The Honorable Mitch McConnell
Majority Leader
United States Senate
317 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Richard Shelby
Chairman–Committee on Appropriations
United States Senate
U.S. Capitol, Room S-128
Washington, D.C. 20510

The Honorable Charles E. Schumer
Minority Leader United States Senate
322 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Patrick Leahy
Vice Chairman–Committee on Appropriations
United States Senate
U.S. Capitol, Room S-128
Washington, D.C. 20510

Re: Support for IT Modernization to Improve COVID-19 Pandemic Response and Relief Efforts

Dear Senators:

As deliberations continue regarding additional legislative package(s) to provide resources for COVID-19 response and recovery efforts, the undersigned organizations urge the inclusion of funding for federal and state information technology (IT) and cybersecurity modernization initiatives that enable effective and secure program delivery, as well as meaningful mission outcomes.

To date, public sector Chief Information Officers (CIOs) have performed commendably as they have sought to ensure continuity of operations while also ramping up IT systems that facilitate government management and oversight of COVID-19 recovery initiatives. However, the prevalence of outdated legacy IT continues to hamper the effectiveness of recovery efforts. Citizens are being denied positive digital government experiences as they seek access to much needed programs, such as securing business loan programs, receiving economic security payments, or applying for unemployment benefits.

These issues, and many other IT and cybersecurity challenges across numerous Federal agencies were recently detailed in the first report from the Pandemic Response Accountability Committee (PRAC).[1] These problems are not limited to the Federal government but also extend to state, local, tribal, and territorial (SLTT) governments as well. Although these government entities, even in times of incredible duress, have performed admirably in scaling and managing the delivery and security of their IT systems, infrastructure, and services, Congress must continue to provide flexible, agile funding that

[1] The Pandemic Response Accountability Committee (PRAC) was created in the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), Pub. L. 116-136 §15010.

can be leveraged by SLTT governments to address issues that will propagate as employees either come back to office buildings to perform their work or maintain a continued enhanced telework posture.

Congress' work to provide necessary funding to address current and expected technology and cybersecurity challenges should be a high order priority in any subsequent relief and response package.

There are numerous options Congress can pursue in supporting effective, targeted, and appropriate funding for commercial technologies and cybersecurity capabilities that are of immediate need. As the public sector continues to address the COVID-19 pandemic, increasing economic insecurity, and broader recovery efforts at the Federal and state level, more funding will become essential at all levels of government.

Technology Modernization Fund

In 2017, Congress enacted the Modernizing Government Technology (MGT) Act, which created a centralized "Technology Modernization Fund" (TMF) within the General Services Administration (GSA) that agencies could borrow from to effectively finance broad, government-wide IT modernization projects. However, only token amounts of funding have been provided to the TMF in prior years, limiting the impact that this transformative IT financing mechanism can have across the Federal enterprise.

It was heartening to see that the House HEROES Act would provide $1,000,000,000 to the TMF, which would represent the most meaningful, centralized effort to improve agency IT systems and digital transformation in recent history. We encourage the Senate to provide the same amount, or more, to the TMF. This will enable government to quickly and effectively leverage commercial capabilities and services that are vital for maintaining operations, deprecating legacy systems, and improving the ability of agencies to manage IT resource effectively throughout changing circumstances.

One of the reasons the TMF can be particularly powerful during these unique times in agency operations is that the fund has several built-in transparency mechanisms, which include the submission of spending plans to Congress, quarterly public status reporting, and preferences for adoption of commercial capabilities. The TMF is also overseen by a Board of the government's top technology, acquisition, and financial management experts, meaning that all TMF projects pass rigorous vetting. For all of these reasons, and because such funding can enable a more immediate and credible response to COVID-19, we strongly urge your support of this key fund.

Elimination or relaxation of onerous requirements to pay back the TMF if borrowing agencies use the funding for COVID-19-related IT modernization initiatives would also spur greater utilization of TMF resources by eliminating the significant disincentive of having to accurately calculate the ability to payback any TMF loans.

IT Working Capital Funds

The MGT Act also authorized the creation of IT working capital funds within federal agencies that were intended to provide flexibility to agencies to fund IT upgrades. However, because of issues related to the original legislative text or variances in agency authorities, such funds have not been widely implemented. As agencies deal with the critical challenges and opportunities created by the COVID-19 response and recovery, it is imperative that Congress provide necessary authorities to

the requisite Federal agencies so they can make smarter, more financially sound investments in IT modernization and cybersecurity.

Funding for State Local and Territorial Government

It is vital Congress provide targeted funding to State, Local, Tribal, and Territorial (SLTT) governments specifically to address the incredible service delivery and cybersecurity challenges occurring beyond the Federal level. Malicious cyber actors have used attention on COVID-19 to their advantage, continuing to target SLTT government and individual citizens with ransomware, phishing, and computer-enabled financial fraud. SLTT governments are on the front lines of program delivery for key Federal assistance programs, such as unemployment insurance and ensuring citizens have access to appropriate information and resources to deal with COVID-19 related disruptions. However, many of the IT systems and websites that deliver these services are prone to numerous cybersecurity vulnerabilities, run on outdated legacy infrastructure that undermines performance, and fail to provide the ease, accuracy, and usability that citizens have come to expect in their personal lives through enhanced commercial technologies. It is critical that Congress take this unique opportunity to make evidently necessary and profoundly important investments in the modernization and security of SLTT information systems so they can protect citizen data, improve digital service delivery, and ensure that state and local governments are able to effectively and capably adjust to changing dynamics as the country continues to deal with our current and future exigent circumstances.

Continuous Diagnostics and Mitigation

Federal agencies are undergoing unprecedented attacks from malicious actors. The COVID-19 pandemic has dramatically exacerbated this problem. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program provides critical help to agencies so they can identify potential vulnerabilities, mitigate threats, or respond to potential cybersecurity attacks. Although Congress has provided trillions of dollars in recent legislation to help agencies recover and respond to COVID-19, there has not been a corresponding investment in the CDM program and vital cybersecurity products and services it provides to agencies. Due to the dramatic increases in CDM services required of the agencies that have taken on the largest response efforts (and rightly so), there may be challenges in providing necessary cybersecurity protections to other agencies which still face elevated risks. In order to enhance effective cybersecurity across the Federal enterprise and to ensure that agency CDM requests are met, we strongly encourage Congress to provide additional funds to this vital program.

Below, we reiterate previous requests we have made to Congress[2] and strongly encourage the inclusion of the following priorities in any upcoming response and recovery legislation:

1. Support the Technology Modernization Fund (TMF) at a level that would allow for meaningful investment in cross-agency IT modernization initiatives. To expedite the resourcefulness of such funds, existing requirements directing agencies to payback TMF funds should be relaxed when such funds are tied to pandemic or disaster recovery efforts;
2. Provide direct funding to federal agencies to modernize and secure IT systems beneficial to COVID-19 and future emergency responses. Such funding should be made available for

[2] A copy of the letter sent to Congressional leaders on April 15, 2020 can be found here: https://alliance4digitalinnovation.org/wp-content/uploads/2020/04/Multiassociation-Letter-to-Congress_IT-Principles-for-Future-Stimulus-2.pdf

expenditure over multiple years, but does not necessarily need to flow through agency working capital funds;

3. Establish and fund a mechanism that provides federal financial support to state and local government agencies in need of IT modernization and upgrades to foster better recovery efforts. Such investments should focus on interoperability between programs that rely on federal, state, and local IT systems, where applicable. Language providing additional resources to the Coronavirus Relief Fund for IT improvements is an avenue Congress should explore;
4. Provide necessary legislative authority for agencies to establish IT working capital funds with strong governance and reporting requirements to enable both Congress and the Executive Branch to more effectively budget for and finance significant IT modernization initiatives;
5. Support funding to improve the Federal Risk Authorization and Management Program (FedRAMP) cloud technology security program by automating the security authorization process to increase government access to secure commercial cloud service and technology providers
6. Provide increased funding to the CDM program so that DHS can promptly and completely fulfill all requests for service and ensure robust threat detection and mitigation against increased adversarial attacks at all Federal agencies;
7. Establish a dedicated cybersecurity grant program for SLTT governments to enable greater resiliency and enhanced security of critical technology systems and networks; and
8. Ensure that IT modernization efforts include focused attention and investment in commercial technologies that strengthen cybersecurity, empower effective workforce training, and ensure robust digital transformation.

The attached document provides additional details and recommendations. We look forward to working with the Senate on this matter that directly affects pandemic response efforts and the delivery of relief to the public during this unprecedented time.

Thank you for your consideration.

Sincerely,

The Alliance for Digital Innovation
BSA | The Software Alliance
Coalition for Procurement Advocacy
CompTIA
Cybersecurity Coalition
Information Technology Industry Council (ITI)
Internet Association