AUBURN UNIVERSITY

McCRARY INSTITUTE

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

Before the U.S. House of Representatives Committee on Homeland Security

"Securing the Homeland: Reforming DHS to Meet Today's Threats"

July 15, 2021

1214 Shelby Center, Auburn, AL 36849 | Tel: (334) 844 - 2489
mccrary.auburn.edu

Introduction

Chairman Thompson, Ranking Member Katko, and distinguished Committee Members, thank you for the opportunity to testify before you today. The array of threats to this country has evolved substantially over time and therefore so too must our national architecture for countering these threats. Your proactive approach to taking on this challenge by examining the Department of Homeland Security (DHS) in particular, is commendable and I hope to help you move the ball forward in this statement and in my verbal remarks at this hearing.

Evolution of the Department's Threat Landscape

Allow me to begin with a bit of history and context. DHS was established in 2002 in direct response to the horrific attacks of 9/11. At the time, the principal threat to the country was from terrorists, specifically al Qaeda and likeminded (self-styled) "jihadists". Counterterrorism was thus the animating purpose of the Department. At the same time however, DHS had, and continues to have, a wide set of missions including transportation security, border security, emergency management and response to manmade and national disasters, protecting U.S. economic security, and strengthening preparedness and resilience – to name a few.

Today, all these missions and threats persist; and DHS continues to be instrumental in preparing for and responding to them. Having said that, the most prevalent and most pressing threat now is cyber. The ecosystem has evolved such that in 2021, cyber is the system's blinking red light, the most imminent threat facing the country. Accordingly, cyber is the area where we must now double down and work the hardest to enhance our capabilities – not at the expense of other missions and threats, but in addition to them.

The case for focusing on the cyber mission and ensuring that DHS is both well-structured and well-funded to meet it, is so strong that it practically makes itself. Consider the events of just the past six months, in which we have seen a rash of incidents from the SolarWinds and Microsoft Exchange hacks targeting the IT supply chain, to the Kaseya ransomware incident (only days ago) and a spate of other significant ransomware attacks that preceded it – many directed against critical national infrastructure and functions, including U.S. pipelines and the food supply. While not necessarily the most significant cyber threat, ransomware is perhaps the most prevalent. It is hitting epidemic proportions, targeting entities from schools to businesses; no one and nothing is off-limits.

The breadth of entities affected by cyber incidents has been striking, as has the severity of the actual consequences, which continue to be uncovered week by week. Perhaps most disturbingly, these incidents have targeted and undermined the very trust upon which the entire system is founded. For all these reasons, current circumstances

demand that DHS be postured robustly to reflect and respond to the reality that the cyber threat is nothing short of front and central today.

Maturing the Department to Meet Today's Threats

Leadership. In concrete terms, this means starting at the top, literally. Meaningful maturation of the Department requires the posts in its senior echelons (cyber and Department-wide) to be filled, and to be occupied in a manner that supports the principle of continuity of leadership. This crucial measure is in Chairman Thompson's recently reintroduced DHS Reform Bill.[1] In particular, the Director of the Cybersecurity and Infrastructure Security Agency (CISA) should be emphasized requisite with its importance. As the Cyberspace Solarium Commission (on which I serve as a Commissioner) recommended, codifying a 5-year term for the Director of the agency and elevating the role would ensure continuity across the organization and attract the best the nation has to offer.

To be clear, many of those who took on key roles in an acting capacity performed a true public service for the nation at a critical juncture in time. But to rely on these individuals over-much and over-long is not fair, either to them or to DHS.

Congress and this Committee. Congress and this Committee also have an important role to play in moving the Department forward. Specifically, there is a deep need for this body to reauthorize DHS and be afforded the requisite authorities to oversee the Department. Fulsome oversight is of course a crucial Congressional responsibility; but it is not an either/or proposition, meaning that Congress must authorize DHS in addition to oversee it. Unless we press ahead on both fronts, the Department will not be able to reform itself to properly meet today's threats.

Partners. Though DHS is our focal point, we must look outward as well as inward to understand and appreciate all that needs doing to propel us from where we are, to where we need to be. To achieve our cyber aims and ends, DHS must be able to support its full panoply of principal partners: State, Local, Tribal and Territorial (SLTT) governments, and the private sector. This means two-way flow of information, shared timely and in a manner that facilitates action (i.e., next steps) on both sides. With cyber as with the broader homeland security enterprise, we need to find ways to enhance and enable the front lines.

Workforce. Reaching this bar requires more than technology. It also requires people – a skilled and sufficiently deep bench to meet the mission. Building and sustaining a cyber workforce of the caliber and size needed by the Department (and beyond) is a truly urgent priority. The most effective way to get there is to proceed in a multitrack way that encompasses both shorter- and longer-term measures, including in-career training,

[1] "Department of Homeland Security Reform Act of 2021" https://homeland.house.gov/imo/media/doc/DHS%20Reform%20Act%20of%202021.pdf

recruitment, and retention efforts, plus K through 12 and postsecondary initiatives. Special emphasis should be accorded to upskilling veterans and recruiting a more diverse workforce.

Interagency. Precisely because the cyber threat is so pervasive and complex, tackling it requires a whole-of-nation approach. In turn, providing the private sector and other levels of government with the support they need from federal entities must be a team effort. In this regard, DHS and specifically CISA[2] should work hand-in-glove with NSA's Cybersecurity Division and FBI as a triad, that is powered by the unique capabilities and authorities that each element brings to bear. Together with the National Cyber Director (NCD), a new position, synergy and strategy should take on new salience, as everyone will finally be working off the same sheet of music.

Response. There have been a number of great developments and actions taken by Congress as of late to respond to the increase of cyber attacks, including codifying the Cyber State of Distress and the Cyber Response and Recovery Fund. In the event of a significant cyber incident, the government needs a mechanism to surge critical resources to facilitate response, mitigation, and recovery. The Solarium Commission therefore recommended the ability for the President or designated federal official to declare a cyber state of distress. Such declaration would strengthen the Secretary of Homeland Security's ability to ensure adequate preparation and coordinate asset response.

Coupled with the declaration authority, it is vital for the government to have available recovery funds. The cyber response and recovery fund, another Solarium Commission recommendation, will be used to augment U.S. government response teams and their ability to assist SLTT governments and the private sector in responding to and recovering from an attack. In addition, the recommendations in Ranking Member Katko's Five Pillar Plan will add to the success.[3]

National Risk Management. To fulfill its potential as an interagency partner and beyond, CISA must mature and be strengthened. To this end, the Agency's National Risk Management Center (NRMC) should be codified. Elevating the NRMC in this way would help underscore and advance the difficult and exceptionally important work that the Center does. One example, which deserves far more attention than it has received, is the NRMC effort to identify national critical functions.

The NRMC's work on national critical functions provides a strategic foundation for prioritizing critical infrastructure and related risk management measures, thereby delineating a targeted path to enhancing the country's resilience. That ability to bounce

---

[2] CISA was established by the Cybersecurity and Infrastructure Security Agency Act of 2018, sponsored by Representative Michael McCaul.

[3] "Ranking Member John Katko SolarWinds Campaign Response Five Pillar Plan" https://republicans-homeland.house.gov/wp-content/uploads/2021/02/Katkos-5-Pillars.pdf

forward after an incident diminishes the returns that an adversary can expect to reap from an attack on U.S. entities or interests and serves as a disincentive to attack in the first place. The NRMC should therefore continue and amp up its efforts to build out our understanding of national critical functions, to better position the U.S. to (simultaneously) remain resilient and deter foes.

A specific application of this recommendation relates to the intersection of two domains: cyber and space. Increasingly, space is fundamental to continuity of a host of other critical national operations and functions, such as positioning, navigation, and timing (PNT). As cyber threats pose an ever-increasing risk to U.S. space assets, the NRMC should redouble its focus on expanding and deepening its understanding of national critical functions in this area.

However, the work of the NRMC and the Department on national cyber risk reduction cannot and should not stop with identification. The Department should be vested with a consistent, multi-year fund to enable it to drive strategic investment aimed at reducing and mitigating risk to critical infrastructure and enhancing the nations resiliency.

Planning. Industry and government must work together to plan and prepare for the cyber threats our nation is facing. As recommended by the Solarium Commission, the newly created Joint Cyber Planning Office (JCPO) within CISA should be stood up swiftly and serve as the center of gravity for public-private coordination of defensive cyber activities based on the priorities set by the National Cyber Director.[4] Cross-sector collaboration is key to the success of JCPO and to creating comprehensive plans to respond to and recover from future incidents.

Preparation Grants. Local government partners require improved defensive capabilities to protect themselves against emerging and evermore frequent cyber threats and attacks. The DHS Homeland Security Advisory Council (HSAC) SLTT Cybersecurity Subcommittee, which I co-chaired, recommended the creation of a dedicated grant program to improve local government cybersecurity and create bulk purchasing vehicles for vital cyber necessities.[5] The use of grants will enable SLTT partners to improve their preparation and capabilities substantially.

Deterrence. While resilience supports deterrence, it does not eliminate the need for a broader U.S. strategy to deter our adversaries by imposing real costs and consequences upon them. For too long, China and Russia (for example, but they are not alone) have been allowed to engage in cyber behavior that has damaged U.S.

---

[4] "Gas pipeline hack reveals cyber vulnerabilities. But Biden infrastructure plan doesn't fix them." https://www.nbcnews.com/think/opinion/gas-pipeline-hack-reveals-cyber-vulnerabilities-biden-infrastructure-plan-doesn-ncna1267021

[5] "Homeland Security Advisory Council Final Report of the State, Local, Tribal and Territorial Cybersecurity Subcommittee"
https://www.dhs.gov/sites/default/files/publications/2._sltt_final_report_0.pdf

national and economic security, without corresponding effects being visited upon the perpetrators.

Until we use all instruments of statecraft to influence the decision calculus of our adversaries, bad behavior will go unchanged. This means getting serious about even the more passive forms of hostile behavior, such as nation-states (like China and Russia) stymieing the long arm of the law by affording safe haven to cybercriminals committing ransomware attacks that affect critical infrastructure in this country and others. It is surely no accident, for instance, that the enormous Kaseya ransomware/supply chain attack was powered by malware designed to avoid Russian-language systems.[6]

Unified Security. Stepping up our offense must also be complemented by a more comprehensive and coherent defense. Our current approach to .gov security is too scattershot. CISA can and should occupy a more central role here. The FY 2021 National Defense Authorization Act empowered CISA to hunt for cyber threats on U.S. government networks. This is a good start; but more robust defense requires substantially more visibility than presently exists.

Amplified visibility, which feeds our understanding of threat and underlies both response and resilience, requires genuine partnerships within and outside government. The imperative to turn the nouns about public-private partnership into verbs has never been clearer. Both national and economic security urgently demand greater visibility across the entirety of our supply chains, as underscored in a recent report of the HSAC Economic Security Subcommittee which I chaired.[7] Yet, as things now stand, cyber incident reporting is not mandatory and barriers to information sharing persist. This situation gives rise to dangerous blind spots.

Information Sharing. Against this concerning background, the Cyberspace Solarium Commission has recommended that a joint collaborative environment be established by law, for the purpose of sharing cyber threat data among federal entities and between the U.S. government and the private sector. The proposal further envisions CISA at its center, as manager of the programs supporting the JCE.

In addition, the Solarium Commission proposes that the most critical of the critical – meaning systemically important critical infrastructure (SICI) – be codified and subject to enumerated benefits and burdens, in service to the U.S. national interest. The idea is to impose a cyber incident reporting requirement on SICI companies in return for liability

---

[6] "Code in huge ransomware attack written to avoid computers that use Russian, says new report" https://www.nbcnews.com/politics/national-security/code-huge-ransomware-attack-written-avoid-computers-use-russian-says-n1273222

[7] "Homeland Security Advisory Council Final Report: Economic Security Subcommittee" https://www.dhs.gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf

protection for such incidents and direct intelligence support from the U.S. intelligence community.

More consistency in incident reporting is needed. Without situational awareness, government cannot properly support and defend the nation. Earlier reporting will allow the government to provide more tools and capabilities in this regard. Fortunately, Congress is now moving in this direction with multiple bills on data breach notification and incident reporting, including Ranking Member Katko's leadership to identify and secure SICI, with CISA playing a lead role in the designation process.

Industrial Control Systems. The industrial control systems (ICS) that power critical infrastructure merit special consideration. Identifying and remedying vulnerabilities in ICS is crucial, in part because ICS represent the interface where information technology and operational technology intersect. Put differently, this is where cyber domain and the physical world coincide. In this context, a breach on the IT side can cause catastrophic effects in the real world.

The hybrid threat here demands that our ICS be shored up carefully. A bipartisan bill sponsored by Ranking Member Katko and co-sponsored by Chairman Thompson and other Committee Members[8], H.R. 1883,[9] intended to do just that. The proposed legislation would enhance U.S. capabilities in this area and entrench in law CISA taking point on that task, including by providing free tools and services to critical infrastructure stakeholders.

Conclusion

The threat landscape will continue to evolve as cyber domain brings new challenges and opportunities for America and its adversaries alike. Placing the country on a more solid footing to confront these pressing threats is a must, especially in relation to our most critical infrastructure. Today's hearing is a significant step in that direction.

Moving ahead, the Department must be calibrated to adapt to this cyber imperative while also retaining and advancing the ability to counter the wide range of other threats and to fulfill the many missions for which DHS was established.

Thank you for the opportunity to testify before you today.[10] I look forward to trying to answer any questions that you may have.

---

[8] Rep. Cammack, Rep. Clarke, Rep. Garbarino, Rep. Gimenez, Rep. Langevin, and Rep. Pfluger

[9] "DHS Industrial Control Systems Capabilities Enhancement Act of 2021" https://www.congress.gov/bill/117th-congress/house-bill/1833/text?r=11&s=4

[10] Thank you also to Sharon Cardash and Matthew Edwards for their skillful assistance in preparing this testimony.