Internet Association

September 20, 2017

To: American Technology Council

Re: Request for Comment on the Federal Report to the President on Federal IT Modernization prepared by the American Technology Council.

Internet Association (IA) represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including cloud innovation. Our companies are global leaders in the drive to develop lower cost, more secure, and resilient cloud services to customers including public sector customer.

Internet Association welcomes the opportunity to provide comments to the Federal Report to the President on Federal IT Modernization prepared by the American Technology Council (ATC) and signatory agencies.

IA shares the vision set out in the report and strongly endorses the proposed implementation plan. Modernizing Federal information IT systems will allow agencies to better leverage American innovations developed by our member companies that can provide better service for the public in a more cost-effective and secure manner. As the private sector across all industries adopts commercial cloud services to modernize their IT infrastructure, the Administration should look for opportunities on how to best leverage these same modern computing technologies to benefit the public.

The report's emphasis on opportunities to leverage commercial cloud services is the right approach. Commercial cloud services can be leveraged to improve the federal government's IT posture and the report captures important issues that will facilitate the federal government's use of commercial cloud services including:

- updating relevant network security policies to meet modern computing standards;
- modernizing contracting vehicles and procurement policies to enable agency adoption of commercial cloud services; and
- an implementation plan that makes the proposed modernization strategy actionable.

The following is a set of specific recommendations from IA member companies to support the federal government's momentum toward commercial cloud services:

1) IA members strongly support the acquisition pilot (Appendix D). It is a crucial first step to ensure that the modernization plan can effectively be implemented across the government by reducing uncertainties through the lessons learned in the pilot.

    - Such pilot programs can be an effective mechanism for accelerating the adoption of commercial cloud services that have been proven to improve security, productivity, and innovation in the broader enterprise and consumer sectors.

2) Industry has experience and expertise in designing and adopting enterprise wide cloud services. The private sector should work in partnership with agencies and be an integral part of the discussion to support the implementation plan. (Appendix F)

- This is particularly important in updating security requirements that were designed for the on-premise, perimeter security model. Such standards do not translate well to the cloud-based, defense-in-depth environment, and government should work closely with leaders in cloud security innovation to create future-proof standards.

- Different initiatives should be considered to foster regular dialogue between cloud service providers, private sector commercial cloud users and agency IT decision makers to share best practices and information about leading trends commercial cloud security and adoption.

3) Commercial cloud services provide a modern and future-proof approach to security compliance. The federal government could improve its security posture by leveraging these state of the art services that, among other things, can rapidly push security updates across the entire infrastructure quickly and seamlessly. For the modernization plan to be successful it must establish a modern security compliance regime that can leverage the unique security advantages of cloud computing services.

    - The current approach to continuous monitoring merits review. Continuous monitoring and vulnerability scanning requirements come from an antiquated security design approach and are not adapted to leading cloud based defense in depth security architectures.

    - The ATC should propose a plan to support the PMO's efforts to work with JAB agencies to evolve policies and processes for continuous monitoring. The plan should focus on being responsive to agency security visibility needs and outcomes-focused approaches that allow cloud service providers to have flexibility in implementation of requirements.

4) Federal IT requirements and certifications should reference leading global industry data security standards developed through the international standards process. US Specific standards limit the government's option for new leading-edge cloud based services and a competitive vendor environment because tools developed by smaller vendors will comply with international industry standards but it is often cost prohibitive for smaller vendors to comply with a completely different set of federal requirements.

    - US-specific standards have global implications and have the effect of encouraging more countries to pursue their own unique sets of standards, creating distinct sets of regulatory and compliance requirements that add complexity and cost without necessarily enhancing security outcomes. US-specific standards also prevent innovative providers without large compliance teams from accessing the government market.

    - Security should be assessed through a risk- and outcomes-based lens, not a prescriptive, compliance for compliance sake exercise.

5) We also urge the administration to ensure consistency of security and compliance requirements across all agencies, including the Defense Department for all unclassified data applications.

Leveraging the innovation, security, flexibility and competitive costs of commercial cloud services can be most easily achieved when requirements are consistent across the government.

- Specifically, we recommend convening cross-agency workshops to ensure consistent understanding of all existing cloud policy requirements for cloud services.

- While the FedRAMP Program Management Office (PMO) has improved the process of achieving an authority to operate (ATO) through FedRAMP Accelerated, there is potential for greater efficiencies in initial authorization, both through automation and reciprocity. To enable reciprocity, or agency re-use of a Joint Authorization Board (JAB) Provisional ATO, the ATC could promote updates to to FISMA, which currently requires each agency to accept the risk of any application/platform, resulting in duplicative review processes at the core cloud platform layer. Updating FISMA could permit agencies to accept through reciprocity a JAB P-ATO and then only conduct a complementary agency-specific review, saving Federal resources. Likewise, improvements to the process of maintaining an ATO (i.e., continuous monitoring) could save additional Federal resources.

We look forward to working with you to support the administration's efforts to modernize federal IT systems in order to make it more secure and resilient.

The Internet Association thanks the ATC and signatory agencies for the opportunity to submit comments on this report. We look forward to working with you to support the administration's efforts to modernize federal IT systems to continue to improve services to citizens in a cost effective and secure manner.

Respectfully submitted,

____

Michael Beckerman
President & CEO
The Internet Association