



Internet Association

The Honorable Patrick Leahy
Chairman
U. S. Senate Committee on Appropriations
Washington, D.C. 20510

The Honorable Richard Shelby
Vice Chairman
U.S. Senate Committee on Appropriations
Washington, D.C. 20510

The Honorable Rosa L. DeLauro
Chair
U.S. House Committee on Appropriations
Washington, D.C. 20515

The Honorable Kay Granger
Ranking Member
U.S. House Committee on Appropriations
Washington, D.C. 20515

May 19, 2021

Dear Chairman Leahy, Chair DeLauro, Vice Chairman Shelby, and Ranking Member Granger,

We are writing today to urge you to increase the Cybersecurity and Infrastructure Security Agency's (CISA) budget to effectively meet the cybersecurity challenges and threats our country is facing today as well as in the years ahead. In order to do this, we encourage you to increase the 302(b) allocation, specifically the 050 budget funding allocation, for the fiscal year 2022 (FY22) Homeland Security Appropriations Subcommittee by \$750 million or to ensure a commensurate increase happens if there is no 050 breakout.

Over the last year alone, our country's government agencies and private sector companies have been attacked repeatedly by both nation actors and cyber criminals seeking to steal our nation's intellectual property and harvest our most sensitive information. The recent SolarWinds, Colonial Pipeline, and Pulse Connect Secure attacks have shown just how vulnerable our public and private sector information technology (IT) systems are to these nation state actors and cyber criminals.

These attacks come on top of our unprecedented battle against the COVID-19 pandemic, which led many government agencies and businesses to push their workforce and critical services to virtual and remote environments. To do this, many organizations have quickly shifted



Internet Association

significant portions of the IT infrastructure to cloud based and hybrid environments and rearchitected the way they deliver services. While this shift helps stem the spread of COVID-19, it has left many of these same organizations vulnerable to an expanded and, in many cases, less secure attack surface that can be exploited by hackers. Importantly, as the country comes back from the pandemic, many of the changes that have enabled remote work will likely remain in place, creating a more permanent, expanded attack surface.

Given this combination of larger attack surfaces and increased use of sophisticated cyber-attacks by our adversaries, we must act quickly to strengthen our nation's security posture. CISA has the mandate to protect, defend, and secure both federal agency and critical infrastructure IT and communications systems from these growing threats. We were encouraged by Congress's \$650 million investment in CISA as part of the American Rescue Plan; however we recognize that this was meant as an immediate, one-time capital infusion to combat some of challenges outlined above. While this quick injection of capital will be used to address immediate short-term challenges, it represents only a tiny fraction of the long-term investment needed to build and empower CISA to meet the challenges of protecting our nation's federal agencies as well as our critical infrastructure.

It is imperative that Congress take a long-term approach to growing CISA into an agency fully capable of dealing with today's challenges while preparing our nation's IT and communications infrastructure for the challenges of tomorrow. To do this, we **strongly urge** the committee to increase the 050 budget funding allocation for the fiscal year 2022 (FY22) Homeland Security Appropriations Subcommittee by \$750 million to address the growing threat of cybersecurity attacks to our nation.

In fiscal year 2021 (FY21), the 050 budget authority was \$750.7 billion. Of that amount, only \$2.55 billion or 0.34 percent was allocated to DHS of which \$2.02 billion or 0.27 percent went to CISA.¹ Increasing the 050 allocation for the Homeland Security Appropriations bill by \$750

¹ [OMB Final Sequestration Report to the President and Congress for Fiscal Year 2021](#)



Internet Association

million would materially improve CISA's ability to meet its critical cybersecurity mission. Specifically, we recommend this money go towards:

- Offering shared services that augment agency and critical infrastructure cybersecurity risk management plans
- Accelerating and expanding the Continuous Diagnostics and Mitigation (CDM) program to build out the core cyber defenses for federal departments and agencies
- Expanding the National Cybersecurity Assessments and Technical Services program to protect national critical infrastructure
- Expanding outreach services and funding to more fully assist state and local governments
- Enhancing sector engagement capacity to increase outreach and improve information sharing between CISA and the critical infrastructure sectors
- Modernizing or replacing current government-wide protection programs like the National Cybersecurity Protection System to take advantage of automation, behavioral analytics, and other defenses
- Promoting more modern, more secure designs of our federal IT networks through approaches like Zero Trust Architectures.
- Investing in cyber professionals and upskilling the cybersecurity workforce, while concurrently ensuring that cyber billets throughout government are appropriately aligned to available funding.

As the lead civilian cybersecurity agency, CISA is responsible for protecting the federal ".gov" network and the security of the nation's critical infrastructure. Because of its cybersecurity mission, the bulk of CISA's funding is directly tied to the defense or 050 allocation provided to the Homeland Security Appropriations Subcommittee. Unless the Committee significantly increases the Subcommittee's 050 allocation, CISA will not have the funding necessary to support its critical mission.

Additionally, we recommend that the Committee continue to expand this allocation over the next several years commensurate with the growth in CISA's mission and capabilities. Based on



Internet Association

conversations with CISA, our public sector partners, and our private sector colleagues, we believe that CISA’s annual operating budget – and therefore its 050 allocation – should grow to \$5 billion over the next decade, if not sooner. This robust and sustained funding will allow CISA to invest in the capabilities it needs to meet the challenges of defending and hardening our IT and communications infrastructure.

Our daily life, economic vitality, and national security depend on a stable, safe and resilient digital infrastructure. Defending and hardening that digital infrastructure should be of the utmost priority to Congress. Given this urgency, we strongly encourage the committee to raise CISA’s 050 allocation or ensure a commensurate increase in FY 2022 and beyond.

Sincerely,

Alliance for Digital Innovation
CompTIA
Cybersecurity Coalition
ITI
Internet Association

CC:

House Appropriations Homeland Security Subcommittee Chairwoman Lucille Roybal-Allard
House Appropriations Homeland Security Subcommittee Ranking Member Chuck Fleischmann
Senate Appropriations Homeland Security Subcommittee Chairman Chris Murphy
Senate Appropriations Homeland Security Subcommittee Ranking Member Shelley Moore
Capito