ALLIANCE FOR DIGITAL INNOVATION BETTER IDENTITY COALITION CompTIA. Cybersecurity Coalition

February 12, 2021

The Honorable Nancy Pelosi
Speaker
United States House of Representatives

The Honorable Kevin McCarthy
Minority Leader
United States House of Representatives

The Honorable Charles Schumer
Majority Leader
United States Senate

The Honorable Mitch McConnell
Minority Leader
United States Senate

Dear Speaker Pelosi, Majority Leader Schumer, Minority Leader McConnell, and Minority Leader McCarthy:

We are writing to urge the inclusion of dedicated cybersecurity funding in any COVID Relief funding package to bolster the government's ability to protect and defend against future cyber-attacks targeting our government agencies and critical infrastructure providers.

As the president noted in his January announcement of the proposed "American Rescue Plan,"[1] our response to the COVID-19 pandemic and the health of our economy are intertwined. This unprecedented battle against the COVID-19 pandemic has led many businesses and government agencies to push critical services to online, virtual environments with breakneck speed. These efforts have forced our agencies and critical infrastructure partners to quickly move many sensitive systems into newly architected environments to ensure that government workers, critical infrastructure workers, and citizens who rely on services provided by those organizations can virtually interact with one another. While this shift to a virtual environment helps stem the spread of COVID-19, it has left many of these same organizations vulnerable to an expanded and, in some cases, less secure attack surface for hackers.

According to a report published in June of this year[2], nearly half of all workers surveyed indicated that the move to telework caused by COVID-19 was their first experience working from home. Information technology and information security departments at companies and government agencies have struggled to keep pace with the proliferation of new devices on networks due to increased telework and expanded BYOD policies[3]. Increased use of cloud applications and collaboration environments in the wake of COVID-19 has also greatly increased the attack surface that government agencies and critical infrastructure companies face each day[4]. The security and technical challenges associated with rapid cloud adoption and move to telework environments has placed a significant burden on public and private sector entities as they continue to provide critical services helping to fight the pandemic.

The pandemic-accelerated shifts toward more flexible work arrangements will sustain long after we solve the COVID-19 crisis; in fact, Gartner asserts that 2020-21 social distancing has caused a "permanent change in workforce structure," including a 66% growth in remote work from 2019 to 2022 and an acceleration by 5 years of plans to transform infrastructure and operations to a digital framework[5]. Of the workers who have been remote during the pandemic, Gartner estimates that 30% will remain home permanently, 40% home 1-4 days a week, and 30% home one day a week[6], the normalization of which we believe will open economic opportunities to the underemployed (especially to those who need and want more flexible work including part-time, differently abled, and furloughed workers, retirees, and at-home caregivers) thereby creating a more inclusive, sustainable, and robust post-pandemic economy.

The president's American Rescue Plan calls for increased cybersecurity funding to "secure federal IT and networks" and to "boost U.S. defenses, including of the COVID-19 vaccine process." To do this effectively, the president calls for the following:

- $690 million for the Cybersecurity and Infrastructure Security Agency (CISA) to bolster security monitoring and incident response activities, including piloting new shared security services; and
- $200 million in Information Technology Oversight and Reform funding to bolster hiring of cybersecurity and engineering experts;
- $300 million for the General Services Administration (GSA) to build secure shared services for government agencies to leverage as they continue to modernize their IT environments in response to COVID-19;
- $9 billion in the Technology Modernization Fund to fund the launch of "major new IT and cybersecurity shared services" at CISA and GSA.

The Director of the Office of Management and Budget nominee, Neera Tanden, stated in her nomination hearing on February 9, 2021, "Of particular concern is the fact that the federal government spends more taxpayer dollars on maintaining old legacy IT systems than investing in new, agile, and secure systems." She also noted that, "this not only opens federal systems up to cyber-attacks, but also fails to provide the level of customer service that the American people expect in the 21st Century." We agree with Ms. Tanden's statements and strongly support all investments in funding to bolster cybersecurity whether directly through cybersecurity workforce expansion or through secure development, design, and deployment of more modern systems.

As we have seen in the recent SolarWinds compromise of both federal government and critical infrastructure companies, the need to invest in our nation's ability to protect against, detect, respond to, and recover from these attacks is critical. Our government agencies and critical infrastructure companies rely on information and communication technology (ICT) to facilitate critical government services and modern economic growth. This incident, which targeted the ICT supply chain and identity management trust relationships, further underscores the need for robust and sustained funding for government organizations who lead the fight to identify and counter the persistent and growing cybersecurity threats against our government agencies and critical infrastructure companies. In addition, the government and its critical infrastructure partners are moving to fully understand the impact of the SolarWinds incident. These ongoing discovery and remediation efforts will take significant time and resources given the nature of the breach. Therefore, investment in our government agencies with funds that can be used over multiple years is essential to sustaining the efforts to support the long-term remediation and recovery efforts happening across our government agencies and critical infrastructure partners.

We also support the direct investment in cybersecurity shared services that government agencies and/or critical infrastructure owners and operators can leverage to bolster their defenses, such as for more robust digital identity infrastructure. Healthcare, transportation, energy, utilities, and other critical infrastructure industries are increasingly digitizing their operations. The cyber attack last week against the water treatment plant in Oldsmar, Florida, where hackers were able to change the amount of lye in the city's drinking water for a brief period of time, highlights the critical importance of managing the cybersecurity challenges associated with the convergence of IT and Operational Technology and Industrial Control System environments.

In addition to the above investments, there is an urgent need for cybersecurity funding for state and local entities that have already faced significant cyber events such as the city of Baltimore ransomware attack in 2019[7]. COVID-19 has caused the same shifts to remote work for state and local governments, further increasing the cybersecurity attack surface. As states mobilize to provide support to health systems, to administer and track vaccinations, and to digitize as many critical government services as possible, they need additional, dedicated funding for cybersecurity services. Targeted state funding will help secure supply chains, reduce fraudulent behavior, and create resiliency in new systems that need to function consistently at the highest levels. We strongly urge Congress to expressly call out cybersecurity as one of the critical areas in which states can use additional COVID-19 relief funding.

Sincerely,

The Cybersecurity Coalition
The Better Identity Coalition
The Alliance for Digital Innovation (ADI)
The Computing Technology Industry Association (CompTIA)

Cc:

Chairman Patrick Leahy and Vice Chairman Richard Shelby of the U.S. Senate Appropriations Committee

Chairman Chris Murphy and Ranking Member Shelley Moore Capito of the U.S. Senate Homeland Security Appropriations Subcommittee

Chairman Chris Van Hollen and Ranking Member Cindy Hyde-Smith of the U.S. Senate Financial Services and General Government Appropriations Subcommittee

Chairman Gary Peters and Ranking Member Rob Portman of the U.S. Senate Homeland Security and Government Affairs Committee

Chairman Bennie Thompson and Ranking Member John Katko of the U.S. House Committee on Homeland Security

Chairwoman Carolyn Maloney and Ranking Member James Comer of the U.S. House Committee on Oversight and Reform

[1] https://www.whitehouse.gov/briefing-room/legislation/2021/01/20/president-biden-announces-american-rescue-plan/

[2] https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Morphisec-2020-WFH-Employee-Cybersecurity-Threat-Index-FINAL.pdf

[3] https://www.law.com/2020/07/15/companies-may-be-refreshing-bring-your-own-device-policies-during-covid-19/?slreturn=20210111184129

[4] https://www.securitymagazine.com/articles/93687-remote-work-and-covid-19-brings-new-challenges-in-securing-cloud-services

[5] Ranjit Atwal, Neha Gupta, Dean Blackmore, Christian Canales, Grigory Betskov. “Forecast Analysis: Remote Work IT Spending, Worldwide.” 5 January 2021

[6] Gartner. “Forecast Analysis: Remote Workers Forecast, Worldwide.” 21 August 2020

[7] https://mayor.baltimorecity.gov/city-baltimore-faq