



December 9, 2022

The Honorable Patrick Leahy
Chairman, Appropriations Committee
United States Senate

The Honorable Richard Shelby
Vice Chairman, Appropriations Committee
United States Senate

The Honorable Rosa DeLauro
Chair, Appropriations Committee
United States House of Representatives

The Honorable Kay Granger
Ranking Member, Appropriations Committee
United States House of Representatives

Re: Fiscal Year 2023 Appropriations for Technology and Cybersecurity Modernization

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

Our group, the Alliance for Digital Innovation (ADI), is a nonpartisan alliance of the nation's most cutting-edge technology firms. Our members represent key critical technologies at all levels of the federal government's technology stack, including cloud infrastructure, digital identity, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services critical to the United States' national security. Our mission is to break down barriers for government to bring the technological advancements in commercial innovation to the public sector to build a modern, 21st century digital government.

We are following up on the letter we sent to you on May 31, 2022¹ regarding ADI's recommendations for prioritization of funding in the various FY 2023 appropriations bills. In that letter, we highlighted the need to meet the President's request for funding in the Technology Modernization Fund (TMF) and the Federal Citizen Services Fund. Additionally, we advocated for focused cybersecurity enhancement funding, increases in funding for the Cybersecurity and Infrastructure Security agency, leveraging the authorities of the Modernizing Government Technology (MGT) Act² to enable individual agency working capital funds, and broader

¹ <https://alliance4digitalinnovation.org/wp-content/uploads/2022/06/ADI-FY23-Appropriations-Letter-05-31-2022.pdf>

² <https://www.congress.gov/115/bills/hr2227/BILLS-115hr2227rfs.pdf>

flexibilities in the color of monies that are used for IT modernization, technology procurement, and cybersecurity protections.

As Congress enters into a critical time for finalizing appropriations for FY 2023, we urge Congress to consider the importance of this appropriations process as it relates to IT modernization, cybersecurity enhancement, and technology procurement. Given the continued discussions and negotiations between the House and the Senate, ADI asks Congress to consider the following areas as Members work through the final stages of a potential omnibus appropriations bill.

Additional Funding for the Technology Modernization Fund (TMF).

Earlier this year, the Administration requested \$300 million in its FY 2023 budget request. ADI notes that the House mark includes \$100 million for the TMF while the Senate bill does not include additional funding. We understand that Congress must make difficult decisions, especially given the topline allocations for each appropriations bill. That said, given the number of outstanding TMF proposals — 130 proposals from 60 agencies and components totaling over \$2.5 billion, according to the director of the TMF program management office — we strongly urge the adoption of the House mark of \$100 million in FY 2023.

With this additional funding, ADI supports Congress' efforts to provide additional oversight of the fund and the specific projects that are awarded. ADI believes that the priorities of the various agencies should align with the efforts of the Administration and Congress to improve both the customer experience of citizen services and cybersecurity of the agencies.

Increase Amount and Cap of the Federal Citizen Services Fund (FCSF).

The GSA FCSF supports some of the biggest programs driving innovation and enabling security compliance. In FY 2023, the Administration has requested \$116 million for the fund to support GSA's vision for fully managing and improving shared services at the Technology Transformation Service (TTS). The House bill fully funds the FCSF at the level requested by the Administration. The Senate bill provides a slight increase from years past at \$57.8 million. As we have noted in prior letters, this fund allows GSA to operate the Federal Risk and Management Program (FedRAMP), which has accredited over 245 unique cloud offerings that have been reused approximately 3,500 times across the federal government. Additionally, GSA estimates that the FedRAMP program has saved the government \$700 million in agency assessment and authorization costs when bringing in new, modern cloud-based technology.³

ADI believes that the current FCSF funding levels lead to a budget for FedRAMP that is insufficient to meet the demand. Therefore, ADI encourages Congress to align with the House-passed funding for the FCSF, which would enable greater commercial technology access across agencies while maintaining a high bar for security.

³ https://www.gsa.gov/cdnstatic/GSA_FY_2023_CJ_Optimized.pdf

Focused Cybersecurity Enhancement.

Over the last several years, federal departments and agencies have seen major cybersecurity incidents and vulnerabilities, such as the SolarWinds incident⁴ and the Log4j vulnerability.⁵ In response to this proliferation of dynamic cybersecurity threats, policymakers have issued an Executive Order,⁶ several policies⁷ and strategies,⁸ and many other pieces of collateral⁹ and guidance¹⁰ to departments and agencies. The FY 2022 appropriations bills provided a combination of budget increases and specific line items for cybersecurity for some of the agencies impacted by the SolarWinds attack. However, all agencies must continue to invest in their cybersecurity defenses to meet the requirements issued by policymakers to restructure their environments and implement modern cloud-based cybersecurity tools and services.

Currently, several bills in the House and a few bills in the Senate either expand the operations budget of the Chief Information Officer for cybersecurity or create specific cybersecurity “enhancement” accounts. ADI supports these efforts and encourages the appropriations committees to exceed the Administration’s 11 percent increase in cybersecurity funding for federal civilian agencies. Given the influx in cybersecurity policies, agencies are struggling to meet the requirements today that they have not been able to adequately budget for during the FY 2023 process. The Office of Management and Budget acknowledges this lag time in its Zero Trust Strategy when it asks agencies to submit a budget estimate for FY 2024. Given the urgency of requirements, ADI encourages Congress to provide additional resources in FY 2023 to assist agencies in achieving critical cybersecurity milestones.

Cybersecurity and Infrastructure Security Agency (CISA).

The Cybersecurity and Infrastructure Security Agency (CISA) is an important partner in protecting our public sector networks and environments. For FY 2023, the Biden Administration asked for \$2.5 billion to support operations, research and development, and several cybersecurity shared services. Currently, the House bill provides CISA with \$2.93 billion and the Senate bill provides CISA with \$2.91 billion to achieve their mission objectives. ADI supports the committees’ efforts to fully fund CISA’s efforts above the Administration’s request. As we stated in our previous letter, ADI supports the continued funding of the National Cybersecurity Protection System (NCPS) and the Continuous Diagnostics and Mitigation Program (CDM) while they transition from hardened local network protections to more internet and cloud-based zero trust services. ADI also supports continued investments in operational technology and funding for projects and programs that address internet of things (IoT), industrial control systems (ICS)

⁴ <https://www.cisa.gov/uscert/remediating-apt-compromised-networks>

⁵ <https://www.cisa.gov/news/2021/12/17/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-apache-log4j>

⁶ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

⁷ <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

⁸ <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>

⁹ <https://www.cisa.gov/news/2021/09/07/cisa-releases-cloud-security-technical-reference-architecture-and-zero-trust>

¹⁰ <https://www.cisa.gov/binding-operational-directive-23-01>

security, and sector-specific cybersecurity challenges. Fully funding CISA will help federal, state, and local governments transition from legacy cybersecurity tools and services to more modern, cloud-based cybersecurity environments.

Authorizing Additional Working Capital Accounts and Extended Color of Money.

ADI appreciates the continued support of many of the appropriations committees that have authorized use of the working capital funds created by the Modernizing Government Technology (MGT) Act.¹¹ These funds will allow agencies to reallocate resources to assist with modernization of technology and investments in critical cloud-based commercial solutions. ADI recognizes that many committees have included this language; however, there are still others that are not taking advantage of the flexibility provided by these authorized funds. ADI strongly encourages the subcommittees that have not authorized use of the MGT working capital funds to do so in the FY 2023 bill, especially for small and independent agencies. Additionally, as we stated in the previous letter, investments in modern, cloud-based architectures and modern zero trust cybersecurity environments often take several years to plan for and implement. While agencies can move quickly, these types of large-scale information technology transitions often require multiple years to fully complete. To assist with these multi-year time horizons, ADI urges the appropriations committee to consider leveraging its use of flexible timing of appropriated dollars by providing agencies with “multi-year” or “no-year” funding as part of their technology budgets.

Finally, ADI appreciates the Senate Financial Services and General Government (FSGG) Subcommittee’s efforts to fully leverage existing funds to bolster modernization efforts as authorized in Sec. 721 of the FSGG appropriations legislation. ADI supports creation and utilization of all flexibilities that enable agencies to modernize government services and improve cybersecurity. ADI believes that this fund will allow for the Chief Information Officer (CIO) council and other councils to collectively work on specific, cross agency services that can benefit multiple agencies. That said, ADI encourages the committee to provide additional flexibilities that allow those funds to augment other projects selected as part of the TMF work. ADI also urges the committee to consider providing seed funding to help drive some of the initial investments that are in addition to the current funding for the TMF provided by the House bill. Finally, ADI believes that these flexibilities are important but should not be considered a substitution for broad investments in technology through programs like the TMF and the FCSF. We believe that all possible flexibilities and funding pathways must be leveraged to achieve the cloud-forward, modernization goals that will enable better customer experience and more secure technology environments. As the committee considers adding flexibilities, we encourage you to add similar flexibilities to other funds that invest in IT modernization and promote use of cloud-based commercial technologies and services.

Investments in Quantum Computing.

Several agencies are looking to make investments in quantum computing, but some are taking different approaches. The multi-agency National Quantum Initiative (NQI) was deliberately crafted to be technology-neutral, and this neutrality should be maintained in any and all quantum-

¹¹ <https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf>. The MGT Act was passed as part of the National Defense Authorization Act of 2018.

related appropriations and authorization bills. Quantum Information Science (QIS) is a multi-disciplinary field and includes a wide array of quantum technologies. However, the FY23 Energy and Water appropriations reports could potentially narrow the focus of our government's efforts and hinder our nation's ability to be a global leader in quantum technology innovation. The report language currently calls out only two of many quantum modalities: photonics and ion traps. This could significantly limit the government's focus. This language should be removed from the appropriations and replaced with technology-neutral language.

Thank you for your long-standing partnership and engagement with the private sector and for considering our views on the FY 2023 appropriations legislation. We look forward to working with you to drive modernization, security, and digital innovation across the federal government. Please consider us a resource as the committee continues to deliberate on the FY 2023 appropriations legislation.

Sincerely,

The Alliance for Digital Innovation

Cc: The Honorable Chris Van Hollen
The Honorable Cindy Hyde-Smith
The Honorable Mike Quigley
The Honorable Steve Womack
The Honorable Chris Murphy
The Honorable Shelley Moore Capito
The Honorable Lucille Roybal-Allard
The Honorable Chuck Fleischmann