AUBURN
UNIVERSITY

McCRARY INSTITUTE FOR
CYBER AND CRITICAL
INFRASTRUCTURE SECURITY

CENTER FOR CYBER
AND HOMELAND SECURITY

Testimony of Frank J. Cilluffo
Director, McCrary Institute for Cyber and Critical Infrastructure Security; and
Director, Center for Cyber and Homeland Security
Auburn University

Before the U.S. House of Representatives Committee on Homeland Security,
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

"Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help"

June 25, 2019

Chairman Richmond, Ranking Member Katko, and distinguished Members of the Subcommittee, thank you for this opportunity to testify before you today. As we all know, cybersecurity challenges are daunting enough to deal with at the Federal level. At the State, Local, Tribal, and Territorial (SLTT) levels, where resources and in many cases expertise are in relatively shorter supply, these challenges are exponentially more difficult to tackle. Recognizing this mismatch and taking steps to address it is an absolute imperative in a country as large, varied and decentralized as the United States.

Your leadership in confronting this issue head-on today and in legislation that is reportedly under discussion[1] is deeply commendable as these are important steps in breaching a real and pressing gap in our national and economic security posture. We must work to safeguard the continuity of commerce and the delivery of mission-critical services for the American people. Unless and until we foster and have in place a robust baseline capability across the board, from a State and Local standpoint, we will remain more vulnerable than we ought to be to nation-state and non-state cyber actors with malicious intent.

In testifying before you today, I will be sharing thoughts about how to move forward smartly. These ideas pertain only to those Federal entities that fall within the jurisdiction of the Committee. Moreover, a number of these recommendations are based on the May 2019 Interim Report of the Homeland Security Advisory Council's State, Local, Tribal and Territorial Cybersecurity Subcommittee.[2] I served as Co-Chair of that effort, together with Paul Goldenberg (Co-Chair) and Robert Rose (Vice-Chair). However, I testify before you today in my capacity as director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security.

Setting the Scene

State and Local Governments face the full panoply of threats that the Federal Government does, from hostile nation-state actors to cyber criminals and everything in between. To the extent that the Federal Government is effectively outgunned and outmatched in this fight, the State and Local level are all the more so. The potential consequences are serious: bear in mind that cyber threat actors can cause loss of life, property damage and financial loss by disrupting critical infrastructure operations or other means.

[1] Maggie Miller, "House Homeland Security Republicans to introduce slew of cybersecurity bills," *The Hill* (June 18, 2019), https://thehill.com/policy/cybersecurity/448971-house-homeland-security-republicans-to-introduce-slew-of-cybersecurity?wpisrc=nl_cybersecurity202&wpmm=1.

[2] https://www.dhs.gov/sites/default/files/publications/19_0521_final-interim-report-hsac-state-local-tribal-territorial-subcommittee.pdf.

Nor is the cyber threat spectrum static. It continues to expand and evolve, sharpening focus on State and Local targets. The ransomware incidents in Atlanta[3] and Baltimore[4] that disrupted city operations are cases in point and by no means will they be the end of the story. To the contrary, the scale and scope of the problem is striking, affecting everywhere from relatively robust States to major metropolitan areas to smaller cities and counties. Data on reported ransomware attacks reveal that 48 States and the District of Columbia have been hit. Targets include police and sheriff departments, schools and libraries, health agencies, transit systems, and courts – the list goes on and seemingly, no jurisdiction is too small or too large to go unaffected. The first known case of ransomware targeted the Swansea Police Department in Massachusetts in November 2013 and since then entities from Anchorage to Augusta have joined the ranks.[5]

Cyber attackers and adversaries will continue to target weaker links in the U.S. chain so long as it remains profitable or otherwise beneficial to these threat actors to do so. To make matters worse, the Internet of Things with all that it entails from smart cars to smart cities and beyond will expand the surface of attack by orders of magnitude. Security must therefore be more than a footnote or afterthought, especially where critical infrastructure is concerned. In addition, both cyber and physical infrastructure are vulnerable to attack, and the one can cause disruption or destruction in the other. This convergence of cyber domain and the physical world is another significant feature of the threat landscape.

Looking ahead, State and Local infrastructure and the cyber vulnerabilities that inhere in it will take on added salience for defenders and attackers alike. Election year 2020 reinforces the point: States and Local communities will again be at the tip of this spear, taking a multiplicity of approaches to administering voting. There is no one model or mechanism of cybersecurity governance in use at the State level, whether for elections or taken more broadly. Approaches are varied and so too are capabilities. The same is true at the Local level, only more so.

There are examples and pockets of State and Local Government cybersecurity excellence to be sure; but there are also significant gaps and seams where the Federal Government can help and can do so without subverting the principle that the level of government that is closest to the people knows best how to serve them. Cyber needs at the State

[3] Benjamin Freed, "One year after Atlanta's ransomware attack, the city says it's transforming its technology," *StateScoop* (March 22, 2019), https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/

[4] Emily Stewart, "Hackers have been holding the city of Baltimore's computers hostage for 2 weeks," *Vox* (May 21, 2019), https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers

[5] Allan Liska, "Early Findings: Review of State and Local Government Ransomware Attacks" (Recorded Future: 2019), https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf.

and Local level are many: more money, more experts, more tools, more information/awareness and more collaboration (between government and industry, and among governments and regions) – to name just a few.

Against this background what can and should the Federal Government do? How best can the Federal Government leverage its resources in the broadest sense of the word, to help State and Local Governments amplify their strengths and mitigate their weaknesses? Enhancing the pool of financial resources available to support a range of cybersecurity purposes is just one – albeit very important – way. Other ideas are set out below.

Moving Forward Smartly

Directed Federal Funding

Funding is crucial of course and building capability is impossible without it. Purchasing, maintaining and upgrading equipment, hardware and software comes at a financial cost. So too does recruiting and retaining skilled workers. Educating the next generation and expanding the cyber workforce by training or retraining the existing talent pool also requires an investment of dollars, time and effort. For all of these purposes and more, a Federal grant program to shore up State and Local cybersecurity capabilities is needed and long overdue. As things now stand, less than 4% of grant monies from the Homeland Security Grant Program are directed to cybersecurity. This is not a tenable situation. Nor is the answer to redirect existing monies for cyber purposes. Robbing Peter to pay Paul simply will not work.

A dedicated Federal grant program should have built-in safeguards to ensure that there is return on Federal investment in the form of measurable State/Local and by extension national capabilities. Simply throwing Federal money at the problem is not the answer. Instead, there must be a thoughtful strategy and accompanying metrics to support the request for funds and any subsequent grant. The program would therefore be risk-based and tailored to particular context. Among the purposes that such a program could and should support would be both State-level and regional exercises. Notably momentum for directed Federal funding is building as evidenced for example by the recommendations in the May 2019 Interim Report of the Homeland Security Advisory Council's State, Local, Tribal and Territorial Cybersecurity Subcommittee.[6]

[6] https://www.dhs.gov/sites/default/files/publications/19_0521_final-interim-report-hsac-state-local-tribal-territorial-subcommittee.pdf.

Amplify Training Opportunities

The Federal Government could further assist by providing opportunities for State and Local officials to gain and hone cybersecurity skills, as well as how to identify and counter foreign influence. While education and training programs certainly do exist they are neither as numerous nor as evenly available across the country as would be ideal. A national focal point where those whose community is underserved by training opportunities could advance their skills and career and by extension the national interest, would serve us all well.[7] All the equipment, tools and resources in the world will be of little assistance if the technical expertise needed to employ them to full advantage is not cultivated in the requisite official quarters.

Among the beneficiaries of such training could be State and Major Urban Area Fusion Centers, whose cyber-specific capabilities have long lagged behind their other homeland security and law enforcement capabilities.[8]

Leverage Lessons Learned

Over the past twenty years, the country has learned many lessons about preparing for, responding to and bouncing back from major incidents such as terrorist attacks and natural disasters. These experiences have ultimately made us smarter, stronger and more resilient as a nation, though we still have a ways to go. Among these lessons is the value of taking a regional approach to capacity-building and mutual assistance, which builds upon existing relationships and arrangements, and follows logically and naturally from proximity and geography, rather than duplicating efforts and according formal borders/boundaries undue influence. The EMAC – Emergency Management Assistance Compact – concept is as relevant here as in the traditional emergency management context. Pioneered in the South, use of the construct has expanded over time[9] and would transpose well to the cyber domain. The basic idea is to pool resources and expertise in order to offer mutual assistance.

When it comes to cybersecurity, such an approach would for example have States undertake planning, incident response and resilience enhancement measures from a regional perspective. Here the Federal Government could and should act in support of

[7] Note also that the HSAC's SLTT Cybersecurity Subcommittee Interim Report recommends the creation of a National Cybersecurity Academy to train SLTT Government employees – an idea whose time has come.
[8] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing and Keith D. Squires, *Counterterrorism Intelligence: Fusion Center Perspectives* (June 2012).
[9] EMAC Overview (August 2006), https://www.fema.gov/media-library-data/20130726-1726-25045-0915/060802emac.pdf.

these efforts including by acting to expand awareness of best practices and guidance on how best to implement them.[10]

A further lesson learned over time relates to recognizing the importance of being out in the field rather than at headquarters. There is no substitute to having boots on the ground. To this end, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) should extend its operations and work towards having State cybersecurity coordinators for all 50 States to provide technical assistance and incident response support. This would broaden and complement existing DHS efforts and field personnel (State Cybersecurity Advisors) focused on community engagement and awareness as well as the provision of enhanced strategic advisory services. The arrangements proposed here would also help convey and highlight the Federal consequence management capabilities and tools that can support and supplement State capabilities — in effect a bad day "geek squad."

Circumscribed Election Assistance

One of the most significant cybersecurity challenges to State Governments relates to the 2020 election and in particular preparing to administer the vote and ultimately doing so. Protecting the integrity of the process from beginning to end is of paramount importance as this exercise provides the bedrock for our democracy; trust and faith in the process is the glue that binds us together. The Federal Government can and should share more widely and actively its unique informational and other assets with State-level counterparts for the targeted purposes of identifying and mitigating threats in this context.[11]

To be clear, this would involve concerted Federal efforts to create and maintain a rich picture of the threat from the national perspective and a companion effort to support State officials in responding effectively and timely to that dashboard as it specifically pertains to them/their State.[12] Such a division of labor is properly respectful of the division of powers and capitalizes upon the strengths that reside at each level of government. By working together in this way, the nation stands the best chance of defeating adversary attempts to exploit not just our technology but also our hearts and minds, by means of weaponizing information and influence. Fortunately, we are seeing

[10] Note that the HSAC's SLTT Cybersecurity Subcommittee Interim Report also highlights the value of a regional approach.

[11] But note that the Multi-State Information Sharing and Analysis Center (MS-ISAC) does yeoman's work in terms of amplifying situational awareness (for example by providing threat alerts to all 50 States and manifold localities); and helping to coordinate incident response. For details, see https://www.cisecurity.org/ms-isac/.

[12] A variation of this idea is proposed in the HSAC's SLTT Cybersecurity Subcommittee Interim Report.

some positive indicators already, with (DHS) CISA deepening its outreach to and work with the Nation's Governors.

This series of recommendations focuses on technology, training, incident response, and the workforce. The list is not exhaustive and speaks instead to the actions that could have the highest impact on the cybersecurity challenges of greatest priority in the context of State and Local Government.

Ending On a Good News Story

In addition to assessing how the Federal Government can help State and Local Governments to address cybersecurity challenges, it is important to acknowledge that there is good work underway outside the Federal sphere and that State and Local entities are taking substantial steps to help themselves. Keep in mind that States have a correlative and ongoing responsibility to lead and lean forward, and should not expect the Federal Government to supplant State efforts or to be there all the time. In this regard consider for example the Alabama School of Cyber Technology and Engineering (full disclosure: I serve on the School's Board of Trustees). This magnet school for grades 7 through 12 will stand up in August 2020 in the Huntsville Research Park. Our vision for the ASCTE is to "educate, develop and inspire the next generation of leading national professionals and technologists in engineering and cyber technology."[13]

This effort complements the many cybersecurity programs and initiatives including partnerships with industry and government that are underway at Auburn University and other educational institutions within the State of Alabama and in the Southeast more broadly. While the coasts of this country tend to garner the bulk of attention when it comes to coverage of cyber and science & technology matters more generally, it is important to recognize that other jurisdictions are quietly plowing ahead on significant efforts in these same issue areas that are so critical to our national security. These under-reported successes serve us all well since Federal measures alone will not get us to goal or keep us there even if they could.

Thank you once more for this opportunity to participate in this important conversation and assessment.[14] I look forward trying to answer any questions that you may have.

[13] https://www.alabamasce.org/school

[14] I would also like to thank my colleague Sharon Cardash, deputy director of the Center for Cyber and Homeland Security, for her assistance in preparing this testimony.