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

September 17, 2009

M-09-32

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

From: Vivek Kundra
Federal Chief Information Officer

Subject: Update on the Trusted Internet Connections Initiative

The purpose of this memorandum is to provide an overview of the Trusted Internet Connection (TIC) initiative and to request updates to agencies' Plans of Action and Milestones (POA&Ms) for meeting TIC requirements.

BACKGROUND

In November 2007, OMB announced the Trusted Internet Connections (TIC) Initiative to optimize individual agency network services into a common solution for the Federal government. Agencies were required to develop and submit comprehensive Plans of Action and Milestones (POA&Ms) to reduce and consolidate the number of external access points, including Internet connections; and ensure that all external connections are routed through an OMB-approved TIC.

Based on solicited agency Statements of Capability, OMB also designated twenty agencies as TIC Access Providers (TICAPS). Each TICAP agency was authorized two locations where they must reduce and consolidate all external connections. Agencies must present an evidence-based rationale for acquisition of more than two locations. Please send an email to tic@dhs.gov for the template and instructions.

SPECIFIC ACTIONS REQUESTED

Agencies shall update and report formal Plans of Action and Milestones (POA&Ms) to the Department of Homeland Security by September 25, 2009, and provide updated status to DHS every six months thereafter, until completed.

All agencies seeking Trusted Internet Connection Access Provider (TICAP) services shall utilize the template in enclosure (1) and submit it to tic@dhs.gov. For reference by TICAP agencies only, a blank TICAP agency POA&M is provided in enclosure (2). DHS has separately contacted the 20 TICAP agencies with instructions on how to update their POA&Ms.

In addition to the POA&M, TICAP agencies must schedule by September 25, 2009 their initial TIC compliance on-site assessments with DHS. All other agencies must also collaborate with DHS to complete their initial TIC compliance self-assessments by December 31, 2009.

Federal policy requires all agencies to undertake immediate responsibility for executing essential agreements and updating POA&Ms to facilitate not only TIC preparations, but also due diligence for integrating the National Cyber Protection System (NCPS, operationally referred to as Einstein) deployments and synchronizing with US-CERT.

Agencies will work with DHS on studies of Federal network infrastructure, and report data from the agency's inventory of network connections to DHS as requested. Each agency is responsible for maintaining a current inventory of its network connections, including details on the service provider, cost, capacity and traffic volume for each connection.

Agencies that are seeking service through the Networx contract vehicle will work with the General Services Administration (GSA) to estimate costs of adopting the MTIPS option by September 30, 2009. Please contact GSA at (866) 472-0274.

Questions or concerns should be addressed to:

- DHS TIC Program Management Office: Sean Donelan, (703) 235-5122, tic@dhs.gov
- DHS TIC Compliance Validation Program Management Office: Don Benack, (703) 235-5037, fns.compliance@dhs.gov
- GSA Networx: Frank Tiller, (703) 306-6872, frank.tiller@gsa.gov or Karl Krumbholz, (703) 306-6079, karl.krumbholz@gsa.gov
- National Cyber Security Protection System (Einstein Deployment Team): Joshua Paquette, (703) 235-5189, einstein-info@us-cert.gov

Related TIC policy memoranda are listed below:

(a) OMB M-08-05, Implementation of Trusted Internet Connections
(b) OMB M-08-16, Guidance for Trusted Internet Connection Statement of Capability Form
(c) OMB M-08-26, Transition from FTS 2001 to Networx
(d) OMB M-08-27, Guidance for Trusted Internet Connection Compliance
(e) NSPD-54/HSPD-23, Comprehensive National Cyber Security Initiative

Enclosures: (1) POA&M Template for Agencies Seeking TICAP services
(2) POA&M Template for TICAP Agencies

TRUSTED INTERNET CONNECTIONS INITIATIVE
MAJOR MILESTONES

1) Inventory agency's external connections. In accordance with M-08-05, "Implementation of Trusted Internet Connections," all agencies should have identified external connections. Appendix A of the TIC Reference Architecture, available on the OMB MAX Portal Trusted Internet Connections page, clarifies the definition of external connection. This information was used to establish the starting baseline for the Initiative and should have been completed.

2) Determine agency's capability to meet TIC critical technical capabilities. In accordance with M-08-16, "Guidance for Trusted Internet Connection Statement of Capability Form," TICAP agency CIOs should have determined the gap between their agencies' current capabilities and the 51 capabilities identified in the Statement of Capability (SOC) Document. Appendix B of the TIC Reference Architecture lists and clarifies the 51 critical technical capabilities. This information was used to select designated TICAP agencies and should have been completed.

3) Develop a plan to reduce and consolidate agency's external connections through approved access points, and implement critical TIC capabilities. References (a), (b), and (d) tasked Agency CIOs with developing a comprehensive Plan of Action and Milestones (POA&M). Agencies will update and report POA&Ms to DHS by September 25, 2009, and provide an updated status to DHS every six months until completed. Please note that TICAP agencies should utilize a different POA&M reporting template than the agencies that are seeking TICAP service – refer to enclosure (2).

4) Acquire telecommunications connectivity through the Networx Contract. M-08-26, "Transition from FTS 2001 to Networx," states that all agencies should utilize the Networx Contract to acquire telecommunications connectivity.[1] Agencies are encouraged to purchase the Managed Trusted Internet Protocol Services (MTIPS) CLIN through the Networx Contract. TICAP agencies are also encouraged to purchase the MTIPS CLIN, but may also utilize Networx services to customize their security capabilities.

5) Implement the plan to reduce and consolidate agency's external connections through approved access points. All Agency CIOs will need to sign a Banner Memorandum of Agreement (MOA) and execute a Service Level Agreement (SLA) with DHS. TICAP Agency CIOs will also need to sign an Interconnection Security Agreement, sign a Memorandum of Agreement (ISA/MOA), and collaborate with DHS to stand up their TICAP locations.

.

[1] Agencies seeking to contract services from sources other than Networx must perform a cost-benefit analysis in accordance with M-08-26, "Transition from FTS 2001 to Networx," and receive approval from appropriate agency acquisition officials and their CIO.

6) Collaborate with DHS to measure and validate agency compliance with the TIC Initiative. The Comprehensive National Cyber Security Initiative (NSPD-54/HSPD-23) directs DHS, in partnership with OMB, to validate agency compliance with the TIC initiative. DHS will also assess the capabilities of the Networx TICAPs prior to the service being available. All 20 TICAP agencies must schedule with DHS the on-site portion of their initial TIC compliance validation assessments by September 25, 2009. All other agencies must submit a completed TIC Compliance Validation Self Assessment form to DHS by December 31, 2009, in order to complete initial TIC compliance validation self-assessments.