HOMELAND SECURITY ADVISORY COUNCIL

FINAL REPORT OF THE CYBERSECURITY SUBCOMMITTEE:

Part II – State, Local, Tribal & Territorial

June 2016

This page is intentionally left blank.

This publication is presented on behalf of the Homeland Security Advisory Council, Cybersecurity Subcommittee, co-chaired by Steve Adegbite, Juliette Kayyem, Jeff Moss and Dr. Paul Stockton as ***Part II – State, Local, Tribal & Territorial*** of the final report and recommendations to the Secretary of the Department of Homeland Security, Jeh C. Johnson.

<Signature on file>

Steve Adegbite
Chief Information Officer
E*Trade Financial Corp

<Signature on file>

Juliette Kayyem
Founder
Kayyem Solutions, LLC

<Signature on file>

Jeff Moss
Founder
Black Hat and DEF CON Conferences

<Signature on file>

Dr. Paul Stockton
Managing Director
Sonecon LLC

This page is intentionally left blank.

CYBERSECURITY SUBCOMMITTEE MEMBERS

Steve Adegbite (Co-Chair) – Chief Information Security Officer, E*TRADE Financial Corporation; Member of Homeland Security Advisory Council
Juliette Kayyem (Co-Chair) – Founder, Kayyem Solutions, LLC; Member of Homeland Security Advisory Council
Jeff Moss (Co-Chair) – Founder of Black Hat and DEF CON Conferences; Member of Homeland Security Advisory Council
Paul Stockton (Co-Chair) – Managing Director, Sonecon LLC; Member of Homeland Security Advisory Council

State, Local, Tribal & Territorial Group

Thad Allen – Executive Vice President, Booz| Allen| Hamilton Inc.; Member of Homeland Security Advisory Council
David Behen – Director, Department of Technology, Management and Budget and State Chief Information Officer, State of Michigan
Scott E. DePasquale – Chairman and Chief Executive Officer, Utilidata; Chairman, Rhode Island Cybersecurity Commission
Jane Harman – President and Director, Woodrow Wilson International Center for Scholars; Member of Homeland Security Advisory Council
Jeremy Jackson – Director, Kansas (State) Intelligence Fusion Center
Agnes Kirk – State Chief Information Security Officer, State of Washington
Jane Holl Lute – Special Coordinator on Improving United Nations Response to Sexual Exploitation and Abuse; Member of Homeland Security Advisory Council
Robert Rose – President, Robert Rose Consulting, LLC; Member of Homeland Security Advisory Council

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Sarah Morgenthau, Deputy Assistant Secretary for the Private Sector Office and Executive Director, Homeland Security Advisory Council
Erin Walls, Director, Homeland Security Advisory Council
Mike Miron, Staff, Homeland Security Advisory Council
Jay Visconti, Staff, Homeland Security Advisory Council
Katrina Woodhams, Staff**,** Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

I. INTRODUCTION

Cybersecurity is an issue that transcends the capabilities and even the responsibilities of the Federal government. The Department of Homeland Security (DHS) therefore has, unique challenges working collaboratively with state, local, tribal, and territorial (SLTT) government representatives to help them better manage their current cybersecurity risk posture and prepare for future risks.

DHS has made tremendous strides in nurturing its relationships with its core partners, the SLTT community. Through information sharing and close coordination with all levels of government, national associations, and governing bodies, DHS utilizes multiple approaches to provide ample resources and build trust with its partners.

Much work still needs to be done. Recognizing that cybersecurity is too often discussed, but not often addressed, Jeh C. Johnson, the Secretary of the Department of Homeland Security charged this Subcommittee with the following mandate:

> In an effort to strengthen the security and resiliency 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 state, local, tribal, and territorial (SLTT) government officials with information and resources in an effort to manage cyber risk, to include: cybersecurity briefings, information on available resources, and partnership opportunities to help protect their citizens online. How can the Department provide a more unified approach (to include Components responsible for allocating funds, providing threat briefings, and building resilience) to support SLTT cybersecurity?

While this mandate focuses on what DHS can do to better integrate cybersecurity efforts for its SLTT partners, it also recognizes DHS' unique role in providing standards for them. As a result, it became clear to this Subcommittee the need to assess the state of play of the SLTT network because its capabilities and responsiveness have a direct impact on how DHS should be assessing its programs and validating its efforts.

In sum, the Subcommittee observed that DHS is developing programs, best practices, and guidance to help SLTT governments, as well as the private sector, more effectively protect against cybersecurity risks. DHS is clearly working to develop standards and policies across various agencies that can help better protect public networks and give the private sector additional tools to address the problem. However, what also became clear to this Subcommittee is that – at this stage in cybersecurity efforts – the gap between the threat and overall SLTT progress is simply too great. Indeed, in likely no other threat environment, the disparity between what we know collectively as the potential harms of a cybersecurity attack (or even failure of the network caused by other means) and the capabilities to prevent and respond to it on the SLTT level is without precedent.

This page is intentionally left blank.

II. THE CYBER CONUNDRUM

There is no dearth of information out there that seeks to provide both DHS and the SLTT community with information on prevention, preparedness, and response planning. And yet there has been, almost too often, a singular primary focus between DHS and the SLTT community on notification protocols in the event of a cyber incident; that is, how DHS would notify an SLTT government about a cybersecurity incident affecting privately owned networks in a particular jurisdiction (Information regarding incidents affecting SLTT networks is generally shared via the Multi-State Information Sharing and Analysis Center, or MS-ISAC, and does not implicate the considerations below). While DHS is willing to share information about incidents affecting privately-owned networks with relevant SLTT governments, any information sharing mechanism must include safeguards for sensitive information protections. At the time of this report, SLTT governments have not developed a consensus mechanism on protecting information received from DHS about cybersecurity incidents affecting private networks. As a result, investments have been slow, cooperation has been hampered, and progress has been stymied.

It is time to move beyond the sole issue of notification to the challenges that confront both DHS and its partners given this new, non-traditional threat. In other words, this report takes as a given that the cyber threat is persistent and consistent. It is unquestionable at this stage in our networked environment. The threat may come from a foreign government, a lone actor, a disgruntled employee, a transparency activist, a modern-day robber, a blackmailer, or even just someone wanting to have some fun by exposing the vulnerabilities of SLTT networks. The reality is that it does not matter. Preparedness for a cyber-attack does not depend on the motivation of the attacker.

However, this Subcommittee determined that the best way forward is to assume that we could not immediately solve the challenges associated with assessing and notifying risk. This is not to say that we don't believe there should be a way forward that can balance notification needs with privacy and sensitive information concerns and that a portion of this obligation rests on DHS. It is only to say that there first needs to be a recognition that there is so much work to be done that can minimize the risks to our nation and that work should not be delayed.

The SLTT Subcommittee includes experts from Federal and state government, fusion centers, technology companies, and non-profits focusing on cyber and communication issues (see Appendix A for complete biographies). The Subcommittee has examined the Department's efforts to coordinate with SLTT partners to provide both findings and recommendations on best practices as well as structural changes that may need to take place as challenges evolve. In addition, we assessed the current state of the SLTT level to provide standards and practices that these partners should be taking to begin to bridge the chasm. Unfortunately, too many of these partners have failed to take cybersecurity efforts as seriously or as forcefully as others, or as the threat requires.

On the state level, another major factor that has stymied progress is the failure for traditional public safety agencies (fire, police, emergency managers, etc.) to recognize how integral cyber protections are in supporting their efforts. Too often, new technologies are

purchased with homeland security funding with no specific commitment to cyber defenses. Too often, the lead experts and planners in cyber security are not even at the table when federal homeland, infrastructure or transportation funding is allocated. And too often, cyber vulnerabilities are viewed as either overblown or too technical to be fully embraced by strategic planners outside the narrow lane of IT or chief information officers.

Our focus on core principles – rather than rehashing debates – was welcomed by many of our SLTT members and often led to a surprising conclusion: instead of wanting less oversight, policies or guidance from DHS, many of the SLTT partners interviewed wanted more from DHS that extended well beyond just seeking increased funding. They view the Federal Government as the only entity that can help them prioritize this important effort for their constituencies, require traditional public safety agencies to understand how the cyber network is an essential partner for their core capabilities, and provide the know-how and expertise that can take SLTT agencies years to nurture on their own. Indeed, in what is likely a rare instance in federal/SLTT efforts, many of these partners argued that DHS was being too deferential with its partners. Whether that is the case in all instances, or by all SLTT partners, is still subject to debate.

III. VULNERABILITIES

A 2015 PricewaterhouseCoopers report on the Global State of Information Security[1] indicates that data breaches and cyber-attacks are growing at unprecedented rates, but security spending and budgets are not keeping up with the increasing number of incidents. Notwithstanding the various efforts in place, cybersecurity continues to be the lowest-rated core capability in state and territory self-assessments, according to the 2015 National Preparedness Report[2].

SLTT-level governments have expressed increasing concern with their struggles to align with the national cybersecurity framework and implement modern cyber defense programs. In an environment where data and critical infrastructure protection must happen at all levels, there is an opportunity for this Subcommittee to help close this chasm.

These vulnerabilities are, given the nature of our networked environment, somewhat infinite. The economy, defense, transportation, medical, government, telecommunications, energy, critical infrastructure, computers, cable, and phones are all vulnerable sectors; none are solely owned or protected by a governmental entity. The cyber component of each of these sectors is difficult to secure. Cyberspace and its underlying infrastructure are simply vulnerable to a wide variety of risks whose vulnerabilities are exploited by sophisticated and unsophisticated actors and nation-states.

These vulnerabilities can only be addressed by a joint commitment to addressing the risk from integrating public-private preparedness and response capabilities, identifying and assessing dependencies and interdependencies, and sharing of information and intelligence with all partners.

[1] See *Managing cyber risks in an interconnected word: Key findings from The Global State of Information Security Survey 2015 at* http://www.pwccn.com/webmedia/doc/635527689739110925_rcs_info_security_2015.pdf

[2] See *2015 National Preparedness Report* at page i, http://www.fema.gov/media-library-data/1432751954859-fcaf2acc365b5a7213a38bbeb5cd1d61/2015_NPR_508c_20150527_Final.pdf

This page is intentionally left blank.

IV. PRELIMINARY FINDINGS

Throughout the Subcommittee's analysis, a few core themes comprise the areas where improvement is most needed. These themes addressed the range of needs for SLTT partners: cyber threat analysis and information sharing; education, training and workforce development; research and development; and shared best practices.

- There is still confusion and a perception of overlapping responsibilities regarding federal obligations to notify SLTT partners of a significant cyber-attack on private networks within a particular state. This leads to a sense, by its partners, that DHS is not fully transparent.
- At the SLTT level, cybersecurity remains a secondary and adjacent effort, not fully integrated into core missions. Leaders have voiced their concerns that this approach is limiting the abilities of those charged with cybersecurity to ensure all aspects of an agency, company, and product are secure.
- While DHS resources exist to help state agencies and the private sector train employees, address vulnerabilities, and tackle ongoing threats and attacks, there is a need for greater education and awareness about these offerings and expertise. Those in greatest need of these resources are often unaware of them.
- SLTT governments would benefit from more meaningful engagement, direction, and assistance from entities within DHS, including the National Protection and Programs Directorate (NPPD) and the Federal Emergency Management Agency (FEMA). Unlike training for first responders - including fire service, law enforcement, and others - the highly technical nature of cybersecurity work requires a different type of engagement. This includes standards to protect privacy rights.
- Lack of stakeholder understanding prevents recognition of threats, or the ability to address them. Moreover, often the people who most understand the threat are not involved in the processes related to grant funding application or allocation (Chief Information Security Officers (CISO's) and Chief Information Officers (CIO's)). Further complicating the issue is that many jurisdictions do not have the human capital or talent to understand, let alone work on cyber-related issues. As a result, investments fail to be made, or other interests prevail.
- Rapid changes in technology are often adopted by SLTT first responders with financial support from DHS, such as Next Gen 911, with little to no requirement that cybersecurity defenses be put in place.
- Approximately 95% of the current cybersecurity workforce did not receive their education or begin their careers in cybersecurity. While multiple efforts to increase the number of cybersecurity graduates and new workforce entrants are currently underway, there exists a clear and immediate need to ensure the current cybersecurity workforce receives proper and relevant training.

This page is intentionally left blank.

V. RECOMMENDATIONS: FOCUSING ON BASELINE CAPABILITIES

Even a short review of the literature about SLTT capabilities and DHS resources for cybersecurity highlights the following: there is no dearth of recommendations out there. It can be overwhelming for someone unfamiliar to the field. It is with this in mind that the Subcommittee decided our best role would be to focus the Secretary's efforts on primary, actionable take-aways that could lay the foundation for future work in this space.

It is worth noting that this approach is consistent with other challenges the Department has faced in the past. The tremendous amount of information and proposed programs in the cyber space is akin to what happened to traditional public safety entities immediately after the terrorist attacks on 9/11. The early years of DHS guidance for SLTT preparedness (most notably, the grants program) were not always perfect and it took years to create metrics, baseline capabilities and standardized core capabilities that were accepted by both the SLTT community and DHS. The back-and-forth between SLTT partners and DHS is built into the fabric of our federal system.

The Subcommittee has divided its recommendations into two discrete sections, though they have many commonalities. We first examine what DHS can do to focus its own internal efforts so as to maximize its capabilities to its SLTT partners. We next focus on what strategic policies the SLTT community can do to maximize its own efforts to protect its cyber networks.

1. Recommendations for the Department of Homeland Security

A. Eliminate Redundancies and Assess Programs: Keep it Simple

The level of activity at DHS to address these threats is both impressive and, potentially, overwhelming. It is, in many ways, exciting to see the level of integration, effort and energy; the challenge is whether the activity is being translated into progress. Over the last several years, DHS has increased its efforts, support and outreach to its SLTT stakeholders. The programs are aligned functionally within DHS' Office of Cybersecurity and Communications (CS&C)[3] and include programs that range from best practices in threat assessment to DHS' Continuous Diagnostics and Mitigation (CMD) program, Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR), National Security Deployment (NDS), Federal Network Resilience (FNR), Office of Emergency Communications (OEC), and the National Cybersecurity and Communication Integration Center (NCCIC). These do not even include the efforts by DHS' Office of Intergovernmental Affairs (IGA) or separate stakeholder engagement by component

[3] The goal of the NPPD Transition is to focus operational efforts on ensuring coordinated support to stakeholders that reflects the growing convergence and complexity of cyber and physical risks. This goal also fosters integrated field delivery of key services to operational and mission support entities. Through this transition, the new organization will be able to leverage relationships more effectively and efficiently in support of operational activity countering physical and cyber risks. By bringing together collaborative engagement activities that currently exist throughout programs across NPPD and applying more uniform customer relationship management processes, DHS will be able to take greater advantage of these existing relationships across the entire mission and increase capacity building operations.

agencies like FEMA. At the center of this activity is the NCCIC that funds and works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which improves the overall cybersecurity posture of SLTT governments. Supported by DHS, the MS-ISAC intends to fill a critical need, providing technical expertise and full-time operations to a community that is too often poorly funded and staffed, ensuring critical mitigation information is disseminated quickly and efficiently.

These programs – with multiple mandates, coordinators, and communication efforts, as well as the MS-ISAC capabilities – have numerous and overlapping stakeholders. These stakeholders include, but are not limited to, the big associations, governors and state homeland security advisors, emergency managers, National Guard assets, state and local CIOs and CISOs, FEMA regional equities, fusion centers and SLTT law enforcement, public universities and academia, and tribal partners.

These multiple lines of communication and programming are also supported and buttressed by multi-state efforts by stakeholders, including Information Sharing and Analysis Organizations (ISAOs) that are connected to the NCCIC for the purpose of sharing cyber threat information and intelligence. These efforts focus on policies and protocols for information sharing and technology platforms. Their lessons learned would then serve as a model to other states, ultimately forming a nationwide network for cyber threat information sharing, training, and developing a cyber workforce.

DHS leadership in this arena are understandably proud of these programs and efforts. DHS must assess its major efforts and multiple programs, each with their own mandate and stakeholders, to ensure that they are aligned functionally and that there is consistency of effort to communicate to their stakeholders. We do not doubt that the number of interested parties is broad and varied, but the consistent theme of DHS' partners is either that they were confused by the DHS framework or simply did not know of many of its capabilities. A program unknown or underutilized is, essentially, no program at all and risks wasting funds and energy in an issue that is so essential for our homeland security. It also, in the long term, undermines DHS' efforts if it is too often viewed (fairly or unfairly) as disorganized or mismanaged. Unfortunately, there is currently no formal assessment of SLTT program effectiveness by DHS itself.

The Subcommittee recommends that DHS provide a service catalogue for its SLTT partners to ensure transparency and coordination. More is not necessarily better over clear and concise. In this process, DHS' Office of Cybersecurity and Communications might recognize where it can better focus its outreach. As significantly, it can more successfully divide services during incident response with those that are more focused on preparedness, funding, and training.

B. More aggressively help SLTT partners motivate their constituencies and leadership

As noted above, one of the surprising themes to come out of this task force is the extent that SLTT partners were looking to DHS to assist them in their often herculean – and often ignored – efforts. The following recommendations highlight specific concerns raised by SLTT partners about notification and programming; they are in no way comprehensive, but give a flavor for the struggles that SLTT partners are having in maximizing their needs.

- Focus on consistency of message for all cybersecurity awareness programs so that those outside the field can understand and implement.
- Incorporate a feedback mechanism for improving Multi-State Information Sharing & Analysis Center services so that they can serve as a baseline to support budget requests at the state and local level.
- Enhance communication with SLTT governments regarding availability of cybersecurity training that focus on political leadership.
- Bridge higher education intellectual leadership as strong and effective partners with the SLTT community and merge SLTT cyber planners with other constituencies.
- Establish stronger directives to ensure that all grants programs integrate cyber protections and cyber personnel; simply put, too often major preparedness planning and allocations are made without cyber expert input.

All of these insights have a common theme from the SLTT community: DHS needs to better distribute resources, funding, and capabilities to the most effective level of execution. In the case of cybersecurity, this means that the distribution has to be focused on the primary agencies or disciplines in the SLTT who are responsible for preparedness, response, recovery, and mitigation with regard to cyber threats or incidents, as well as entities that support those primary agencies. This should largely be determined by implementing more effective and detailed governance jointly between the state and local levels. We recognize that by requiring that a percentage of grant funding be spent on cybersecurity, DHS could make meaningful steps in increasing cybersecurity protections in all new technology purchases and force SLTT cyber planners be part of decision making processes for grant allocations. These are simple, easy steps that require no new funding, but are a strong statement by DHS that "cyber" is not some parallel lane to traditional public safety but an integral part of an all-hazards approach to preparedness. At the very least, we believe that SLTT partners must be required to engage their cybersecurity programming and personnel into grant applications. Too often, cybersecurity subject matter experts are simply not at the table when major grant efforts and priorities are made by SLTT governments. That must end, and only DHS can require it in grant guidance, though we recognize that some SLTT partners might object to dedicating a required percentage of ever dwindling grant dollars to cybersecurity.

SLTT homeland security and emergency management offices can fund local initiatives and plans using state homeland security grants, Urban Area Security Initiative (UASI), and other grant programs. Unfortunately, those in administrative positions lack a clear understanding of both the risks and threats posed by cyber vulnerabilities. Without a clear statement about formalizing cyber protections into grant guidance, little will get done. Without such a statement, it is a vicious cycle for these overall efforts: lack of understanding means that those who do have equities are not often involved in grant funding efforts which means that cyber efforts are not integrated into overall homeland security planning, which then means that the experts are isolated from overall strategic planning.

C. Require SLTT partners adopt a unified state model

DHS has too often taken a deferential approach to SLTT capabilities. The subcommittee recognizes that this recommendation may be controversial, but DHS should no longer expend energy or resources on governance structures that are not clearly aligned or integrated. The litany of overlapping programs at the federal level is causing confusion, as we note above, but the lack of integrated homeland security leadership within states themselves is magnifying the effect. This situation clearly calls for a streamlining of processes. In many cases, there is a lack of full understanding at the state level of available federal support and funding opportunities — but this is often driven by fragmented ownership of the problem at the state level. A better rhythm for state outreach by the Federal Government will only be as good as each state's ability to engage in a coordinated homeland security process — with leadership dedicated to this role. In states that do have dedicated homeland security leadership, cybersecurity is not always a key part of the strategic portfolio.

Nearly a decade ago, DHS did the same with communications interoperability efforts. Recognizing that significant money had been distributed to SLTT partners without an equal requirement that the SLTT community plan and prioritize, the Department conditioned interoperability on both the existence of a state interoperability coordinator and a state interoperability plan. This was not simply to "punish" states; quite the contrary. State and communication leaders found that only with that DHS requirement could they then require their partners to plan before buying, prioritize regional solutions, and spend dollars more wisely. The time is now that DHS require the same in the cyber arena.

This would not be a "one size fits all" requirement. It would simply mean that DHS require that states take governance issues around cybersecurity as their first and primary step. Many have done so; too many have not. Some SLTT governments have benefitted from creating Chief Information Security Officer positions and establishing an Information Security Office. In another case, an inter-agency Information Security Working Group was established to assist the CISO in developing and adopting a framework of plans and policies. If DHS wants to take core capabilities seriously, it must begin by insisting that states recognize that cybersecurity is not a technological challenge, it is a governance one.

2. Recommendations for the SLTT Community

A. Create a framework for governance

Recommendations above related to DHS reforms in the cybersecurity space must be mirrored by similar activity on the SLTT level. As noted in the introduction, this Subcommittee made a strategic decision to utilize this platform to provide priorities for SLTT partners which we relate below in order of chronological importance. Any fair assessment of where this nation needs to be with this threat cannot put the burden solely on the Federal Government. State leaders also have a shared responsibility to secure their critical infrastructure as well as the data that has been entrusted to them by their citizens.

Again, cybersecurity is not just a technological problem; it is a governance one. Thinking about cybersecurity separately from physical security and the very human element behind cyber-attacks is a mistake. Computers don't attack people, businesses or the government

— people do that. This is a very local and human problem that requires digitally enhanced law enforcement, intelligence capabilities, and resources be further developed at the state level — and fully integrated into the homeland security function. Unfortunately, there is not a systemic approach or model for states to follow. A dozen states have started to address cybersecurity, and many more are now creating integrated homeland security policies — but we are far from a scalable state model that can be utilized writ large. Simply put: few states have elevated the issue strategically as a core homeland security function.

There is some good news, however. There are remarkable efforts throughout the SLTT network. In many cases, these are self-motivated and self-funded; in others, they work in tandem with DHS efforts. It is important that we highlight these, as examples, to not only show the tremendous progress, but also to show that the discrepancy amongst SLTTs. States such as Florida, Michigan, and Rhode Island have initiated multi-stakeholder efforts to focus on governance issues, including integrating private sector and academic experts. Washington State recently created an Office of Cyber Security during a reorganization of state information technology (IT) to best coordinate efforts between all branches of government and the private sector, and address privacy concerns.

Governance remains the biggest challenge for many of these SLTT stakeholders; simple questions like "who is in charge" need to be addressed at the front end. Through a strong commitment to governance, states can then more easily focus on other related and baseline capabilities such as:

- Identify funding to support the effort. This funding need not be limited to state or UASI grant programs but draws on state budgets, transportation, critical infrastructure, and education resources.
- Hire strong talent. Delegating or contracting out cybersecurity does not provide a long-term strategy that will help SLTTs for the future. Strong cyber programs require strong talent.
- Perform a comprehensive assessment. With the goal of honestly benchmarking the current state of SLTT information security, governments should undertake a full assessment of their cybersecurity readiness. It can also be useful to engage private sector partners to perform a risk assessment of the various environments in order to test defenses, integrating technical, business process, and policy components.
- Partner with the private sector, educational institutions, and other stakeholders. Local and state partnerships can often help to alleviate budgetary burdens and also engage essential efforts in a state's overall cybersecurity planning.
- Focus and train for incident response in the event of a cyber-attack. With a strong governance structure, tabletops and exercises can expose deficiencies in performance should a cyber-attack occur.
- Design a roadmap. While emphasizing consistent cross-sector communication on emergent threats and reviews of national and international best practices, SLTT governments should invest in improvements to their readiness. This includes training, technologies, and partnerships – including ISAOs – that better identify and mitigate threats.

None of these will occur in a focused and successful fashion until cybersecurity is treated as a core homeland security function with a mature governance structure.

B. Start with the State's Own Network

From running their own health insurance networks with personal information to school systems with a child's identifiable information to motor vehicle registrations that maintain credit card details, the amount of information residing in state networks is both vast and deeply personal. SLTT partners have so often been focused on critical infrastructure and private sector capabilities that they have neglected their own platforms' security.

The Subcommittee makes this recommendation not to minimize the needs of strong cyber protections in the private sector, but because it believes that citizens expect and deserve that their government – their state and local governments – has taken the basic precautions to protect their information. The Federal Government, because of the Office of Personnel Management (OPM) breach, has learned this lesson the hard way. Government must get its own house in order first.

C. Facilitate a network for cyber intelligence analysis that fits a state's critical needs

Intelligence capabilities would be best served by a flattened distributed network of the intelligence community with capability at the state level. Over time SLTTs should be capable of leveraging intelligence analysis on par with federal agencies and simultaneously accessing local/state/industry subject matter expertise to:

- Perform comprehensive risk assessment customized for geographic areas and disciplines by overlapping nationally developed threat analysis with local vulnerability and consequence analysis;
- Provide earlier and more readily available detection, identification, and warning of pre-attack cyber activity by correlating classified cyber threat indicators with local state government network data;
- Generate intelligence reporting from locally generated analysis that can inform and help prioritize the operations of federal agencies, Intelligence Community members, and Department of Defense entities who have distinct authorities to take various actions against cyber threat actors.

In other words, SLTTs have the capacity to fashion federal priorities. DHS could facilitate the integration of critical infrastructure, through this distributed state level intelligence analysis capability, to support those priorities and compare threat data to their own network data. This overall effort will only be enhanced by the continuing success and efforts of DHS, working with the interagency, to declassify much of this data and intelligence. This Subcommittee very much supports those efforts because one of the benefits of limiting the expansive drive towards classification is that it will benefit our SLTT stakeholders, many of whom do not hold security clearances.

In this case, DHS will have to take into account the varying degrees of development of cyber capabilities at the state and local level and the varying development of intelligence analysis

capabilities. Various local and state homeland security capabilities (not just fusion centers as they are primarily criminal intelligence/criminal case support operations) should be leveraged in this type of distributed intelligence analysis network to support cyber security efforts at all levels of government and critical infrastructure without leading to unnecessary duplication of effort, confusions over authorities, and appropriate roles and additional difficulties with governance. To this end, states should identify and evaluate existing organizational structures that can be modified or the need for new organizational structures to fulfill this intelligence analysis role.

This Subcommittee is not demanding or rejecting the notion that this capacity reside in fusion centers. As noted above, once the governance structure is in place, the exact model will depend on a state's particular needs and present capacity. Simply put, models will differ from state to state. Some state fusion centers have invested in cybersecurity efforts already and have likely seen initial success in coordinating collaboration or sharing cyber information. However, the overwhelming criminal analysis/criminal case support focus of fusion centers may render many of them less than suitable foundations for development of a cyber intelligence analysis operation. It is important to recognize the significant demand at the state and local level for the criminal intelligence that the fusion centers are providing and that they will find it increasingly difficult to spare resources for a more homeland security focused effort such as this. In some instances, the assets of the National Guard in each state could be leveraged as they have the capacity to support classified analysis operations, already employ personnel with critical cyber and intelligence analysis background, skills and expertise, and possess experience building partnerships with local government and critical infrastructure partners.

This page is intentionally left blank.

VI. CONCLUSION

In the end, cybersecurity is not just relevant to information technology and network operations teams, but now also directly affects the effectiveness of state and local law enforcement, emergency response, and National Guard professionals. It is becoming clear that the unique landscape and reach of cyberspace, in concert with the growing threats from radical, idolized, and home grown violent extremist groups, require states to play a more active role protecting and advancing our country's national security.

This page is intentionally left blank.

APPENDIX A – SLTT MEMBER BIOGRAPHIES

Steve Adegbite (Co-Chair)

Steve Adegbite is the Chief Information Security Officer at E*Trade. 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. Mr. Adegbite has also served as the Director, Cyber Security Strategies at Lockheed Martin Information Services and Global Services. Prior to joining Lockheed Martin, Mr. Adegbite was the Chief Security Strategist for Adobe Systems Inc. within the Adobe Secure Software Engineering. Mr. Adegbite has also worked with Operations positions at the National Security Agency, the National Geospatial-Intelligence Agency and the Defense Intelligence Agency, both as a government employee and as an associate consultant for Booz Allen Hamilton, a strategy and technology consulting firm.

Juliette Kayyem (Co-Chair)

Juliette Kayyem has spent over 15 years managing complex policy initiatives and organizing government responses to major crises in both state and federal government. She is the founder of *Kayyem Solutions, LLC*, providing strategic advice in technology, risk management, mega-event planning and more. Currently, Kayyem serves on the faculty at Harvard's Kennedy School of Government. She is an on-air security analyst for CNN and hosts a regular podcast entitled "Security Mom" for WGBH, Boston's local NPR station.

Previously, Kayyem was President Obama's Assistant Secretary for Intergovernmental Affairs at the Department of Homeland Security. Her book, "Security Mom: An Unclassified Guide to Protecting Our Homeland and Your Home," was published by Simon & Schuster in 2016.

Jeff Moss (Co-Chair)

Jeff Moss is a Nonresident Senior Fellow at the Atlantic Council within the Brent Scowcroft Center on International Security. He is the former Chief Security Officer for the Internet Corporation for Assigned Names and Numbers (ICANN). Prior to joining ICANN, Mr. Moss served as the Director of Black Hat and Techweb. Prior to founding Black Hat, Mr. Moss was a Director at Secure Computing Corporation, where he helped establish the Professional Services Department in the United States, Asia, and Australia. Mr. Moss has also worked for Ernst & Young, LLP in their Information System Security division. Mr. Moss speaks frequently on topics of computer and information security.

Paul Stockton (Co-Chair)

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support to FEMA and DHS during Superstorm Sandy, Hurricane Irene, and other disasters. Dr.

Stockton also served as DOD's domestic crisis manager and was responsible for Defense Critical Infrastructure Protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors.

Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation and associate provost of the Naval Postgraduate School (NPS). Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the lead co-author of "Curbing the Market for Cyberweapons" (*Yale Law & Policy Review*, 2013) and numerous other studies on cybersecurity issues. Dr. Stockton is senior fellow of the Johns Hopkins University Applied Physics Laboratory and serves on the boards of Analytic Services, Inc, Idaho National Laboratory, and the Center for Cyber and Homeland Security Studies at the George Washington University.

Admiral Thad W. Allen

Admiral Thad W. Allen (US Coast Guard retired) is an Executive Vice President at Booz| Allen| Hamilton, Inc. He is a national thought leader and strategist in homeland security, maritime security, disaster response and recovery, and energy. He is known for his expertise in public-private sector collaborative efforts to improve national resiliency and create whole of community solutions to complex man-made and natural disasters. Allen completed his distinguished thirty-nine year career in the U.S. Coast Guard as its 23rd Commandant in May, 2010, when President Barack Obama selected him to serve as the National Incident Commander for the unified response to the Deepwater Horizon oil spill in the Gulf of Mexico. Prior to his assignment as Commandant, Allen served as Coast Guard Chief of Staff. During his tenure in that position, he was designated Principal Federal Official for the US government's response and recovery operations in the aftermath of Hurricanes Katrina and Rita. For his service in those responses, Admiral Allen was the first recipient of the Homeland Security Distinguished Service Medal. Allen also currently serves as a director on the Coast Guard Foundation and Partnership for Public Service, a Fellow in the National Academy of Public Administration, and a Member on the Council on Foreign Relations.

David B. Behen

David B. Behen, Director of the Michigan Department of Technology, Management and Budget and the State Chief Information Officer, leads an agency of 2,700 employees with an annual budget of $1.2 billion that provides business and technology services to 18 state agencies.

A champion of strategic planning, Behen is involving all department staff in the process aimed at advancing customer service and promoting employee satisfaction. Under his direction, DTMB has invested $107 million since 2013 into an IT investment fund that is financing more than 40 projects to replace legacy equipment and improve services for citizens.

Behen is the driving force behind Michigan's emergence as a leader in cybersecurity. During his tenure, the state has hosted four international cyber summits, developed strategies and response plans that serve as a model for government cybersecurity across the country and positioned Michigan to develop the talent necessary to support an expanding cyber economy.

Behen has received a number of awards that recognize his CIO and technology leadership. Before joining the State of Michigan, he worked as CIO and deputy administrator of Washtenaw County and cofounder of a software company. Behen is an alumnus of Eastern Michigan University, where he earned bachelors and master's degrees.

Scott DePasquale

Scott DePasquale is a Senior Fellow at the Atlantic Council's Brent Scowcroft Center on International Security. He currently serves as Executive Chairman of Utilidata, Inc., and is an operating partner for New York-based venture capital fund, Braemar Energy Ventures. Mr. DePasquale also serves as the Chairman of the Rhode Island Cybersecurity Commission, appointed by Governor Gina M. Raimondo and is a member of the DHS Homeland Security Advisory Council Subcommittee on Cybersecurity. Previously, DePasquale was a Senior Vice President at General Electric (GE) Energy Financial Services, where he led the group's energy-tech activities. Before joining GE, DePasquale spent several years managing analytics and dispute resolution for an energy security think tank, working closely with several multinational energy concerns, national oil companies, and governments to resolve issues related to energy security, trade, and risk. DePasquale currently serves on the board of the Rand Corporation's Center for Global Risk and Security, the Internet Security Alliance, and Northeast Clean Energy Council. DePasquale holds a master of arts in international relations and affairs from the Fletcher School of Law and Diplomacy at Tufts University, a master of science in finance from Suffolk University, and Bachelor of Science in business administration from Bryant University.

Jane Harman

Jane Harman is the head of the Woodrow Wilson International Center for Scholars, a Washington, D.C. think tank devoted to the ideals of former U.S. President Woodrow Wilson. Congresswoman Harman served in congress from 1993-1998 and 2001-2011. Following her resignation from Congress on February 28, 2011 she joined the Woodrow Wilson Center as its first female Director, President and CEO. During her time in congress she represented the Aerospace Center of California during nine terms in Congress; she served on all the major security committees: six years on Armed Services, eight years on Intelligence and four on Homeland Security. Congresswoman Harman has made numerous Congressional fact-finding missions to hotspots around the world including North Korea, Syria, Libya, Afghanistan, Pakistan, Yemen and Guantanamo Bay to assess threats against the U.S. Harman received the Defense Department Medal for Distinguished Service in 1998, the CIA Seal Medal in 2007, and both the CIA Director's Award and the National Intelligence Distinguished Public Service Medal in 2011.

Jeremy Jackson

Jeremy Jackson is the Director of the Kansas Intelligence Fusion Center (KIFC). Mr. Jackson has led the KIFC's unique integration of multi-agency/multi-discipline subject matter experts into homeland security intelligence analysis since the center's inception in April 2010. Prior to directing the KIFC, Mr. Jackson worked on a team that designed and developed homeland security capabilities, including the Kansas Intelligence Fusion Center, on behalf of the Kansas Adjutant General's Department. Mr. Jackson also serves part time as an Air National Guard Intelligence Officer at Kansas Joint Forces Headquarters, where he performs strategic analysis and planning regarding intelligence and cyber capabilities. His past experience as an Intelligence Officer includes both the development of threat and vulnerability assessment for military and government computer networks as well as the supervision of intelligence analysts directly supporting war-fighters in Iraq and Afghanistan. Starting in 1993, he has served previously in the Army Reserve and the Army National Guard. Mr. Jackson also has nearly 10 years private sector engineering and project management experience, focusing primarily on electronic building systems and industrial controls for the power industry.

Agnes Kirk

Agnes Kirk is the Chief Information Security Officer for the State of Washington. Ms. Kirk is responsible for shaping the strategic direction of state security, security policy development, delivery of statewide security services, managing the state's Information Sharing Analysis Center, Security Operations Center and Statewide Incident Response, coordinating the state's participation in national cyber security efforts, coordinating efforts with the Department of Homeland Security, and representing the State of Washington in a variety of professional collaborative groups. She frequently presents at local and national security events and collaborates closely with private sector partners in securing critical infrastructure resources. Ms. Kirk was selected by Government Technology Magazine as one of the nation's Top 25 Doers, Dreamers and Drivers. She is a member of Washington State's Domestic Security Executive Group, a steering committee member of the Pacific Northwest Alliance for Cyber Security, has served on the Executive Committee of the Multi-State ISAC, is past Vice-President of the Rainier Chapter of ISSA, and chairs the State of Washington Computer Incident Response Center.

Jane Holl Lute

Jane Lute is the Special Coordinator on improving the United Nations (U.N.) response to sexual exploitation and abuse. Ms. Lute also serves concurrently as the Special Adviser to the Secretary-General on the relocation of Camp Hurriya residents outside of Iraq. Prior to re-joining the U.N., Ms. Lute served as the Chief Executive Officer of the Center for Internet Security. Ms. Lute served as Deputy Secretary for the Department of Homeland Security from 2009 until 2013. As the Department's chief operating officer, Ms. Lute was responsible for the day-to-day management of the Department's efforts to prevent terrorism and enhance security, secure and manage the nation's borders, administer and enforce U.S. immigration laws, strengthen national resilience in the face of disasters, and ensure the nation's cybersecurity. From 2003 until 2008, she held several positions at the U.N. including Assistant Secretary-General for Peacekeeping, acting Under Secretary-General, and Assistant Secretary-General for Peacebuilding. Ms. Lute was also executive vice-president and chief operating officer of the United Nations Foundation

and the Better World Fund and worked on the Carnegie Commission on Preventing Deadly Conflict. Ms. Lute served on the National Security Council staff under President George H.W. Bush and President Clinton and had a distinguished career in the United States Army. She has a Ph.D. in political science from Stanford University and a J.D. from Georgetown University.

Robert Rose

Bob Rose is Founder and President of Robert N. Rose Consulting, LLC, a boutique consulting firm focused on leveraging a deep knowledge of cybersecurity combined with an extensive network of senior level government and private sector relationships to add value to organizations across a variety of domains. He is a member of several federal government Advisory Boards to include, the Department of Homeland Security's Homeland Security Advisory Council and its Cybersecurity subcommittee, the Department of State's International Security Advisory Board and National Security Agency's Cyber Awareness and Response Advisory Panel. Additionally, Mr. Rose also serves as a member to a number of corporate Advisory Boards which include, Chertoff Group, Securonix, SquirrelWerkz and Zafesoft. Mr. Rose formerly acted as the Senior Advisor to the Chairman of Bridgewater Associates, a global investment firm.

This page is intentionally left blank.

APPENDIX B – TASK STATEMENT

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

Homeland Security

August 6, 2015

MEMORANDUM FOR: Judge William H. Webster
Chairman, Homeland Security Advisory Council

FROM: Jeh Charles Johnson
Secretary

SUBJECT: Homeland Security Advisory Council
Establishing a Cybersecurity Subcommittee

I respectfully request the Homeland Security Advisory Council ("Council") establish a Cybersecurity Subcommittee to advise the Council on existing and emerging cybersecurity issues. The Council will provide those recommendations to the Department. As the Council is comprised of senior level officials from industry, state and local government, academic experts, and community leaders, it is uniquely positioned to provide actionable findings and recommendations on cybersecurity. In addition to the establishment of a subcommittee, I request recommendations on the following two topics:

1) The Department and its public and private sector partners are making significant progress to protect the electric grid, water and wastewater systems, and other lifeline infrastructure sectors from cyberattack. Given the increasing severity of the cyber threat, it is essential to strengthen U.S. plans, capabilities, and coordination mechanisms to restore infrastructure services if our defenses fail. The Department intends to finalize the National Cyber Incident Response Framework within the next year. In order to support this effort, I request that the subcommittee identify the readiness of our lifeline sectors to meet the emerging cyber threat and provide recommendations for building cross-sector capabilities to rapidly restore critical functions and services following a significant cyber event. This effort should take into account the recommendations outlined in the recently published National Security Telecommunications Advisory Council Report on Information and Communications Technology Mobilization.

   I request that the subcommittee provide interim recommendations to the Council within six months and final recommendations within nine months.

2) In an effort to strengthen the security and resilience of critical infrastructure, the Department maintains strong partnerships with non-federal public stakeholders and associations (e.g., the National Association of Counties & National Governors Association). The Department provides appointed and elected state, local, tribal and territorial (SLTT) government officials with information and resources in an effort to manage cyber risk, to include: cybersecurity briefings, information on available resources, and partnership opportunities to help protect their citizens online. How can the Department provide a more unified approach (to include Components responsible for allocating funds, providing threat briefings, and building resilience) to support SLTT cybersecurity?

   I request that the subcommittee provide interim recommendations to the Council within nine months and final recommendations within twelve months.

I would like to express my gratitude to you and the Council for the work that has been done to date on a number of efforts. I look forward to working with you on this next endeavor.

APPENDIX C – SUBJECT MATTER EXPERTS

Timothy Blute – National Governors Association

Scott Breor – Director, Protective Security Coordination Division, Office of Infrastructure Protection, National Protectorate & Programs Directorate (NPPD)

Kelvin Coleman – Branch Chief, Office of Cybersecurity & Communications (CS&C), NPPD

Scott DePasquale – Chairman & CEO, Utilidata

Thomas Duffy – Center for Internet Security

Caitlin Durkovich – Assistant Secretary, Office of Infrastructure Protection, NPPD

John Felker – Director, National Cybersecurity and Communications Integration Center (NCCIC), CS&C, NPPD

Leonard Gentile – Office of Intelligence and Analysis, DHS

Rick Harris – Acting Director, Stakeholder Engagement & Cyber Infrastructure Resilience, CS&C, NPPD

Karen Jackson – Chief Technology Officer, Commonwealth of VA

Colonel Timothy Lunderman – Cyber Operations Director, National Guard Bureau

Jeanette Manfra – Counselor to the Deputy Secretary

Michael Masters – Senior Vice President, The Soufan Group

Phil McNamara – Assistant Secretary, Office of Intergovernmental Affairs

Andy Ozment – Assistant Secretary, CS&C, NPPD

David Quam – National Governors Association

Phyllis Schneck – Deputy Under Secretary, CS&C, NPPD

Suzanne Spaulding – Under Secretary, NPPD

Jessica Tisch – Deputy Commissioner, New York Police Department

Greg Touhill – Deputy Assistant Secretary, CS&C, NPPD

Ian Wallace – Senior Fellow, New America Foundation

This page is intentionally left blank.