January 18, 2019

To: Ms. Suzette Kent
The Office of the Federal Chief Information Officer
Office of Management and Budget
Executive Office of the President

Internet Association Comments on the Draft Update to the Trusted Internet Connections (TIC) Initiative

Internet Association (IA) represents over 45 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our companies are global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. IA welcomes the opportunity to provide input to the federal government's draft Update to the TIC Initiative.

IA appreciates the Federal Chief Information Officer's continued commitment to improving the TIC Initiative and removing barriers to cloud adoption and implementation of modern technology. We applaud the rescission of the four prior memos referenced in the policy, and recognize the cloud-forward direction this move signals to agencies as they continue to plan for and procure commercial cloud solutions.

We commend the risk-based approach to TIC modernization, as outlined in the Use Case approach methodology, for long-term technical flexibility. To ensure its effectiveness, we recommend that the new TIC policy outline deliverables and time-tables for acceptance and documentation of TIC Use Cases. Without deadlines for DHS or OMB, agencies planning for upcoming IT modernization projects will not know when to expect new guidance or updates on lessons learned. Additionally, the agencies should notify the public of ways to submit use cases for consideration. Enhanced clarity and transparency will aid both government and industry in planning for and delivering commercial cloud solutions in accordance with the IT Modernization Report and President's Management Agenda.

The draft policy recognizes that it is critical for agencies to have "increased flexibility to use modern security capabilities."[1] To that end, we support leveraging the intelligence and core capabilities of commercial cloud providers themselves to augment the security posture of the cloud connected endpoints. Cloud providers are spending billions to protect themselves and their customers from cyber attacks and malware globally, and customers can benefit from cloud-based intelligence and automated protections as a first line of defense that can vastly improve visibility and situational

[1] Office of the Federal Chief Information Officer. (2019). *Update to the Trusted Internet Connection (TIC) Initiative.* Retrieved from https://policy.cio.gov/tic-draft/

awareness. Government/Agencies should incorporate into their proposed use cases the cloud-based intelligence and automation already available.

IA offers the following recommendations to the draft and is happy to assist or clarify so that they may be included in the final policy.

Inclusion of PaaS
We recommend Section 1 inside Appendix A be made inclusive of all prevalent cloud models, including Platform as a Service (PaaS), to better align to the NIST Special Publication 800-145, or any updates made thereafter. We further recommend incorporating by reference the NIST standard definitions for cloud services.

Clarify Which Entity Authorizes Pilots
Section C outlines specific actions for agencies, OMB, DHS, and GSA, but it does not clarify which entity will authorize pilot projects. We recommend that the policy outline a clear approval chain for pilot projects so that both government and industry are aware of key decision makers for projects.

Establish Transparent Process for Iteration, Approvals, and Feedback
We strongly support the idea that both Use Case and reference documentation should be reviewed and updated on a continuous basis. However, the current draft does not specify how these would be revised. We recommend the policy outline and adopt a transparent and continuous process for review and iteration of Use Cases and, where applicable, relevant architecture documents that aligns to the pace of innovation. This will result in greater predictability and transparency for both government and industry as more commercial cloud solutions are deployed across government.

Reflect Existing Accreditation and Security Controls Processes
As the government looks to implement updates to the TIC policy, we recommend that it ensure that the requirements of other accreditation services, such as Federal Risk and Authorization Management Program (FedRAMP) or Continuous Diagnostics and Mitigation (CDM), be taken into account and make efforts to avoid duplication.

Deadlines for Publication of Use Cases, Documentation, and Examples
Agencies are required to make updates to their own networks within a year of the release of this memorandum, but the draft is silent on when they can expect more information regarding use cases and reference documents. Furthermore, we recommend the draft include clear processes set out for how to submit use cases or leverage existing pilots. This policy should contain clear onboarding or submission procedures for use cases as well as deadlines for when these should be approved. Furthermore, the use cases should be publicly posted on a timely basis for other agencies to leverage and for industry to support. Increased transparency into this process will be useful for both agency staff and industry, as commercial cloud providers stand ready to partner with government on modernization.

Create Industry Advisory Board as Stated in the Federal Cloud Computing Strategy
Internet companies are on the front lines of government IT modernization. Accordingly, IA

recommends that the draft TIC policy include the opportunity for internet companies to provide the administration feedback on TIC pilots and use cases as technology evolves. IA asks for the creation of an Industry Advisory Board (IAB), convened by OMB, to provide timely and regular feedback to OMB, DHS, GSA, and the CISO Council as they implement and iterate on TIC guidance and to show how agencies could optimize the security posture of the cloud connection points via unified security management capabilities that are inherent to the platforms. We note that such a body was specifically contemplated in the draft Federal Cloud Computing Strategy.[2] Specifically, Action 4 in the draft Strategy states the following, to be done within six months of the issuance of the final Federal Cloud Computing Strategy:

> The Office of Management and Budget will work with the General Services Administration, the Chief Information Officers Council, and the Department of Homeland Security to update the Trusted Internet Connection (TIC) Policy to ensure program objectives can be achieved. Policy goals will be updated using security architectures that are scalable and allow for the efficient use of cloud. ***This includes creating a public-private forum for working with industry to collect their input.*** (emphasis added)

Internet Association appreciates the opportunity to provide feedback to the federal government's draft Update to TIC. We look forward to continuing to work with OMB as the draft is finalized and implemented.

Sincerely,
Alla Seiffert
Internet Association

[2] Office of the Federal Chief Information Officer. *Federal Cloud Computing Strategy.* Retrieved from https://cloud.cio.gov/strategy/