Hearing Before the Subcommittee on Emerging Threats and Spending Oversight
Homeland Security and Governmental Affairs Committee
U.S. Senate

"Addressing Emerging Cybersecurity Threats to State and Local Government"

June 17, 2021

Dan Lips
Vice President for National Security and Government Oversight, Lincoln Network

Chairman Hassan, Ranking Member Paul, and Members of the Subcommittee,
Thank you for the opportunity to testify.

My name is Dan Lips. I am the vice president for national security and government oversight at Lincoln Network, a non-profit organization focused on bridging gaps between the technology and policy communities.

As a former HSGAC staffer from 2011 to 2019, I'm sincerely honored to have the opportunity to testify today. I have a deep respect for the members and staff of the Committee and the important bipartisan work that is done in this hearing room.

My testimony focuses on policy and oversight options to help state, local, territorial, and tribal governments, and the private sector address growing cyber threats.

We are all now aware that organizations across the United States are being targeted by ransomware attacks at an alarming rate. According to one recent estimate, U.S. organizations experienced 65,000 ransomware attacks in 2020.[1] At that rate, more than seven organizations will likely suffer a ransomware attack over the next hour.[2] The victims of these attacks include private sector and non-profit organizations, owners and operators of critical infrastructure, and governmental organizations (such as states, municipalities, school districts, and hospitals).

As the Committee will hear from the other panelists, ransomware attacks can stop organizations' operations while leaders make the difficult choice of whether to pay the ransom while working to unlock and restore information systems. Given attackers' economic incentives and the profitability of these kinds of attacks, we should expect ransomware to be an increasing problem moving forward. Beyond ransomware, organizations continue to face a broad range of cyber-attacks, such as nation-state sponsored economic and industrial espionage, traditional espionage, other financial crimes, and potential threats against critical infrastructure.

These threats require a proactive response by the federal government. But Congress should be thoughtful about the resources currently available to spend on cybersecurity as well as government agencies' capacity and track-record managing cyber responsibilities and grant

[1] David Gura, "U.S. Suffers Over 7 Ransomware Attacks An Hour. It's Now A National Security Risk," *NPR*, June 9, 2021.
[2] Ibid.

programs. According to Comptroller General Gene Dodaro, the United States is on an unsustainable fiscal path.[3] The Government Accountability Office (GAO) has warned that interest payments on the federal debt will exceed $1 trillion by 2033 and that the growing debt could bring a "large reduction in the value of the dollar" and limit Congress's ability to use fiscal policy to respond to future national emergencies.[4]

With this context, what should Congress, and specifically the Committee and Subcommittee, do to help states, localities, tribal, and territorial governments to manage growing cybersecurity risks?

I will offer four recommendations.

1. **Congress should streamline federal rules to reduce state governments' compliance costs to allow more state resources to be spent on improving security.**

For years, a top advocacy priority of the National Association of State Chief Information Officers ("NASCIO") has been for the federal government to "harmonize disparate federal cybersecurity regulations" and normalize the federal agency audit process.[5] For example, the Internal Revenue Service, Social Security Administration, and the Health and Human Services Department, among many others, have specific, and in some cases contradictory, rules for how to protect Americans' information. In 2020, GAO issued a report examining this problem and found that "the percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent."[6]

As a result, state officials spend much of their time on bureaucratic compliance. In 2018 testimony before the House Oversight Committee, the Oklahoma state CIO said that his office spent 10,712 hours on "compliance activities and support" that year, which amounted to five employees' entire year of work and nearly half of his team's time spent answering federal rules and audits.[7]

Streamlining federal rules would reduce the compliance burden imposed on state governments and free up time and resources currently devoted to compliance towards security. This would improve the cybersecurity posture of both state and local governments. In 2020, NASCIO and the National Governors Association issued a joint report describing how state governments were establishing initiatives to partner with localities to improve cybersecurity.[8]

---

[3] U.S. Government Accountability Office, GAO-21-275SP, *The Nation's Fiscal Health: After Pandemic Recovery, Focus Needed on Achieving Long-Term Fiscal Sustainability* (2021), https://www.gao.gov/products/gao-21-275sp.
[4] Ibid.
[5] "NASCIO Releases 2021 Federal Advocacy Priorities: Continues Call for Harmonized Cyber Regulations," NASCIO, January 14, 2021, at: https://www.gao.gov/products/gao-21-275sp.
[6] U.S. Government Accountability Office, *GAO-20-123, Cybersecurity: Select Federal Agencies Need to Coordinate on Requirements and Assessments of States* (2020), https://www.gao.gov/products/gao-20-123.
[7] James "Bo" Reese, "Regulatory Divergence: Failure of the Administrative State" Statement Before Oversight and Government Reform Committee, 2018.
[8] NGA and NASCIO, *Stronger Together: State and Local Cybersecurity Collaboration* (2020), https://www.nga.org/wp-content/uploads/2020/01/NASCIO_NGAStatesLocalCollaboration.pdf.

In the past, the National Governors Association has joined NASCIO in writing to the Office of Management and Budget (OMB) to ask the administration to address this problem of overlapping and contradictory federal information security rules.[9] Last May, GAO reported that OMB had issued guidance directing federal agencies to coordinate information security rules and compliance requirements, but had not required agencies to do so.[10] The Committee should pass legislation directing OMB to require agencies to harmonize information security rules to reduce the compliance burden on state governments.

2. **Congress should prioritize cybersecurity in existing homeland security grant programs and states should use currently available federal funds to close cybersecurity capability gaps.**

Simply streamlining the compliance burden alone will not close state and local governments' capability gaps to address current cyber threats. This will also require additional resources. I appreciate that there is interest in Congress and among members of the Committee to establish a new federal grant program for cybersecurity.

But the Department of Homeland Security, through the Federal Emergency Management Agency, already awards more than $1 billion annually to state and local partners to address homeland security needs including cybersecurity.[11]In the past, DHS has required states and localities to use 5 percent of their homeland security grant funds to improve cybersecurity capabilities. In February, Secretary Mayorkas stated that the Department would increase that requirement to 7.5 percent.[12] Congress, however, could require even larger percentages to be spent on cybersecurity. DHS's homeland security grants were expanded after the 2001 terrorist attacks to address existing counterterrorism and public safety capability gaps and buy-down risk. But past oversight by GAO and members of the Committee, including my former boss Senator Tom Coburn, have raised questions about the extent to which these funds have been used to measurably buy-down risk[13] or instead to subsidize routine public safety costs.[14] Given current threats, it would be appropriate for states and urban areas to use existing DHS grant funds to improve cybersecurity capabilities.

Importantly, states and localities do not need to wait for new grant awards to do this. They already have billions in unused homeland security grants that could be readily deployed to address current cyber threats this year. In 2020, OMB reported that states had not spent $2.7

---

[9] Letter to Mick Mulvaney, OMB Director, "Reducing Burdensome Cyber Regulations," NGA and NASCIO, November 6, 2017, at: https://www.nga.org/advocacy-communications/letters-nga/reducing-burdensome-cyber-regulations/.

[10] U.S. Government Accountability Office, GAO-20-123, *Cybersecurity: Select Federal Agencies Need to Coordinate on Requirements and Assessments of States* (2020), https://www.gao.gov/products/gao-20-123.

[11] "FY2021 Homeland Security Grant Program," Federal Emergency Management Agency, https://www.fema.gov/grants/preparedness/homeland-security.

[12] Benjamin Freed, "DHS announces $25M increase in cybersecurity grant funding," *State Scoop*, February 25, 2021.

[13] U.S. Government Accountability Office, GAO-18-354, Homeland Security Grant Program: Additional Actions Could Further Enhance FEMA's Risk-Based Grant Assessment Model (2018), https://www.gao.gov/products/gao-18-354.

[14] Senator Tom Coburn, *Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities* (2012), Homeland Security and Governmental Affairs Committee.

billion of the $5.3 billion that had been provided through the State Homeland Security Grant and the Urban Area Security Initiative programs between 2015 and 2020.[15] In other words, roughly 50 percent had not been spent. This means that at least $2 billion, and perhaps more, is likely still unspent and could be used today to address current cybersecurity capability gaps.

Also, states, localities, and even state education agencies and school districts should consider how other currently available federal resources could be spent to improve cybersecurity. For example, the American Rescue Plan is providing $350 billion to state, local, territorial, and tribal governments. According to the Treasury Department, Congress "provide[d] substantial flexibility" for governments to use these funds to meet local needs.[16] Moreover, Congress has provided an unprecedented infusion of federal emergency funds to state education agencies during the pandemic. But at least $180 billion of these emergency funds remained unspent as of this spring.[17] These funds should primarily be used to reopen schools and help disadvantaged children recover from prolonged school closures that occurred during the pandemic. However, state education agencies could use some of the available funding to improve cybersecurity defense to protect against ransomware attacks on schools and prevent future schooling disruptions, which could create additional setbacks for American children.

In short, state and local partners should use currently available resources to address current cybersecurity capability gaps before establishing new grant programs and awarding new funding. Congress and the Subcommittee should conduct oversight to determine what resources are currently available.

3. **The federal government should share meaningful threat information and security recommendations to help organizations manage cyber risks.**

Over the past decade, Congress has recognized the importance of improving information sharing about cyber threats and recommending best practices. Congress has passed bipartisan laws to establish federal programs and initiatives to facilitate information sharing. But nonpartisan oversight by GAO and the Inspector General have identified limitations and opportunities to improve DHS's information sharing programs.[18] Concerns have included the timeliness of information shared, limited participation by private sector partners, and over-classification, to name a few. Congress and the Committee should press agencies to answer open

---

[15] Dan Lips, "States and Cities Could Use Billions of Unspent DHS Grants to #Protect2020," *Lawfare*, February 28, 2020.

[16] "Coronavirus State and Local Recovery Funds," U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/coronavirus/assistance-for-state-local-and-tribal-governments/state-and-local-fiscal-recovery-funds.

[17] Dan Lips, "$180 Billion of K-12 COVID Relief Funds Are Still Unspent," *Foundation for Research on Equal Opportunity*, May 19, 2021.

[18] U.S. Government Accountability Office, GAO-21-288, *High Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (2021); DHS Office of Inspector General, OIG-20-74, *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018* (2020).

watchdog recommendations. In addition to sharing information about cyber threats, Congress should require federal agencies to share meaningful information with state and local governments about potential vulnerabilities in the information technology ecosystem to improve their technology acquisitions and strengthen supply chain risk management.

Beyond information sharing, Congress should also focus on ways to leverage the federal government's expertise to help state and local governments understand and implement best practices. For years, security experts have recommended that the National Institute of Standards and Technology (NIST) help organizations improve cybersecurity practices by prioritizing the security controls in the cybersecurity framework. The framework includes a checklist of more than 100 recommendations, which offer high-level guidance that may be difficult for smaller organizations to fully implement.[19] There is a growing consensus in the private sector that organizations must treat cybersecurity as an enterprise-wide risk management challenge.[20] Helping organization identify which security measures to prioritize will help with risk management.

Above all, the federal government can help organizations use available resources to appropriately manage risks by providing clear and focused security recommendations. For example, the Biden administration recently issued a memo to American companies with five specific recommendations to prevent and prepare for ransomware attacks.[21] President Joe Biden's May executive order also includes specific directions for improving information security at federal agencies, such as to "adopt multi-factor authentication and encryption for data at rest and in transit" within 180 days.[22] These directions provide valuable security recommendations for non-federal partners, including state and local authorities.

4. **Congress and the Subcommittee should conduct a strategic review of national cyber threats and assess current and future resource needs to manage long-term cybersecurity risks.**

The recent attacks against state and local government agencies are only the latest serious cyber threats. For a quarter century, national leaders have warned that the United States faces increasing cyber threats jeopardizing American economic and national security. In 2018, the White House estimated that malicious cyber activity cost the United States economy between $57 billion and $109 billion in 2016.[23] Beyond these estimated economic costs, the United States has suffered significant breaches that have undermined national security, such as the 2015 OPM hack and the 2020 Solar Winds breach. Looking forward, the Intelligence Community recently forecast that technological innovations will likely result in increasing competition in the cyber

---

[19] "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework/framework (June 16, 2021).
[20] National Association of Corporate Directors and Internet Security Alliance, *NACD Director's Handbook on Cyber-Risk Oversight* (2020), https://nacdonline.org/insights/publications.cfm?ItemNumber=67298.
[21] Amanda Macias and Christina Wilkie, "Business leaders must take urgent action to counter ransomware threat, White House warns in memo," *CNBC*, June 3, 2021.
[22] The White House, *Executive Order on Improving the Nation's Cybersecurity* (2021).
[23] White House, *The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy* (2018).

domain in the future.[24] Congress should anticipate that these problems will likely grow over time.

Given the scope of the challenge that the nation is facing, Congress and the Subcommittee should examine what resources are being spent on cybersecurity compared to other national security priorities as well as other areas of federal spending. President Biden proposed spending $9.4 billion on federal civilian agency cybersecurity programs in his recent budget request.[25] This represents a 14 percent increase above last year's funding.[26] In comparison, President Biden proposed spending $753 billion on the national defense budget.[27] Congress should review current and anticipated future security threats and consider whether these allocations of resources are appropriately balanced. Beyond national security funding, there are other areas of significant waste that are much larger than what Congress spends on cybersecurity. For example, GAO estimates that the federal government made $175 billion in improper payments in FY2019, including approximately $75 billion reported as a monetary loss.[28]

Since members of the Committee are interested in establishing a new grant program to provide additional resources to state, local, tribal, and territorial governments for cybersecurity, it would be appropriate to identify potential areas of savings in the federal budget and opportunities to reallocate current government spending.

Conclusion

Once again, thank you for the opportunity to testify.

The Unites States faces serious security and fiscal challenges. State, local, tribal, and territorial governments are currently on the front lines facing growing cyber threats. Congress and the Biden administration have an opportunity to help them better manage cyber risks by streamlining federal rules to reduce compliance costs and by sharing useful threat information and security recommendations. For their part, state and local governments have an opportunity to use currently available funding, including more than $2 billion in unspent homeland security grants, to improve their cybersecurity capabilities. Looking forward, Congress and the Subcommittee should review current and anticipated security threats and long-term resource needs to manage cyber risks in the years ahead.

---

[24] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (2021), p.20.
[25] The White House, *FY2022 Budget*, "Information Technology and Cybersecurity Funding," U.S. Defense Department, https://www.whitehouse.gov/wp-content/uploads/2021/05/ap_12_it_fy22.pdf.
[26] Ibid.
[27] "The Department of Defense Releases the President's Fiscal Year 2022 Defense Budget," May 28, 2021.
[28] US Government Accountability Office, GAO-20-344, *Payment Integrity: Federal Agencies' Estimates of FY 2019 Improper Payments*, (2020), https://www.gao.gov/products/gao-20-344.