EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 12, 2019

DEPUTY DIRECTOR
FOR MANAGEMENT

M-19-26

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret Weichert
Deputy Director for Management

SUBJECT: Update to the Trusted Internet Connections (TIC) Initiative

A. Purpose of the TIC Initiative

The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modern architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

B. Rescissions

In accordance with Office of Management and Budget (OMB) Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, OMB is rescinding the following memoranda:

1. M-08-05, Implementation of Trusted Internet Connections (TIC) (November 20, 2007)
2. M-08-16, Guidance for TIC Statement of Capability Form (SOC) (April 4, 2008)
3. M-08-27, Guidance for TIC Compliance (September 30, 2008)
4. M-09-32, Update on the TIC Initiative (September 17, 2009)

These previous OMB memoranda required agency traffic to flow through a physical TIC access point, which has proven to be an obstacle to the adoption of cloud-based infrastructure.

C. Removing Barriers to Cloud and Modern Technology Adoption

One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect networks from malicious actors. To continue to promote a consistent baseline of security capabilities, the Department of Homeland Security (DHS) will define TIC

initiative requirements in documentation called TIC Use Cases (refer to Appendix A). TIC Use Case documentation will outline which alternative security controls, such as endpoint and user-based protections, must be in place for specific scenarios in which traffic may not be required to flow through a physical TIC access point. To promote flexibility while maintaining a focus on security outcomes, the capabilities used to meet TIC Use Case requirements may be separate from an agency's existing network boundary solutions provided by a Trusted Internet Connection Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS). Given the diversity of platforms and implementations across the Federal Government, TIC Use Cases will highlight proven, secure scenarios, where agencies have met requirements for government-wide intrusion detection and prevention efforts, such as the National Cybersecurity Protection System (including the EINSTEIN suite), without being required to route traffic through a TICAP/MTIPS solution.

D. Collaborative and Iterative Processes to Pilot, Update, and Verify TIC Use Cases

Due to the rapid pace of technology and threat evolution, it is critical that agencies develop pilots to meet their technology needs while promoting appropriate security controls. Further, to ensure they remain relevant, TIC Use Cases, as well as other TIC reference architecture documentation, must be reviewed and updated on a continuous basis. It is also important to migrate from onerous and burdensome "point-in-time" spot checks towards scalable, comprehensive, and continuous validation processes. This memorandum establishes a collaborative and iterative process, incorporating inputs from both industry and Federal agencies.

1. ***Within 60 days of the release of this memorandum, DHS, in coordination with OMB and the Federal Chief Information Security Officer (CISO) Council shall*** *establish and publicly release a detailed process document that incorporates the following elements*:

    a) ***Initiate Pilots: The Federal CISO Council shall*** *solicit and review agency and industry TIC pilot proposals on an ongoing basis, participate in the approval process for updates to TIC Use Cases and other TIC reference architecture documentation, and establish the timeline for DHS to review pilot results and approve updates to TIC Use Cases and other TIC documentation;*
    b) ***Manage Pilots: DHS, in coordination with OMB, the General Services Administration (GSA), and the CISO Council shall*** *oversee and support agency TIC pilots, as appropriate;*
    c) ***Approve Use Cases: DHS, in coordination with OMB, GSA, and the CISO Council, shall*** *review pilot results and approve updates to TIC Use Cases and other TIC reference architecture documentation;*
    d) ***Acquisitions: GSA shall*** *update government-wide procurement vehicles, as appropriate, within 6 months of the approval of new TIC Use Case requirements and other TIC reference architecture documentation; and*
    e) ***Collect Feedback: DHS, in coordination with GSA, shall*** *establish a coordinated process for soliciting agency and industry input on approved TIC Use Cases and other TIC reference architecture documentation. DHS will ensure TIC Use Cases and other TIC reference architecture documentation are kept up to date as changes are approved.*

2. ***Within 90 days of the release of each TIC Use Case, DHS, in coordination with GSA and NIST, shall*** *develop a compliance verification process to validate that agencies are implementing the security controls required by TIC Use Cases. DHS will update this verification process as necessary to promote continuous improvement.*

E. Agency Implementation

In order for TIC program updates to achieve the goal of diversifying technology options for agencies while retaining strong protections for Federal systems and information, OMB, DHS, and the agencies themselves, need to have details of the technologies and defenses deployed across Federal networks. As such, agency Chief Information Officers shall maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection in the event OMB, DHS, or others request this information to assist with government-wide cybersecurity incident response or other cybersecurity matters.

1. ***Within one year of the release of this memorandum, agencies shall*** *complete updates to their own network and system boundary policies to reflect this memorandum, including guidance regarding potential pilots. Agencies will identify which TIC Use Case will be allowed for the agency. OMB and DHS will track agency implementation through Federal Information Security Modernization Act of 2014 (FISMA) reporting.*

Appendix A - Initial Common Trusted Internet Connections (TIC) Use Cases

The list below highlights an initial set TIC Use Cases for agencies. The collaborative and iterative process described in this memorandum should result in the continuous improvement and development of additional TIC Use Cases that account for emerging technologies and evolving cyber threats.

1. **Traditional TIC (Default Use Case)**: For instances not covered in other DHS TIC Use Cases, agencies are required to continue following the Traditional TIC use case. This default use case leverages agency TICAP and MTIPS providers.

2. **Cloud**: These sets of TIC Use Cases cover some of the most prevalent cloud models used by agencies today.
    a. Infrastructure as a Service (IaaS)
    b. Software as a Service (SaaS)
    c. Email as a Service (EaaS)
    d. Platform as a Service (PasS)

3. **Agency Branch Office**: This use case assumes that there is a branch office of an agency, separate from the agency headquarters (HQ), which utilizes HQ for the majority of their services (including generic web traffic). This use case supports agencies that want to enable Software-Defined Wide Area Network (SD-WAN) technologies.

4. **Remote Users**: This use case is an evolution of the original FedRAMP TIC Overlay (FTO) activities. This use case demonstrates how a remote user connects to the agency's traditional network, cloud, and the Internet using government furnished equipment (GFE).