capabilities that FCs developed in accordance with the Baseline Capabilities for State and Major Urban Area Fusion Centers (September 2008) were: planning and requirements development; information gathering/collection and recognition of indicators and warnings; processing and collation of information; intelligence analysis and production; and intelligence/information dissemination. FCs then matured through several increments. The first maturation to the baseline capabilities began with the guidance in Critical Infrastructure and Key Resources (CIKR) Protection Capabilities for Fusion Centers (December 2008). Another maturity increment came following adaptations made to FCs based on the May 2015 guidance named Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers.

However, since cybersecurity threats have now been identified by the Director of National Intelligence as the most serious national and economic security threats facing the nation, it is time to significantly improve upon prior guidance to FCs.[21]

[21] See, for instance, http://www.govtech.com/security/Director-of-National-Intelligence-Digital-Threats-to-United-States-Are-Mounting.html.

The concept advanced here is to build cyber-specific intelligence capabilities at FCs. By expanding their capability to incorporate cybersecurity threats, FCs can better support public-private problem-solving to protect government institutions and functions, critical infrastructure service providers, economic-magnet businesses, and citizens that live and work within the jurisdiction from disruptive and damaging cyberattacks.[22]

In order to support this effort, DHS should take the following steps:

Recommendations:

- Work in partnership with the Intelligence Community to increase the availability of intelligence training for SLTT cyber analysts.
- Support the National Network of Fusion Centers Cyber Intelligence Network (CIN) community on HSIN by having the NCCIC provide overnight management. Most fusion centers do not operate 24/7; providing this much-needed coverage will greatly improve situational awareness.
- Define cyber capabilities to augment existing fusion center (predominantly law enforcement) capabilities, train and expand the PSA program to include Cyber as an available resource.
- Explore whether fusion centers can be used as SLTT Cyber Security Operations Centers in areas that do not have SOCs.
- Support and train to equip fusion centers in this way.
- Review/update/expand guidance documents such as Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers.[23]

In summary, intentionally expanding dedicated focus and cyber capacity within SLTT Fusion Centers is recommended to help ensure that public and private constituents within states can collaboratively improve risk management in the evolving cyber threat environment.

1.2.5 DHS Can Unify Disparate Efforts and Empower SLTT Election Officials More Comprehensively, to Protect the Nation's Elections and Constitutional Democracy

Russia compromised U.S. election systems and informational integrity in 2016. Elections, one of the most essential underpinnings of democracy, are conducted by states, counties, and cities.24

[22] Note as well that Fusion Centers may provide a natural focal point for addressing one important challenge in cyber defense: the language and culture of cyber professionals and law enforcement professionals are different and often clash. The challenge of streamlining collaboration across these cultures is an important aspect of effective situational awareness and national defense.

[23] See https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers.

[24] The Constitution, Article I, Section 4, allows Congress to set time-place-manner terms for elections, but as a general matter, elections have been left to states.

Election security is incredibly complex. Elements of security range from purely technical, to managerial, to informational. The public sector (e.g., election officials, the Intelligence Community) is responsible for carrying out elections; the private sector (e.g., social media, equipment vendors) creates the equipment on which votes are recorded and has an unmeasured capacity to shape how people engage with elections.

Today, CISA and CSD focus on cybersecurity/technical threats to elections, as does the National Association of State Election Directors, the National Association of Secretaries of State, the Federal Bureau of Investigation, and the National Security Agency. (Others do too; this is just a high-level list.)

Today, ICT threats to elections are the focus of much attention and progress on election security is being demanded by multiple quarters. However, the threat to elections stretches well beyond Information and Communications Technology, to include information and disinformation, outside influence and disproportionate amplification. The election ecosystem is under siege, with information, incentives, and access contorted in a variety of complex ways.

The integrity of the election process is not cleanly captured by traditional cybersecurity frames.25 Instead, it is important to assess how the system overall might be undermined. The main mechanisms for undermining system confidence are sometimes called "The Four Ds": Divide, Doubt, Discredit, and Distract. Adversaries' goals in elections can include dividing the population, often by amplifying existing conflict; sowing doubt by undermining faith in U.S. democratic institutions; or discrediting candidates and the electoral process, which can delegitimize the winner of an election and divide the population. All of this creates chaos and confusion, distracting the public from focusing on an adversary's other actions, which is often also a goal of adversaries.

With these goals in mind, an adversary can use a range of techniques. Four primary ways that an adversary can affect an election are:

- manipulating who can vote,
- directly altering cast votes,
- undermining the integrity of the electoral process, or
- influencing voters to cast their votes in favor of a certain candidate or policy.

These techniques can involve elements of both IT and informational systems.

Election infrastructure can be described as falling generally into one of four groups:

- voter registration,[26]
- pollbooks and voter check-in,

[25] i.e., CIA: Confidentiality, Integrity, Availability.

[26] During the 2016 presidential election cycle, adversaries successfully attacked voter registration systems, and it has been alleged that other components were also compromised.

- voting machines and tabulation systems, or
- election night reporting.

In addition to the manipulation of election infrastructure, a dominant mechanism for manipulating the system as a whole—and, therefore, undermining faith in this core democratic process—is cyber-enabled foreign influence operations. For example, if an adversary wishes to discredit a candidate, they might use a cyberattack to steal private emails, leak those emails via the internet, and use social media to shape and amplify public perception of the emails.

While many of the infrastructure elements are themselves owned and operated by state and local officials, the overall ecosystem in which foreign influence maneuvers occur is owned and operated largely by private companies. All the relevant pieces today remain largely uncoordinated.

The SLTT Cybersecurity subcommittee urges that DHS focus on understanding, coordinating, and creating holistic solutions across a fragmented space to support the integrity of operations at the state and local level.

Like baseline cybersecurity capabilities that help both states and the nation achieve shared situational awareness (as described in the section on grants, above), the goal related to Election Security includes increasing national situational awareness. Moving in this direction requires equipping and training Election officers across the SLTT ecosystem. Today, a range of cybersecurity capabilities exist that can be used by SLTT Election officials; but a full complement of capabilities to address a threat that spans cyber and information/influence operations remains undefined and undeveloped.

Recommendations:

- Create and sustain a consolidated portrait of Threat across the entire threat surface, including informational arenas, so that key stakeholders from any part of the ecosystem can understand what the nation faces and the interconnected nature of technology, information, influence, and election outcomes.
- Empower and equip SLTT Election officials to defend, as appropriate, against all threats. Europe and Latin America have started down the path of figuring out how to instruct Election officials to deal with influence operations; we must as well.
- Identify the gaps in mitigation capability across the entirety of the Threat. Using a systems view, support strategic alliances—not specific vendors and products—to problem-solve in ways that SLTT Election officials can use.

1.2.6 DHS Can Lead the Nation Toward Managing the Imminent Risks Introduced by Smart Cities

Many cities are adopting Smart City technology without understanding and managing the risks

that these new technologies present to public safety and critical infrastructure functions.[27] Cities are embracing technology that enables operational efficiency for important functions, which, along with associated cost savings, appeal to officials and taxpayers alike.

At the same time, however, migrating to the Smart City model can bring risks. At face value, smart parking meters do not pose a risk to public safety. However, smart parking meters that are run on management systems shared by a central oversight program, or connected to a transportation coordination center, could implicate the functioning of traffic lights or first-responder dispatch. Without awareness, analysis, correct configuration, and mitigations in place, smart parking meters could place public safety in jeopardy.

Enabling Smart Cities is a natural priority for the Departments of Commerce, Transportation, and others. Unfortunately, surfacing, assessing, and managing Smart City risk has not been equally elevated. Smart City risks to essential functions and citizen-safety fits within the DHS mission.

To the extent that Smart Cities implicate essential functions of critical infrastructure and public safety, DHS is the logical leader.

Recommendations:

- Assess current and planned deployments of Smart Cities throughout the United States.
- Define a path forward to create mechanisms for managing cyber risk in Smart Cities.
- Evaluate resulting or foreseeable risks to public safety and critical infrastructure functions associated with these deployment and plans.
- Inventory known or suspected cybersecurity incidents in Smart Cities globally.

The nature of appropriate mechanisms cannot be described without a precursor investigation such as the one described. Almost certainly, interagency coordination will be required; other potential aspects of a program could include risk management guidelines, conditions upon grant awards, education and outreach, and collaboration with the vendor ecosystem.[28] The approach should be informed and driven by the data on deployment models, grants, options for vulnerability disclosure and threat intelligence sharing, and other research findings.

[27] As an example, consider the case of Columbus, Ohio. In 2015, Columbus won a $40 million grant from the federal Department of Transportation to create Smart City capabilities. See https://www.columbus.gov/smartcity for Columbus' description of activities and progress. The criteria for the grant, and the grant submitted, do not address cybersecurity.

[28] The range of options might include a technical assistance program like that operated today by the NCCIC for ICS generally. Architecture review and Red Teaming in advance of deployment could be valuable, as knowledge and capability grow in this area.

This page is intentionally left blank.

APPENDIX A – PANEL MEMBER BIOGRAPHIES

Paul Goldenberg (Chair)

Paul Goldenberg is the President and CEO of Cardinal Point Strategies (CPS), LLC, a strategic advisory and business intelligence consulting firm. Mr. Goldenberg also served as the past CEO and National Director of the Secure Community Network, the nation's first faith-based information sharing analysis center recognized by DHS as a national model. Mr. Goldenberg's public career includes more than two decades as the first State Chief of the Office of Bias Crimes and Community Relations in New Jersey leading the nation's first full time State Attorney General's effort focusing on hate crimes and ethnic terrorism, Director of the nation's 6th largest county social service and juvenile justice system, and as a law enforcement official leading investigation efforts for cases in domestic terrorism, political corruption, and organized crime. From 2004- 2009, Mr. Goldenberg played a key role in setting policy for the legislation and investigation of ethnic terrorism and hate crimes in his role as senior law enforcement advisor to the Organization for Security and Cooperation in Europe. In the course of his law enforcement career, Mr. Goldenberg received South Florida's most distinguished citation for valor, Officer of the Year, an honor presented after serving as lead agent in one of South Florida's longest-term undercover assignments.

Frank Cilluffo (Co-Chair)

Frank J. Cilluffo directs the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. Prior to joining Auburn, Cilluffo founded and directed the Center for Cyber & Homeland Security at George Washington University where he led several national security and cybersecurity policy and research initiatives. Cilluffo previously served as Special Assistant to the President for Homeland Security. Immediately following the September 11, 2001 terrorist attacks, Cilluffo was appointed by President George W. Bush to the newly created Office of Homeland Security. Before his White House appointment, Mr. Cilluffo spent eight years in senior policy positions with the Center for Strategic & International Studies (CSIS), a Washington-based think tank.

Robert Rose (Vice-Chair)

Bob Rose is a recognized expert providing the U.S. government and companies strategic counseling and governance on a full array of cyber-related issues at the nexus of technology, national security, and privacy. He currently serves as Executive Vice President for Strategic Planning of 1Kosmos and is a member of its Advisory Board and as Senior Adviser to the Chairman of Securonix and is a member of its Advisory Board. Additionally, Bob is a member of the U.S. Department of Homeland Security's Homeland Security Advisory Council. Current corporate and non-profit advisory board service include CrowdStrike Services, The Chertoff Group, the Homeland Security Experts Group (formerly the Aspen Institute Homeland Security Group), Cyber Florida, Plurilock Security Solutions, and the George Washington University Center for Cyber and Homeland Security.

Bob previously served as a senior advisor to the Chairman of Bridgewater Associates, and was an Advisory Board member of the National Security Agency's (NSA) Cyber Awareness and Response Panel, the Department of State's International Security Advisory Board, the National

Counterterrorism Center (NCTC) Director's Advisory Board, and the Director of National Intelligence's (DNI) Financial Sector Advisory Board. Bob has received numerous honors and awards, including: a presidential appointment to the J. William Fulbright Board of Foreign Scholarship, a fellowship with the Wexner Heritage Foundation, the recipient of the U.S. Secret Service's "Outstanding Dedication and Contributions" award and the Connecticut Yankee Council of the Boys Scout's Distinguished Citizen Award.

He holds an active TS/SCI security clearance and received bachelor's degree from Georgetown University School of Foreign Service and a master's degree from Harvard University Kennedy School of Government.

Art Acevedo

Art Acevedo is Chief of Police of the Houston, Texas, Police Department. Prior to this position, Chief Acevedo served as the Chief of Police for Austin, Texas. As Chief of Police, he led a department of over two thousand law enforcement and supported personnel who carried out police operations within the City of Austin, as well as the Austin-Bergstrom International Airport, city parks, lakes, and municipal courts. Under Chief Acevedo's leadership, the Police Department has been re-engineered into a data-driven and intelligence-led policing organization. Chief Acevedo started his career with the California Highway Patrol and was eventually promoted to Patrol Chief in 2005. Chief Acevedo holds various leadership positions with the Major Cities Chiefs Association and the International Association of Chiefs of Police.

Steve Adegbite

Steve Adegbite is the Former Chief Security Officer (CSO) at Cotiviti Corporation. He is the primary executive responsible for ensuring the establishing, executing, and maintaining of Cotiviti Corporation vision, strategy and program structure for all companywide security and business continuity programs. Prior to joining Cotiviti, Steve was the Chief Information Security Officer (CISO) for E*TRADE Financial Services. Prior to joining E*TRADE, he was the Senior Vice President in charge of the Enterprise Information Security Program Oversight and Strategy Organization at Wells Fargo & Co. Prior to joining Wells Fargo & Co., he was the Director, Cyber Security Strategies at Lockheed Martin Information Services and Global Services (IS&GS). Steve also severed as the Chief Security Strategist for Adobe Systems Inc. within the Adobe Secure Software Engineering. Prior to joining Adobe, he worked in various positions in Microsoft's Trust Worthy Computing (TWC) organization most notably on the Secure Windows Initiative (SWI) and Microsoft Security Response Center (MSRC) EcoStrat team. Before he joined the private sector, he was an officer in the United States Marine Corps and served in Information Operations (IO) positions at various Intelligence community agencies both as a government employee and as an associate consultant for Booz Allen Hamilton, a strategy and technology-consulting firm. Steve is longtime member of the US and International security community.

Keith Alexander

Keith Alexander is the CEO and President of IronNet Cybersecurity. In this position, he provides strategic vision to corporate leaders on cybersecurity issues through the development of cutting-edge technology, consulting, and education/training.

Alexander is a retired four-star General with a 40-year military career, which culminated to the role of Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) from 2005-2014. He was appointed by Congress to be the first Commander to lead the U.S. Cyber Command (USCYBERCOM) from 2010-2014. As the Director of NSA, he was responsible for national foreign intelligence requirements, military combat support, and the protection of U.S. national security information systems.

Prior to leading USCYBERCOM and the NSA/CSS General Alexander served as the Deputy Chief of Staff, Intelligence, Department of the Army; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA. He also served as: Director of Intelligence, United States Central Command, MacDill Air Force Base, FL.; Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, on the Joint Chiefs of Staff; and, a member of the President's Commission on Enhancing National Cybersecurity. General Alexander is the recipient of the 2016 United States Military Academy (USMA) Distinguished Graduate Award.

Donald Dunbar

Major General Donald Dunbar is Wisconsin's Adjutant General. He commands the Wisconsin National Guard and is responsible for Emergency Management. He also serves as Wisconsin's Homeland Security Advisor, chairs the Homeland Security Council, and serves as the senior state official for cyber matters. Gen. Dunbar also serves on the executive committees of the Governor's Homeland Security Advisors Council (GHSAC) and the Adjutants General Association of the United States (AGAUS) and is a member of the Federal Emergency Management Agency (FEMA) National Advisory Council. Gen. Dunbar holds an MS in National Security Strategy from the National Defense University, and from 1998-2003 served on the Defense Department staff as an executive officer to director of the Air Operations Group. He came to Wisconsin in March 2005 to command Milwaukee's 128th Air Refueling Wing. He was appointed to his present position on Sept. 1, 2007.

Jeff Moss

Jeff Moss CEO of DEF CON Communications, Inc. A career spent at the intersection of hacking, professional cybersecurity and Internet governance gives Jeff Moss a unique perspective on information security.

Mr. Moss is the founder and CEO of the DEF CON Communications and the founder of The Black Hat Briefings, two of the world's most influential information security conferences. Mr. Moss is an angel investor to startups in the security space, is a technical advisor to the TV Series Mr. Robot, and serves on the Board of Directors for Compagnie Financière Richemont SA.

Mr. Moss actively seeks out opportunities to help shape the cybersecurity conversation. In a prior life Mr. Moss served as the Chief Security Officer and was a Vice President of ICANN, the Internet Corporation for Assigned Names and Numbers. He is a member of the US Department of Homeland Security Advisory Council (HSAC) and a commissioner on the Global Council on the Stability of Cyberspace (GCSC). He is a Nonresident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative, and a lifetime member of the Council on Foreign Relations.

Harold Schaitberger

Harold Schaitberger is General President of the International Association of Fire Fighters (IAFF), representing 300,000 professional fire fighters and paramedics in the United States and Canada. Mr. Schaitberger began his career as a professional fire fighter in Fairfax County, Virginia, and rose to the rank of lieutenant. He helped organize what was then a 500-member department as an IAFF affiliate. In 1970 he was elected the first president of Fairfax County Local 2068 and in 1973, was elected president of the Virginia Professional Fire Fighters.

Prior to his election as IAFF General President in 2000, he served as a top advisor to three IAFF presidents. He came to the IAFF in 1976 to create the union's national political and legislative programs and played a key role in the creation of the Public Safety Officers Benefit, enactment of the FLSA overtime law and the passing of the NFPA 1710 Standard governing the deployment and staffing of professional departments. Additionally, he secured federal funds to create the IAFF Hazardous Materials/Weapons of Mass Destruction training programs.

Mr. Schaitberger has led large-scale efforts to assist IAFF members and their families in the wake of national emergencies such as the September 11th attacks, as well as Hurricanes Katrina, Rita, and Wilma. Mr. Schaitberger is a Vice President on the AFL-CIO Executive Council and is Chairman of the Board of Trustees of the IAFF Burn Foundation and is a Board Member on the IAFF Fallen Fire Fighter Memorial. Prior to his election as General President, he served as a top advisor to three IAFF presidents. Mr. Schaitberger is a retired lieutenant of the Fairfax County Fire & Rescue Department.

Special Considerations to Subject Matter Expert, Emily Frye

Ms. Emily Frye is Director for Cyber Integration for the civilian enterprise at The MITRE Corporation. The Cyber Integration group identifies cyber needs and demands across the civilian sponsor arena and serves as the connective tissue between MITRE offerings and sponsor priorities. This organization is also responsible for driving corporate efforts to develop leading-edge solutions to address emerging cybersecurity challenges that our sponsors face.

Prior to this, Ms. Frye was the Director of National Protection and Resilience within the HSSEDI FFRDC. Ms. Frye has practiced law, moved a startup through three rounds of venture funding, served as the Director of Research for a think tank, and consulted extensively across technical and policy issues in both the public and private sectors. Her expertise brings together technical, legal, and business perspectives to inform homeland security risk and resilience management, cybersecurity policy and critical infrastructure protection. With twenty years of experience in creating novel solutions to the problems associated with emerging technology and security risk, she is seasoned in guiding divergent communities toward uniquely effective solutions. Her relationships with stakeholders across industry and government bring cross-sectoral depth to the design and execution of programs, exercises, analyses, and related events.

At MITRE, she has helped explore options for the future of comprehensive nationwide cybersecurity approaches across both public and private sectors, bridge the divide between federal and state government on cybersecurity initiatives, and strengthen public-private partnerships in support of Critical Infrastructure security and resilience. Her work has focused on

the financial services, information technology, electricity, and telecommunications sectors. She has served on both the Long-Range Planning Committee for the Section of Science and Technology of the American Bar Association, and as advisor to the Diversity Committee.

APPENDIX B – TASK STATEMENT

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 4, 2018

MEMORANDUM FOR: Judge William Webster
Chair
Homeland Security Advisory Council

FROM: Kirstjen Nielsen
Secretary

SUBJECT: **Four New Homeland Security Advisory Council (HSAC) Taskings**

Pursuant to the September 18, 2018 meeting of the Homeland Security Advisory Council, I am requesting you to establish four new HSAC entities to undertake reviews of critical homeland security issues. These entities should include: (1) State, Local, Tribal, and Territorial (SLTT) Cyber Security Subcommittee; (2) Countering Foreign Influence (CFI) Subcommittee; (3) Emerging Technologies (ET) Subcommittee; and (4) CBP Families and Children Care (FCC) Panel. An explanation and proposed scope for each entity is listed below in items A through D.

Recommendations are due to the full Council no later than 180 days from the date of each entity's formation. I would like an update and provisional findings from each subcommittee or panel at our next public meeting, which we will hold in late January 2019.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

Secretary

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: Judge William Webster
Chair, Homeland Security Advisory Council

FROM: Kirstjen M. Nielsen
Secretary

SUBJECT: **State, Local, Tribal, and Territorial Cybersecurity Subcommittee**

Pursuant to the September 18th, 2018 HSAC meeting, I instruct the Homeland Security Advisory Council (HSAC) to establish a new subcommittee titled "The State, Local, Tribal, and Territorial (SLTT) Cybersecurity Subcommittee" to provide recommendations regarding the following issues surrounding SLTT Cybersecurity:

Our nation faces serious and evolving cyber threats. As cyber and physical systems become more interconnected, the digital attack surface is extending further into our daily lives, with the potential for malicious cyber actors to create dangerous, real-world effects. Federal, State, Local, Tribal, and Territorial (SLTT) entities must collaborate and coordinate extensively with critical infrastructure private sector owners, operators, and stakeholders to identify and address these cybersecurity challenges. All parties need a common understanding of the threat, mechanisms to mitigate the threat, and the ability to detect and disrupt the threat. The SLTT Cybersecurity Subcommittee will examine DHS cybersecurity engagement with SLLT partners, and the Subcommittee will provide recommendations for improving DHS support to these stakeholders in order to better protect our nation' s networks and systems. The subcommittee's mandate will include, but is not necessary limited to, the following:

1. How can DHS most efficiently and effectively, across all DHS components, support SLTT agencies and partners in pursuing cybersecurity and resilience of their 1T infrastructure, to include incident response and recovery?

2. What programs, services, and outreach should DHS prioritize that would provide the greatest benefit to SLTT stakeholders in reducing risks to IT infrastructure?

3. How effective has the Homeland Security Grant Program been in addressing cybersecurity risks at the SLTT levels? How could the Homeland Security Grant Program, including associated grant guidance and technical assistance,be best structured to address cybersecurity risks?

APPENDIX C – SUBJECT MATTER EXPERTS

Dr. E. Oscar Alleyne, DrPH, MPH, Senior Advisory for Public Health Programs, National Association of County and City Health Officials

Chuck Brooks, Principal Growth Strategist for Cybersecurity and Emerging Technologies, General Dynamics Mission Systems

Margaret Brunner, Program Director—Cybersecurity, Emergency Communications & Technology—Homeland Security and Public Safety Division, National Governors Association

Thomas Duffy, Sr. Vice President of Operations and Chair MS-ISAC

Tom Filippone, Section Chief, State, Local, Tribal and Territorial Engagement, CISA

Emily Frye, Director Cyber Integration, Homeland Security Center

Michael Garcia, Senior Policy Analyst—Cybersecurity, Emergency Communications & Technology—Homeland Security and Public Safety Division, National Governors Association

Jeff Gaynor, President, American Resilience, LLC

Richard Harris, Principal Cybersecurity Policy Engineer, Homeland Security Center

Kevin Kane, Public Policy Manager at Twitter

Linda Langston, Director of Strategic Relations, National Association of Counties

Anne LaPerla, Individual Contributor

Krista Powers, Director of our Strategy, Policy and Innovation Office

Leslie Reynolds, Executive Director National Association of Secretaries of State

Doug Robinson, Executive Director, National Association of State Chief Information Officers

Saleela Salahuddin, Cybersecurity Policy Manager at Facebook

Dr. Alan R. Shark, Executive Director, Public Technology Institute

Peter Sheingold, Cybersecurity Portfolio Manager, Homeland Security Center

Mark S. Silveira, Incumbent Executive Officer, FEMA, Grant Programs Directorate, DHS

Emily Smith, Lead, Organizational Change Management, Homeland Security Center

Kay Stimson, Chair of the DHS Election Infrastructure Sector Coordinating Council, and Vice President of Government Affairs, Dominion Voting Systems

Eric Tysarczyk, Director of Preparedness for New Jersey's Office of Homeland Security and Preparedness

Tim Weston, lead drafter for our TSA Cybersecurity Roadmap

Bradford J. Willke, Director, Stakeholder Engagement and Cyber Infrastructure Resilience, Cybersecurity Division, CISA

Christopher Wright, Director, Cyber Mission Center, I&A