ALLIANCE FOR DIGITAL INNOVATION Cybersecurity Coalition CompTIA ITI

October 28, 2021

The Honorable Gary Peters
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Peters, and Ranking Member Portman:

We, the undersigned organizations, write to emphasize the importance of cloud computing and its adoption throughout the federal government. Cloud computing is showing considerable potential to help agencies rapidly modernize their information technology (IT) while eliminating the costs to taxpayers associated with building and maintaining those IT products. Because of this technology's rapid and continuous evolution, it is important to foster a dynamic ecosystem that empowers agencies to adopt of cloud products while retaining flexibility to adopt the next generation of technologies.

GSA's Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standardized federal approach to security assessments and monitoring for cloud service providers (CSPs), embracing a "certify once, leverage many times" approach. The program has attracted much attention in the wake of Executive Order 14028 on Improving the Nation's Cybersecurity, which assigns FedRAMP a consultative role in the development of cloud security guidance. However, FedRAMP has faced implementation difficulties since its inception.

As cloud platforms continue to expand, the program's certification capacity has struggled to keep up with demand. CSPs have noted that the process to gain and maintain FedRAMP certification is costly and time consuming; despite recent efforts to expedite the process, it can take years and cost companies millions of dollars to become certified. Moreover, there has been a concerning lack of reciprocity across agencies that undercuts the program's original goal. A large number of agency-specific processes have made it difficult to issue authorizations to operate (ATOs) cloud services even when other agencies are using the same products, causing duplication of efforts and delays in achieving mission objectives. To-date, the FedRAMP Project Management Office (PMO) and its agency partners have authorized 239 cloud products for use in the federal government, with another 96 in the queue. This does not reflect the vast landscape of cloud service offerings that the commercial world enjoys.

The FedRAMP Authorization Act of 2021 was considered by the U.S. House of Representatives earlier this year as standalone legislation (H.R. 21 in the 117th Congress) and, more recently, was adopted by that chamber as an amendment to the Fiscal Year (FY) 2022 National Defense Authorization Act (NDAA). Some of the actions contained in this legislation have the potential to help address several implementation difficulties presently facing FedRAMP. To be effective, the FedRAMP PMO must be resourced adequately to expedite the certification process for commercially available cloud service offerings. Moreover, automating FedRAMP processes beyond recent developments, like the release of OSCAL, will reduce the time lag between the commercial delivery of services and their introduction into government-authorized cloud regions. The process can be further expedited by waiving the sponsorship requirement to allow any applicant to go through the certification process. Striking the agency sponsorship requirement will remove barriers to entry for new companies and products. The Federal Information Processing Standard (FIPS) already uses a similar approach. The FedRAMP PMO should also engage industry as an equal partner and collaborate with agencies to facilitate the speedy adoption of P-ATOs. Finally, FedRAMP should be aligned with other federal security requirements to ensure a coherent approach to risk management.

It is important that cloud security continue to be promoted and the federal government's overall cybersecurity posture enhanced—all while ensuring that the opportunity to contract with the government and attain the certifications necessary to do so is equitable, and that competition between providers remains robust. We believe FedRAMP can drive agencies' migration to cloud services if these foundational conditions are met and respectfully request your committee's support for improving the IT security assessment and monitoring process.

Thank you for your consideration our views on these important matters and for your ongoing work to promote technology advancement and security in the federal IT enterprise.

Sincerely,

Alliance for Digital Innovation (ADI)

Computing Technology Industry Association (CompTIA)

Cybersecurity Coalition

Information Technology Industry Council (ITI)