February 7, 2020

To: Mr. Bryan Ware
Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
4100 Wilson Blvd
Arlington, VA 22203

Internet Association Comments On The Draft Trusted Internet Connections (TIC) 3.0 And National Cybersecurity Protection System (NCPS) Architecture Documents

Dear Mr. Ware:

Internet Association (IA) represents over 40 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 Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) public comment process for both Trusted Internet Connections (TIC) 3.0 and National Cybersecurity Protection System (NCPS) cloud architecture documents.

We appreciate CISA's posture in adapting the TIC program for use with cloud services, and recommend that the Agency continue to move away from the boundary-focused approach to further comply with the cloud-forward goals M-19-26[1]. IA offers the following feedback on the current set of reference documents:

Elaborate On DHS' Goals For Federal Network Defense And Clarify The Role of TIC In The Cloud

Industry appreciates the Agency's role as an integral piece of the federal government's cybersecurity puzzle. However, we ask CISA to provide more information on the government's goals for successful implementation of TIC in the cloud, and allow industry to propose examples of the ways in which our tools would help effectuate those goals. The current set of guidance documents do not clarify how the deployment of cloud security resources would support NCPS goals in a software-defined networking paradigm. For example, the boundary-focused approach outlined in the draft materials contradicts the goal of broad-based

[1] United States Office of Management and Budget. *Update to the Trusted Internet Connections (TIC) Initiative.* Washington, DC: Deputy Director for Management, Margaret Weichert: 2019. https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

cloud adoption. Further, we would appreciate clarity on the intersection of Policy Enforcement Point (PEP) Capabilities and cloud services within the realm of TIC and NCPS.

Specify Differing Reporting Requirements For Various Levels Of Cloud Services
The current NCPS Cloud Reference Architecture Volume 1 is vague with regard to the transaction records and event security logs required by each type of cloud service. We appreciate the acknowledgement that SaaS, PaaS, and IaaS are not the same, but there is little clarity about what telemetry data must be sent by the Cloud Service Providers (CSPs) to CISA and how that data differs based on the cloud service itself.

Provide More Clarity On High Trust In The Cloud
The current drafts of CISA Trust Criteria correlate levels of control with trustworthiness. The TIC documentation incorrectly implies that private data centers provide better security than mature cloud hosting options and thus should be the only option for High Trust situations. We believe that an agency's ownership of a data center does not always result in increased security, and hyperscale cloud service providers are often able to provide more secure solutions for their customers. We ask CISA to define its criteria for a cloud-based High Trust environment.

Tailor Telemetry Data That Lives In The Cloud Log Aggregation Warehouse (CLAW)
With the understanding that PaaS and SaaS NCPS architectures are not yet operational, we recommend that CISA tailor the specific telemetry data asks from those data feeds to be proportional with the risk exposure of each tool. For example, a SaaS collaboration tool creates different logging data than an IaaS capability, and CLAW should ingest only that data which is operationally significant. Further, we encourage CISA to consider security best practices, such as zero-trust architectures, when piloting potential PaaS and SaaS CLAW implementations.

Clarify Timeline To Implementation
In the proposed process handbook, CISA charts a 6 month timeline for a project, and it would be helpful to understand whether the Agency will offer a "fast-track" process for certain approved configurations. Further, IA would like to understand whether CISA intends to allow cloud tools with existing Authorities to Operate(ATO) to run for a period of time prior to re-evaluation within the CLAW guidelines.

Define A Formal ID Format For NCPS In The Cloud
The traditional TIC ID format (e.g. "PEP.01") does not appear in any of the TIC 3.0 public documents. IA would like to know more about CISA's thinking on the numbering format: are the formal numbers being removed, and if so, are documents alone the living resource? For example PEP.02 has no direct mapping, and now seems as though it correlates to "Manage traffic." The significance of this is that without a NIST-like control set, it will be challenging for customers to understand how to implement TIC 3.0 and remain compliant with the letter of the policy.

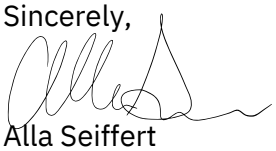
Consider Procurement And Contracting Barriers To Adoption
The NCPS Cloud Reference Architecture documentation places net-new burdens of compliance and reporting on all civilian agencies leveraging cloud solutions. These requirements may not currently fit within the scope of existing contracts that agencies hold with CSPs. Consequently, CISA should consider partnering with the DHS Procurement Innovation Lab (PIL) to create a playbook for TIC implementation. This document should contain sample language for new contracts as well as for issuing contract modifications.

Commit To Ongoing TIC And NCPS Iteration
We applaud the work that CISA has invested in the NCPS documentation thus far, and want to ensure the team maintains its agile posture going forward. As we await the publication of Volume 2 of the NCPS Cloud Reference Architecture, IA would like to encourage the Agency to revisit and update documentation as technology evolves and new security paradigms are adopted throughout the public sector.

Create An Industry Advisory Board
Internet companies are on the front lines of government IT modernization. Accordingly, IA recommends that CISA 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 DHS, to provide timely and regular feedback to DHS, General Services Administration, 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.

Internet Association and our members appreciate the opportunity to provide feedback to CISA's federal network defense mission via the implementation of TIC 3.0 and NCPS in the cloud. We look forward to continuing to work with your team and the rest of the Agency as the draft is finalized and implemented.

Sincerely,



Alla Seiffert
Director of Cloud Policy and Counsel
Internet Association