CompTIA.

July 15th, 2021

The Honorable Chuck Schumer
Democratic Leader
U.S. Senate
322 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mitch McConnell
Republican Leader
U.S. Senate
317 Russell Senate Office Building
Washington, D.C. 20510

Dear Majority Leader Schumer and Minority Leader McConnell:

At CompTIA, we recognize our nation's dire need to advance critical cybersecurity improvements to better protect United States infrastructure. Cybersecurity is a crucial investment for every business, organization, and governmental entity in our country. The importance of cybersecurity has never been more evident than it is today, as we face an increasing number of attacks from malicious actors around the world – with ransomware attacks and cyber threats on the rise over the past several years[1]. The foundation of our global supply chains and critical manufacturing sectors – ranging from food to healthcare to energy and more – are under attack because cybercriminals and state-supported actors understand the wide economic impact and disruption caused by targeting these systems.

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage, and safeguard the technology that powers the world's economy. Through education, training, certifications, advocacy, philanthropy, and market research, CompTIA is the hub for advancing the tech industry and its workforce.

Cybersecurity Must Be a Core Part of Infrastructure Modernization Efforts

Secretary Buttigieg was spot on in his remarks in May 2021 that "cybersecurity has to be core to how we secure our critical infrastructure," as was the White House in its May 2021 Fact Sheet stating, "[c]ybersecurity is a core part of resilience and building infrastructure of the future". To that effect, as Congress and the administration negotiate an infrastructure package, we strongly urge that this historic, once-in-a-generation federal investment include significant funding to ensure that our nation's infrastructure is resilient to all potential harms, including cyber threats. Any infrastructure package should contain legislative provisions that will secure our connected critical infrastructure, enable robust interoperability, and ensure our society's backbone can safely support technological advances. Investing in the resilience of U.S. infrastructure and protecting our systems from cyber threats is to invest in American infrastructure, American jobs, and national security all at once.

[1] https://www.blackberry.com/us/en/products/resource-center/reports/2021-threat-report

CompTIA.

Infrastructure Funding Recipients Must Incorporate Baseline Cybersecurity Protections into Infrastructure Projects

As part of this effort, we urge you to incorporate cybersecurity as a baseline requirement for infrastructure modernization funding and to identify the appropriate gaps in cyber infrastructure. First, public entities and critical infrastructure owners that receive funding from an infrastructure package should be subject to a baseline requirement that they conduct a cybersecurity risk assessment against the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, in order to identify gaps between their current cybersecurity posture and an improved posture based on the assessment. Next, the results of the risk assessment should be used to develop a remediation plan to close identified gaps, including by deploying fundamental risk based vulnerability management practices. Lastly, public entities and critical infrastructure owners should be required to implement the baseline cybersecurity protections outlined in Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger's June 2nd memo.

Conduct Inventory of Operational Technology and Industrial Control Systems

An infrastructure package should include a directive, and the resources necessary, for the Cybersecurity and Infrastructure Security Agency (CISA) to partner with federal civilian agencies to conduct an inventory of federal operational technology and industrial control systems assets. This initiative is critical to gaining visibility into the full range of connected infrastructure in the federal government, which is essential to further the ongoing efforts to bolster federal cybersecurity.

A Software Bill of Materials is Important for Software Supply Chain Security and the Infrastructure it Enables

We also encourage you to advance a crucial aim of President Biden's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity -- to improve software supply chain security. A Software Bill of Materials (SBOM) can be an effective means for improving the integrity and security for software enabling the critical connected infrastructure supported under this plan.

State and Local Government Agencies in Critical Need of Federal Cybersecurity Grant Program

Furthermore, we support the inclusion of programs to adequately fund cybersecurity grant programs at the state and local government level, in order to provide necessary resilience across all units of government in the U.S. To that end, Representative Yvette Clarke (D-NY) has introduced the bipartisan State and Local Cybersecurity Improvement Act (H.R. 3138), which provides a potential model for such a grant program.

Infrastructure Package Should Support Advanced Technology, Such as Artificial Intelligence and Machine Learning, and Basic Cybersecurity Hygiene

Moreover, at CompTIA, we believe the future of technology is evolving at this very moment. In recent years, artificial intelligence and machine learning have been leveraged to develop more powerful cybersecurity tools. We recommend that the infrastructure package support the deployment of such technologies, as well as professional services to protect critical infrastructure from cybersecurity risks.

CompTIA

We also urge you to include in legislation provisions that would maximize the use of vulnerability management, intrusion detection and endpoint security tools to prevent and respond to cyberattacks.

The Federal Government Must Invest in Cyber Workforce

Lastly, the U.S. is expected to face a shortage of 1.8 million skilled cybersecurity workers by 2022, making educating and empowering the next generation of cybersecurity professionals imperative to our future national and economic security. To ensure the implementation of all of these initiatives, it is critical that the federal government must continue to invest in cyber skills and knowledge for government employees, while also seeking creative ways to fill ongoing gaps in the cyber workforce. Furthermore, the federal government must also invest in and leverage technologies that incorporate artificial intelligence and machine learning, which will be essential to filling inevitable cyber labor shortages.

We strongly support efforts in the Senate to use the bipartisan framework to develop a comprehensive infrastructure legislative package. Given the rise of cyberattacks against critical infrastructure, governmental systems, and private sector-owned networks – including those on which the federal government itself is very dependent – it is now more critical than ever to ensure robust and sustainable funding to protect U.S. cybersecurity. We look forward to working with you as we develop critical solutions for today's evolving threats.

Sincerely,

David Logsdon
Staff Director, CompTIA Federal Cybersecurity Committee