ALLIANCE FOR DIGITAL INNOVATION

May 31, 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.

Public sector institutions today face critical decision points about whether and how to leverage modern, commercial technologies to deliver services more effectively to our nation's citizens, defend our homeland from physical and digital threats, and develop technology ecosystems that can grow with their dynamic missions. In the wake of several significant cybersecurity incidents and in response to the pandemic, the Biden Administration has published executive orders, memoranda, and policies that provide direction to federal agencies that move them away from the status quo toward more extensible, flexible, and secure commercial technology solutions[1]. Additionally, the Biden Administration has pushed Executive Branch mission owners to embrace and plan for future technologies such as artificial intelligence and quantum computing.

[1] These documents include *EO 14028, Improving the Nation's Cybersecurity*, *EO 14058, Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*, and *EO 14073, Enhancing the National Quantum Initiative Advisory Committee*, as well as all the Office of Management and Budget (OMB) memoranda, the National Security Memoranda, and the agency guidance documents that have come from or been released with those executive orders.

Congress has done its part to provide federal agencies with both the authority and resources to plan for and adopt new and emerging technology for both mission and enterprise purposes. ADI supports the work accomplished to date – including the appropriation of $1 billion for the Technology Modernization Fund (TMF) as part of the American Rescue Plan Act (P.L. 117-2) as well as the infusion of capital into the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) to bolster cybersecurity efforts across the government and industry.

As the Appropriations Committees work through the development of the Fiscal Year 2023 appropriations bills, we are writing to highlight the areas of investment that are critical to allowing our government to modernize their environments and deliver on the mission essential adoption of modern technology. Below are several areas of investment that ADI supports as well as some critical flexibilities that ADI encourages appropriators to consider as they work with agencies to develop the FY 2023 federal budget.

Additional Funding for the Technology Modernization Fund (TMF).
According to the director of the program management office, the TMF board has received 130 proposals from 60 agencies and components. These proposals, taken together, equal $2.5 billion in proposed investments from the federal government[2]. This demand signals the high level of agency need for modernizing and securing networks outside of the annual appropriations process. The Administration has asked for $300 million in its FY 2023 budget request. ADI believes that $300 million is the minimum amount needed to continue to meet the needs identified by agencies. We encourage Congress to work with agencies to fully understand the backlog of modernization proposals and **either meet or exceed the president's request for additional TMF Funds**. Specifically, we recommend that the committee consider targeted efforts to fund zero trust projects to enhance security and to fund modernization efforts at agencies that provide critical services in line with the identified High Impact Service Providers[3].

At the same time, ADI encourages continued oversight of the TMF process. ADI members directly support many of the agencies that have developed and submitted proposals and – in some circumstances – been awarded funding. While there is an urgency to begin implementation, ADI understands that these multi agency and cross agency projects often have bureaucratic hurdles to overcome before work can begin. We encourage the appropriations committee to work closely with the Office of Management and Budget (OMB) and General Services Administration (GSA) leadership to identify and break down any barriers as agencies move forward with their modernization efforts.

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. The administration has requested $116 million for the fund, which is more than double its current budget. ADI supports this request and encourages the committee to meet or

[2] https://federalnewsnetwork.com/ask-the-cio/2022/05/federal-cio-martorana-says-agencies-adjusting-to-tmf-2-0-model/
[3] https://www.performance.gov/cx/assets/files/HISP-listing-2021.pdf

exceed that number. This fund allows GSA to operate the Federal Risk and Management Program (FedRAMP), which has accredited over 245 unique cloud offerings that have been re-used 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.[4]

ADI believes that the current FCSF budget for FedRAMP is insufficient to meet the demand. Given the lengthy process to grant provisional authorizations to operate (ATOs) and to regularly monitor changes to cloud services, the FedRAMP program has turned into a bottleneck for companies to be able to achieve compliance. This bottleneck also acts as a disincentive for new commercial solutions to sell to government customers. By increasing the funding in the FCSF, GSA can significantly increase the throughput of companies seeking authorizations and approval at both the Joint Authorization Board (JAB) as well as at various agencies. Finally, this funding can help the FedRAMP program invest in approaches that will enable the program to leverage technology to automate some of its processes, such as moving towards more continuous authorization and monitoring. To do this effectively, the program must invest in resources to incorporate automation into the review and approval process. By increasing the funding for the FCSF, Congress can enable greater commercial technology access across agencies while maintaining a high bar for security.

Focused Cybersecurity Enhancement.

In the wake of the SolarWinds incident, the Biden Administration requested $750 million in 2021 for the impacted federal agencies to invest in and shore up their cybersecurity defenses. The appropriations committee provided much of the requested funds to the various agencies in FY 2022 via agency specific cybersecurity enhancement accounts. While this infusion of capital has helped many of the impacted agencies start their recovery process and begin the work of rearchitecting their environments, many agencies – including some that were impacted – did not receive an increase in enterprise cybersecurity funding. Additionally, the Administration has released OMB M 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[5] to provide all agencies with guidance on shoring up their defenses in the wake of the SolarWinds incident. To begin meeting these requirements, the FY 2023 budget calls for an 11 percent increase in cybersecurity funding for federal civilian agencies. With the new requirements to move to zero trust environments, ADI fully supports this request for increased cybersecurity spending and encourages appropriations subcommittees to work with their agencies to fully understand and appropriate the funding needed to invest in new technologies to build out their zero trust environments. ADI anticipates this will be the first of a multi-year funding request from agencies to meet these new requirements.

Cybersecurity and Infrastructure Security Agency (CISA).

The Cybersecurity and Infrastructure Security Agency (CISA) continues to play a critical role in securing our federal agencies as well as providing important services to our critical infrastructure partners. Commensurate with the evolving threat landscape, CISA's budget has continued to

[4] https://www.gsa.gov/cdnstatic/GSA_FY_2023_CJ_Optimized.pdf

[5] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

grow over the last several years. FY 2023 is no exception. The Biden Administration is asking for over $2.5 billion to support operations, research and development, and several cybersecurity shared services. ADI encourages the committee to support the requested spending while, at the same time, encouraging CISA to evolve its delivery of the federal network defense mission. Specifically, both the National Cybersecurity Protection System (NCPS) and the Continuous Diagnostics and Mitigation Program (CDM) were constructed to support older security architectures and legacy agency environments. These protections should continue to support agencies as they transition away from hardened local networks to more internet and cloud-based zero trust environments that leverage operational technologies, creating expanded attack surfaces. Additionally, ADI recommends the committee fund efforts to get ahead of cybersecurity challenges that will arise with greater use of the internet of things (IoT), industrial control systems (ICS), as well as the continued use of legacy systems that cannot be patched and maintained.

Authorizing Additional Working Capital Accounts and Extended Color of Money. ADI appreciates the efforts of the appropriations committee to help agencies securely modernize their environments and to invest in new technology. One tool that ADI urges the committee to consider leveraging is the use of flexible timing of appropriated dollars. To achieve the outlined goals of modernizing customer experience and securing our agency enterprises, departments and agencies must have the ability to undertake bigger, enterprise-wide projects that often take several years to fully implement. The appropriations committee can give agencies this flexibility by allowing unused funding to be placed in working capital funds authorized under the Modernizing Government Technology (MGT) Act[6] and by providing agencies with “multi-year” or “no-year” funding as part of their technology budgets. ADI appreciates the flexibility given to several agencies to leverage their working capital funds as part of the FY 2022 omnibus. We encourage the committee to continue these efforts and allow all agencies to leverage their working capital funds for technology modernization as the committee finalizes the FY 2023 appropriations bills. Further, we encourage the committee to explicitly extend Working Capital Fund authority to small and independent agencies, in addition to the CFO Act agencies whose funds were authorized in 2017.

Thank you for your long-standing partnership and engagement with the private sector and permitting ADI to share its views on the Administration’s Budget request. 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

[6] 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.

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