Audit of the Trusted Internet Connections Initiative at NARA

OIG Audit Report No. 11-17

September 30, 2011

Table of Contents

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of the Trusted Internet Connections (TIC) Initiative at NARA. In 2007, the Office of Management and Budget (OMB) announced the TIC initiative to optimize individual network services into a common solution for the Federal government. This initiative aimed to reduce external connections and improve the Federal government's incident response capability. The purpose of this audit was to assess NARA's efforts to meet this initiative and determine whether NARA had adequately prepared and planned to meet the goals of the TIC initiative.

Our review found NARA had not adequately planned and prepared to meet the goals of OMB's TIC initiative. More than three years after OMB's announcement of this initiative, NARA had not fully completed actions to comply with requirements set by OMB, the U.S. General Services Administration (GSA), and the Department of Homeland Security (DHS). For example, a comprehensive Plan of Action and Milestones (POA&M) had not been developed to reduce and consolidate NARA's external connections and implement crucial TIC capabilities. Further, NARA had not developed contract requirements to determine the appropriate Contract Line Item Numbers (CLINs) needed to implement TIC services. Instead, the contractor providing those services was tasked with identifying the appropriate CLINs. Finally, a process had not been developed to monitor the contractor's performance of these services.

Despite reporting in 2008 that NARA was well into its migration to decrease from seven external connections to two TIC- approved connections, NARA had only eliminated one of their external connections by 2010 and had not yet eliminated the other four external connections to meet its goal. Further, as of May 2011, NARA had not fully implemented the two TIC-approved connections. Therefore, it appeared NARA had not managed this project as a priority and had not identified any constraints or technical gaps to prevent implementation of the TIC initiative. In addition, formal detailed planning documents were not prepared and executed to meet the goals of the initiative or address any constraints or technical gaps preventing implementation. While a lack of transition priority was evident across the Government, progress has recently been reported at NARA and other organizations.

As a result, NARA had not fully implemented TIC as required by OMB and missed out on potential benefits offered by reducing its external connections and utilizing TIC-approved connections. For example, other agencies have experienced benefits such as improved network security and management. By reducing the number of access points, an agency can improve its ability to monitor traffic and protect network attacks.

To meet the requirements of the TIC initiative, we made six recommendations. These recommendations will aid in implementing TIC at NARA and meeting OMB, GSA, and DHS requirements.

Background

In November 2007, the Office of Management and Budget (OMB) issued a memorandum announcing the Trusted Internet Connections (TIC) initiative. The goal of this initiative was to optimize individual network services into a common solution for the Federal government. To meet these goals, each agency was required to develop a comprehensive plan of action and milestones (POA&M) and devote employees to work on the development and implementation of TIC. Subsequent guidelines required agencies to inventory and document all their gateway connections; assess their architecture, policy, and implementation results; and define their target inventory and architecture. In this process, TIC compelled agencies to gain an in-depth understanding of the breadth of their total Internet presence.

Another goal of this initiative included enhancing the Federal government's incident response capabilities through reduction of external connections and called for agencies to consolidate their existing external Internet connections. This would allow agencies to optimize and standardize the security of their external network connections. Although the initiative was intended to secure Internet connections, other external connections to potentially unsecured systems were also required to be routed through an approved TIC access point, even if they did not pass through the Internet. Ultimately, the initiative will improve the Federal government's security posture and incident response capability through the reduction and consolidation of external connections, and provide enhanced monitoring and situational awareness of external network connections.

In 2009, this initiative was re-emphasized as part of the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI consisted of mutually reinforcing initiatives with goals designed to help secure the United States in cyberspace. The first initiative under the CNCI was to manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. According to the CNCI, this consolidation of the Federal Government's external access points would result in a common security solution. Again, this solution would facilitate the reduction of external access points, establishment of baseline security capabilities, and validation of agency adherence to those security capabilities. All federal agencies in the executive branch, except for the Department of Defense, were required to implement this initiative.

Agencies participated in the TIC initiative either as TIC Access Providers (TICAP) or by contracting with commercial Managed Trusted Internet Protocol Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle. As a TICAP, an agency is responsible for providing external connections through a centralized gateway to only internal customers or to their internal and other external customers. Given NARA's size, NARA's Office of Information Services (NH) officials chose not to become an Access Provider and decided to seek these services through GSA's NETWORX contract.

Objectives, Scope, Methodology

The purpose of this audit was to determine whether NARA had prepared to the meet the goals of the Trusted Internet Connections (TIC) initiative. Specifically, we sought to determine NARA's efforts to implement TIC; identify any constraints or gaps in implementation; and evaluate NARA's readiness for compliance.

To satisfy the audit objective, we reviewed various OMB memoranda[1] and guidance related to TIC and NETWORX contracts issued by OMB, the U.S. General Service Administration (GSA), and the Department of Homeland Security (DHS). We also reviewed NARA's internal guidance, including the NARA Enterprise Architecture Technical Infrastructure Design and Information Technology (IT) Infrastructure Segment Program Plan. During the audit, we met with personnel involved in the project, including the Project Manager and NARA's Chief Technology Officer (CTO) [2]. We reviewed NARA's plans for meeting the TIC initiative and asked about any constraints or gaps preventing implementation. We also reviewed Capital Planning and Investment Process (CPIC) planning and scheduling documents related to this project. Finally, we reviewed NARA's contract files for their contract with an approved NETWORX services provider.

Our audit work was performed at Archives II in College Park, MD between January 2010 and June 2011. Due to other auditing priorities, our work was placed on hold from March 2010 until November 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] OMB memoranda related to the TIC initiative include the following:

- OMB M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 20, 2007
- OMB M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, April 4, 2008
- OMB M-08-26, *Transition from FTS2001 to NETWORX*, August 28, 2008
- OMB M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, September 30, 2008
- OMB M-09-32, *Update on the Trusted Internet Connections Initiative*, September 17, 2009

[2] During the timeframe of this audit, NARA underwent a Transformation effort. Office names and symbols have subsequently changed to reflect the reorganization. However, the previous office names and systems are used in the body of this report to reflect the historical names of the offices involved throughout the TIC initiative.

Audit Results

1. NARA Had Not Fully Implemented TIC Initiative

At the time of our audit, NARA had not fully implemented and met the goals of OMB's TIC initiative. Specifically, NARA had not met their goal to consolidate their seven external connections to the target of two and had not completed the Managed Trusted Internet Protocol Services (MTIPS) implementation, as required by OMB. This was caused by NARA not adequately planning and prioritizing to meet these goals, identifying constraints or gaps in implementation, and developing plans to address any constraints in implementing the initiative. As a result, NARA missed out on the potential benefits of the initiative, such as improved network security and management.

The November 2007 OMB memorandum M-08-05 required agencies to reduce and consolidate the number of external access points, including Internet connections, and ensure all external connections were routed through an OMB-approved TIC. Further, in August 2008, OMB required agencies to acquire telecommunications connectivity through the GSA NETWORX contract. Agencies were encouraged to purchase MTIPS Contract Line Item Numbers (CLINs) through this GSA contract. MTIPS[3] enabled agencies to connect to the public Internet or other external connections in full compliance with the OMB TIC initiative.

Prior to the TIC initiative, NARA had seven external connections. In April 2008, NARA determined their target number of external connections was two and the original projected completion date to eliminate five external connections was September 2009. However, as of March 2011, only one of the external connections had been eliminated. Further, NARA was still in the process of implementing the MTIPS at their sites. As of February 2011, the targeted completion date for the migration to MTIPS was May 2011[4]. Thus, NARA had not yet consolidated their external connections to the target of two and none of the other connections went through a TIC-approved connection.

NARA had not met these goals because despite their deadline to eliminate five external connections by September 2009, NARA had not managed the project as a priority or identified any constraints or technical gaps to prevent implementation. In August 2009, NARA revised its goals to eliminate one external connection by September 30, 2010 and

[3] MTIPS is a fully managed solution comprised of public Internet connectivity, the TIC portal, the network infrastructure to transport Internet Protocol traffic between the agency's enterprise wide area network (WAN), and the TIC portal which included management of a premise-based firewall and a security operation center.

[4] This date was pushed back to June 2011. Starting June 15, 2011, NARA began replacing the current internet service with the OMB-mandated TIC services.

another by March 31, 2011. The deadlines to eliminate the remaining connections were listed as “to be determined”.

In our initial meeting in January 2010, we were informed that the necessary plans and OMB requested information had been prepared and submitted to OMB; however, these plans had not been executed. When asked why these plans had not been executed, the CTO stated that with the change of administration, they were unsure if this initiative would continue. However, the TIC initiative was re-emphasized as part of the Comprehensive National Cybersecurity Initiative (CNCI). Since work did not begin until November 2010, despite the original projected completion date of September 2009, it appeared that NARA had not managed this project as a priority.

Further, NARA had not identified any technical gaps or other restraints, such as limited funding, to meet these goals. In their original assessment in April 2008, NARA had not identified any gaps in their current agency-wide policy, governance, or enforcement mechanisms to prevent a successful implementation of TIC. Then again in October 2008, in their report to OMB, NARA stated that nothing prevented them from a successful implementation of TIC. Additionally, the fiscal year 2010 Exhibit 300[5] for NARA’s IT Infrastructure stated that NARA was well into its migration to reduce down to two TICs. In these planning and budget documents, no capability or funding limitations were identified as a factor preventing NARA from meeting the TIC goals. Yet, the initiative was delayed and it appeared that NARA had not actively pursued the goals of reducing their external connections. Without identifying constraints or technical gaps, plans could not be developed to address such constraints or gaps.

Subsequent to our fieldwork, we were provided with documentation showing the delay in Qwest’s obtaining their authorizations from GSA. Specifically, Qwest did not receive the certification and accreditation of their MTIPS Security Operations Center and MTIPS System until June and September 2010, respectively. Therefore, some of NARA’s delay in implementing the TIC was attributed to Qwest not obtaining their authority to operate until September 2010.

By not consolidating to the targeted network connections and implementing TIC, NARA could not capitalize on the potential benefits of the initiative. Reported benefits of the TIC initiative include improvements in network security and network management. By reducing the number of access points needing to be monitored, agencies can improve their network security. Consolidating connections and centralizing security monitoring make it easier to monitor traffic and protect networks from attacks. In addition, the consolidation of external connections can make an agency’s network perimeter more secure. Other agencies have reported that implementing TIC was beneficial because it forced them to gain a greater awareness of their overall network environment, potentially reducing the complexity of the network making it simpler to manage.

[5] Exhibit 300s are the reporting mechanisms used for the annual budget submission to OMB.

Recommendation 1

The Chief Information Officer should ensure the TIC initiative is completed in accordance with OMB, GSA, and DHS requirements. Any exceptions to these requirements should be documented and approved by the Chief Information Officer.

Management Response

Management comments were not received prior to issuance of the final report.

Recommendation 2

The Chief Information Officer should ensure that any limitations related to the TIC initiative are identified and tracked until implementation is complete.

Management Response

Management comments were not received prior to issuance of the final report.

2. NARA Had Not Sufficiently Prepared Planning Documents to Meet TIC Initiative

NARA had not adequately prepared and planned to meet the goals of the TIC initiative. OMB memoranda required agencies to develop a comprehensive plan of action and milestones (POA&M). NARA developed a POA&M to meet this requirement; however, the POA&M was incomplete and had not been reviewed or updated regularly. Further, additional planning documentation was not prepared as planned. As a result, NARA's implementation of TIC was delayed and implementation did not begin until November 2010, despite the original completion date of September 2009.

When the TIC initiative was first announced in 2007, OMB required each agency to develop a comprehensive plan of action and milestones (POA&M). Agencies were required to develop and submit comprehensive POA&Ms to reduce and consolidate their number of external access points, including Internet connections, and ensure that all external connections were routed through an OMB-approved TIC. Planning guidance issued by OMB stated that POA&Ms must show specific milestones and activities for each element of the "As Is" Inventory, showing its transition from the current to the "To Be" target, as well as material underlying dependencies. In September 2009, OMB provided an update to the TIC Initiative and required all agencies to update and report their formal POA&M by September 25, 2009. Further, agencies were required to submit a POA&M to DHS by September 25, 2009 and provide updated status to DHS every 6 months thereafter, until complete.

We found that NARA had not adequately prepared and planned to meet the goals of the TIC initiative. Specifically, NARA developed a POA&M to submit to OMB; however, the POA&M was incomplete and had not been reviewed or updated regularly. For example, in their August 2009 POA&M, NARA had not identified completion dates to reduce their connections to the target of two. Instead, deadlines were listed as "to be determined"[6]. NARA complied with OMB guidance and submitted revised POA&Ms in April 2008; August 2009; and September 2009; however, no other updates were completed for the TIC POA&M. Further, the required subsequent updates were not provided to DHS as required by OMB memorandum M-09-06[7].

Also, additional planning documentation was not prepared as planned. Prior to the development of the Project Schedule in late 2010, no other detailed plans had been developed for this initiative. The 2009 IT Infrastructure Segment Program Plan stated TIC Migration Planning would be completed in second quarter of fiscal year 2010 (January through March 2010). However, the Project Schedule was not started until November 2010 and was not finalized until January 2011.

[6] See Attachment 1 for an excerpt from the POA&M last updated for the TIC initiative.

[7] OMB M-09-32, *Update on the Trusted Internet Connections Initiative*, September 17, 2009

In February 2011, we were informed that the POA&M for this project was no longer being maintained. Instead, only the Project Schedule was being maintained. This schedule aids in completing tasks related to the TIC implementation; however, it did not align with the requirements and deadlines outlined by OMB. Further, no other updates had been made to NARA's POA&M or submitted to DHS as required[8].

As a result, NARA's implementation of TIC has been delayed and project implementation did not begin until November 2010. Further, these delays had not been communicated to OMB and DHS, as required. NARA had not fully implemented TIC and was not in compliance with OMB's intentions. To be in compliance, agencies were required to continue their reduction and consolidation effort. The end-state of the TIC initiative is for each agency to meet the following targets: 100% compliance with the TIC critical technical capabilities and 100% of external connections routed through an approved TICAP. Despite the delayed implementation and limited POA&M documents, NH officials believed they were in compliance with OMB and DHS requirements.

Recommendation 3

The Chief Information Officer should ensure a comprehensive POA&M is completed for the TIC initiative and a periodic review and update of the POA&M is completed until full implementation. Once complete, the Chief Information Officer should ensure a POA&M is reported to DHS as required.

Management Response

Management comments were not received prior to issuance of the final report.

[8] Subsequent to our fieldwork, we were provided with an updated POA&M submitted to DHS later in February 2011. However, this POA&M did not provide an explanation or estimated completion date for the reduction and consolidation of all TIC access points. Further, formal deadlines still had not been established or tracked to disconnect all external non-TIC connections.

3. NARA Had Not Developed Contract Requirements for MTIPS Contract

In contracting for the MTIPS, NARA did not develop contract requirements or determine the appropriate CLINs needed for their environment. GSA provided guidance to agencies on how to determine the appropriate CLINs for their agency. Instead of following this process, NARA relied on their MTIPS contractor to select the appropriate CLINs, which consisted of over $118,000 of set-up or non-recurring costs and almost $720,000 (about $60,000 per month) of yearly recurring costs. With over 4,500 CLINs available, NARA lacks assurance it purchased the services needed for its environment.

Agencies seeking services from a TIC provider were encouraged to purchase the Managed Trusted Internet Protocol Services (MTIPS) CLINs through the NETWORX contract as part of their plan to reduce and consolidate their agency’s external connections. GSA’s guidance stated that agencies should determine their requirements for NETWORX ordering by conducting a complete analysis of current inventory of telecom services as well as projecting future operational needs. This analysis determines how NETWORX service offerings can best meet an agency’s needs. Then agencies should select a vendor through the Fair Opportunity process to meet those requirements.

Additional steps for requirements development were detailed in the NETWORX Fair Opportunity and Statement of Work (SOW) Guide. This guide explains that NETWORX telecommunications service requirements and ordering are directly linked to the NETWORX CLINs. This CLIN structure serves as a determinant of how an order will be placed under the NETWORX contract. The NETWORX contract allows agencies to develop their list of requirements from the universe of over 4,500 CLINs that were competed and competitively priced by vendors to facilitate ordering directly off the NETWORX contracts.

The first step in this process is to determine requirements using the agency’s telecommunications services inventory and other requirement to define their service requirements and group them into a Statement of Requirements (SOR) package. Then the agency should conduct a gap analysis to determine what requirements identified in their SOR can be met using the established CLINs in the NETWORX contract. A SOW is only required if requirements cannot be met using the fixed-price CLINs. When possible, agencies were encouraged to select from pre-determined and priced CLINs as the mechanism to procure TIC services from GSA. If the services can be accommodated solely by the fixed priced CLINs, then the agency should proceed with the Fair Opportunity decision process to select the contractor best suited to provide the required services under NETWORX. The agency should then document the basis for their decision or any exceptions to the Fair Opportunity process. Once completed, the agency may proceed to select qualified contractor and begin placing orders with the selected contractor.

However, we found that NARA had not determined the specific services or CLINs needed to be included in the contract for the NARANet environment. Instead, NARA relied on their NETWORX contractor, Qwest, to determine the appropriate CLINs for NARA's environment. Initially, NARA prepared a Statement of Requirements document, which included information relating to the current architecture, the "to-be" architecture, and their telecommunications requirements. However, the SOR was abandoned when NARA filed for an Exception to the Fair Opportunity Process. The basis for this exception was by issuing the MTIPS order to Qwest; NARA could avoid paying an estimated $180,000 in non-recurring costs and up to three years of duplicate recurring costs. According to the document filed with GSA, these costs would be incurred to allow for rework of another vendor. Therefore, this contract was issued on sole-source basis in the interest of economy and efficiency because it was a logical follow-on to a task order already issued on a competitive basis.

After filing the Exception to the Fair Opportunity Process, NARA selected Qwest as their preferred provider for the NETWORX MTIPS. Then in November 2010, a meeting was held with Qwest and the contractor was tasked with providing a quote and a proposed listing of CLINs for NARA[9]. In response, Qwest provided their price quote comprised of the CLINs selected by Qwest's MTIPS Design Engineer. The CLINs selected by Qwest totaled about $118,000 in non-recurring costs and almost $60,000 of monthly recurring costs.

When asked why NARA had not pre-determined the CLINs for their environment, the CTO stated that many of the CLINs appeared to be similar services and NARA lacked the expertise to distinguish the different services and pick the appropriate ones for NARA's environment. The CTO explained that Qwest was more familiar with their service offerings and the CLINs associated with these services. Therefore, they asked Qwest to determine the appropriate CLINs for NARA.

Since the contract was not selected on a competitive basis and NARA tasked the contractor with determining the appropriate CLINs, NARA lacks assurance it has purchased the appropriate services needed for its environment. Further, NARA lacks assurances that the most cost effective options were selected since NARA allowed the contractor to select the CLINs to be provided.

Recommendation 4

The Chief Information Officer should ensure metrics are identified to monitor the services provided by the MTIPS contractor as they are put in place to ensure they meet the needs of NARA's IT environment.

[9] Subsequent to our fieldwork, additional requirements documents, such as draft Statements of Work (SOW) were provided. However, as suggested by GSA, these SOWs were cancelled prior to awarding the contract to Qwest due to NARA's Exception to the Fair Opportunity Process. Documentation was not provided to demonstrate the requirements given to Qwest to develop their price proposal of NARA CLINs. Instead, we were informed that NARA worked with Qwest through a series of technical meetings to determine the MTIPS requirements. Further, no documentation could be provided for these meetings.

Management Response

Management comments were not received prior to issuance of the final report.

Recommendation 5

The Chief Information Officer should ensure the selected services provided by the MTIPS contractor are assessed once they are in place to ensure they meet the needs of NARA's IT environment.

Management Response

Management comments were not received prior to issuance of the final report.

4. NARA had not Developed Process to Monitor NETWORX Contract

NARA had not developed a formal process or assigned responsibilities to monitor the performance of the NETWORX contract. GSA developed guidance to help agencies manage and monitor the services ordered under the GSA NETWORX contract for IT services. However, NARA had not yet completed this task. By not having a process in place to manage and monitor this contract, NARA cannot ensure the appropriate levels of services are provided by Qwest, their NETWORX contractor. Further, credits can be received if service levels are not meet; however, these credits are not awarded automatically. Instead, NARA must submit requests for credits through the contractor and GSA.

To help agencies manage and monitor services ordered under the NETWORX contract, GSA developed the NETWORX Service Level Agreement (SLA) Management Guide. This guide provided information on managing the SLAs and outlined the roles and responsibilities of the contractor, the agency, and GSA that apply to telecommunications services obtained from NETWORX contractors. SLAs are established agreements between the government and the NETWORX contractors to provide services at performance levels that meet or exceed performance levels specified in the NETWORX contract. If specified service levels are not met, the contractor is required to issue specified credits, when requested to do so by the ordering agency. However, it is strictly up to the agency to decide how to perform its role in managing NETWORX SLAs.

As part of their contract, each NETWORX contractor is required to submit to the agency an "Agency-Specific SLA Monthly Compliance Report". Agencies should review this report and identify any SLAs for which there is a discrepancy. In the event that actual performance is less than required by the SLA, the agency is entitled to a credit. However, NETWORX SLA credits are not awarded automatically. Instead, the agency must request a credit and the agency has up to six months to request SLA credits. In this process, the agency is responsible for verifying the contractor's compliance assessments; resolving each SLA issue that affects the agency; and escalating any unresolved SLA issues to GSA.

We found that NARA had not yet developed a process to manage and monitor the SLAs associated with their NETWORX contract. Further, NARA had not yet assigned these roles and responsibilities within the agency to monitor the performance of Qwest, their NETWORX provider. During the contract planning, NARA should have developed a process and assigned responsibilities to verify the contractor’s compliance assessments and resolve each SLA issue that affects NARA. Also, a process should have been established to escalate any unresolved SLA issues to GSA. After our audit exit conference, we were provided with an email stating that an NH official believed that the Project Manager had been assigned the responsibility for monitoring the SLAs and applying for credits due to NARA.

During the audit, NH officials stated that a process had not yet been developed because the NETWORX contract had not been fully implemented. When asked if anyone had been appointed or assigned to monitor the SLAs, the CTO stated that no one had been appointed yet to monitor the SLAs. Instead, the NH official stated that someone will be appointed during the maintenance and operations phase of the project. While it is strictly up to the agency to decide how to perform its role in managing NETWORX SLAs, GSA recommends the review of the agency-specific SLA monthly compliance report and any resulting requests for SLA credits to be performed on a monthly basis.

By not establishing a formal process or assigning roles and responsibilities, NARA cannot ensure adequate management and monitoring of their NETWORX contractor's performance. Without adequate monitoring, NARA has no assurance they are receiving the services as intended. Further, if the SLAs are not met, NARA risks not receiving SLA credits, since it is NARA's responsibility, not GSA or Qwest, to request these credits.

Recommendation 6

The Chief Information Officer should ensure that GSA's guidance for managing NETWORX SLAs is implemented. Specifically,

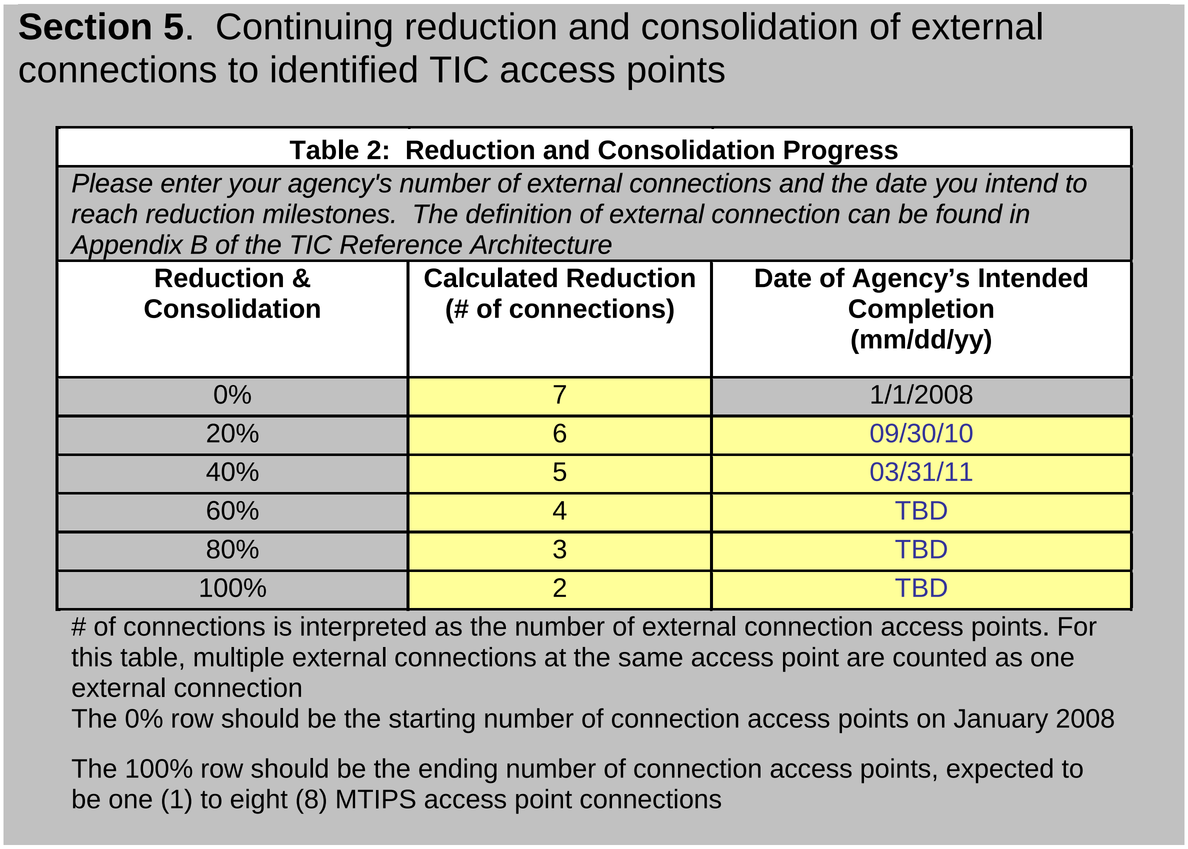
- A process should be developed to verify the contractor's compliance assessments and resolve each SLA issue that affects NARA.
- A process should be established to escalate any unresolved SLA issues to GSA.
- Roles and responsibilities within each of these processes are appropriately assigned.

Management Response

Management comments were not received prior to issuance of the final report.

Attachment 1 - POA&M

Excerpt from POA&M submitted to OMB in September 2009:



Section 5. Continuing reduction and consolidation of external connections to identified TIC access points

Table 2: Reduction and Consolidation Progress

Please enter your agency's number of external connections and the date you intend to reach reduction milestones. The definition of external connection can be found in Appendix B of the TIC Reference Architecture

Reduction & Consolidation	Calculated Reduction (# of connections)	Date of Agency's Intended Completion (mm/dd/yy)
0%	7	1/1/2008
20%	6	09/30/10
40%	5	03/31/11
60%	4	TBD
80%	3	TBD
100%	2	TBD

# of connections is interpreted as the number of external connection access points. For this table, multiple external connections at the same access point are counted as one external connection

The 0% row should be the starting number of connection access points on January 2008

The 100% row should be the ending number of connection access points, expected to be one (1) to eight (8) MTIPS access point connections

Appendix A – Acronyms and Abbreviations

CLIN	Contract Line Item Number
CNCI	Comprehensive National Cybersecurity Initiative
CIO	Chief Information Officer
CTO	Chief Technology Officer
DHS	Department of Homeland Security
GSA	U.S. General Service Administration
IT	Information Technology
MTIPS	Managed Trusted Internet Protocol Services
NARA	National Archives and Records Administration
NH	NARA’s Office of Information Services
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Actions and Milestones
SLA	Service Level Agreement
SOR	Statement of Requirements
SOW	Statement of Work
TIC	Trusted Internet Connections

Appendix B - Management's Response to the Report

On July 27, 2011 management was provided with a copy of the draft report for their review and comment. As usual, we provided management 30 calendar days for their written comments. At the time of report issuance more than 30 days past the original due date, management was still in the process of discussing comments and had not provided their final comments. Therefore, management comments were not provided at issuance of this report.

Appendix C - Report Distribution List

David S. Ferriero, Archivist of the United States, N
Debra Wall, Deputy Archivist, ND
Thomas Mills, Chief Operating Officer, C
Michael Wash, Chief Information Officer, Information Services, I
Haseen Uddin, Chief Technology Officer, CTO
Mary Drak, Strategy Division, Policy, CP