February 2, 2021

The Honorable Nancy Pelosi
Speaker
United States House of Representatives

The Honorable Charles Schumer
Majority Leader
United States Senate

The Honorable Kevin McCarthy
Minority Leader
United States House of Representatives

The Honorable Mitch McConnell
Minority Leader
United States Senate

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

We write in support of President Biden's call for robust funding to modernize and secure federal information technology (IT) and networks in the proposed "American Rescue Plan." The COVID-19 pandemic has greatly accelerated the need for the Federal Government to modernize its aging IT infrastructure. We urge Congress to provide the $9 billion for the Technology Modernization Fund (TMF) that the President has called for in any emergency supplemental legislation. We further recommend that a substantial portion of the total amount provided be exempt from the TMF's usual reimbursement requirements to accelerate urgent IT upgrades.

Since the beginning of the pandemic, Americans, particularly the most vulnerable populations, have been unable to access most government services in person. Yet federal agencies still rely on many outdated and legacy IT systems and paper-based processes that have hampered the effectiveness of government operations and mission delivery. Updating these systems is not only critical to improving access to services but also to ensuring those who are most in need of government assistance receive the emergency funding Congress has appropriated.

Aging IT at the Federal and state levels has hindered the ability of governments to quickly and efficiently get dollars, programs, and services to Americans in need. While commercial best practices are being used in the private sector to enable vaccine distribution, the Internal Revenue Service, Small Business Administration, and multiple state and local employment insurance programs have faced a number of high-profile challenges with tracking vaccines and distributing aid. The new normal, where remote work, social distancing, and virtual interaction are necessary for agencies to safely meet their missions and serve the American public, has exponentially increased the public cost of disruptions. Without the ability to provide in-person services, a cyber attack now could prevent an agency from providing services altogether. Moreover, aging IT applications and infrastructure increase the likelihood of such a disruption. Legacy IT can be difficult to maintain, supported by only a few remaining vendors at great expense, more exposed to cybersecurity risks and single points of failure, less

resilient to critical events, and far less effective than modern commercial capabilities. Additionally, the cumbersome nature of those systems limits oversight and transparency into the aid being provided.

At the same time, the sudden shift to telework for the vast majority of over two million federal employees has created innumerable new vulnerabilities. The recent SolarWinds compromise further highlights the importance of federal investments to counter persistent and growing cyber threats to federal IT in an atmosphere of increased vulnerability. Federal technology lags well behind commercial state-of-the-art technologies embraced throughout the private sector, remains vulnerable, and continues to present significant risk to future breaches. Providing substantial non-reimbursable TMF support is necessary to enabling agencies to transform the way they use technology, more securely meet their missions, and deliver enhanced digital services to the American public.

The cyber remediation activities that will be necessary following recent compromises also create unavoidable and considerable unanticipated costs. 'No-year' TMF dollars can provide the flexibility and resources needed to quickly address exigent issues as they are identified over the coming weeks and months. TMF dollars can be used to meet mission critical needs that have arisen during the pandemic and remain flexible enough to address the backlog of previously-identified critical IT projects to enhance security and service delivery while saving taxpayer dollars. Excusing repayment requirements can also help with federal recovery and ensure that security and resiliency against future critical events of all sorts are incorporated up-front in the technology transformation that will be enabled by these funds.

We continue to support retaining reimbursement requirements for a smaller portion of the additional TMF funding provided as part of this legislation to help maintain a more robust and continuous funding pool for ongoing federal IT modernization. Additionally, to ensure the funds provided are directed to and used optimally for the government's highest priority IT projects, we strongly recommend that Congress ensure that the TMF board is supported by professionals with the appropriate technical, financial, management, cyber, and acquisition expertise.

Finally, it is crucial that additional support for federal IT be accompanied by similarly robust and unencumbered federal financial resources to modernize and harden the systems of state, local, tribal, and territorial governments. Non-federal governments throughout the United States are key to the administration of federal programs and funding, and they face equal if not greater needs for investment in information technology with fewer resources with which to do so.

Thank you for your consideration and for your work on this important priority.

Sincerely,

Alliance for Digital Innovation (ADI)	**Intelligence & National Security Alliance**
BSA I The Software Alliance	**Internet Association**
Center for Procurement Advocacy (CPA)	**National Defense Industrial Association (NDIA)**
U.S. Chamber of Commerce	**Professional Services Council**
Computing Technology Industry Association (CompTIA)	**Security Industry Association (SIA)**
Information Technology Industry Council (ITI)	**Software & Information Industry Association**