Audit Report

OIG-12-076

INFORMATION TECHNOLOGY: Treasury's Security Management of TNet Needs Improvement

September 27, 2012

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations

ATO	authority to operate
CIO	Chief Information Officer
COR	Contracting Officer's Representative
DoS	Denial of Service
IDC	Internet Data Center
ISSM	Information System Security Manager
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PMO	Program Management Office
SLA	Service Level Agreement
TNet	Treasury Network

The Department of the Treasury
Office of Inspector General

September 27, 2012

Robyn East
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Department of the Treasury

This report represents the results of our audit of the Department of the Treasury's (Treasury) security management of Treasury Network (TNet).[1] The objective of this audit was to determine whether Treasury ensured that TNet security controls met federal standards and guidelines.

To accomplish our objective, we reviewed and analyzed TNet's security-related documentation. We performed observation and testing at the TNet contractor, AT&T, facilities in Oakton and Ashburn, Virginia. We also interviewed Treasury and AT&T personnel responsible for the security management of TNet.

We performed our fieldwork in the Washington, DC, metropolitan area from November 2011 through June 2012. The audit was conducted in accordance with generally accepted government auditing standards. Our objectives, scope, and methodology are described in appendix 1.

Results in Brief

Based on the results of our work, we concluded that Treasury's security management of TNet needs improvement. Treasury did not ensure that security controls provided for TNet fully met federal standards and guidelines. Specifically, we found that:

[1] TNet is a wide area network that provides Treasury with e-mail, Internet, and voice traffic applications. The TNet task order was awarded under the General Services Administration Networx universal contract (Contract Number GS00T07NSD0007).

1. Weaknesses existed in physical security protection of TNet at AT&T's primary Internet Data Center (IDC) site.

2. Not all security controls required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3,[2] were tested and implemented.

3. TNet's patch management process was not fully implemented.

4. The Contracting Officer's Representative (COR) and TNet Program Management Office (PMO) did not adequately monitor TNet's security performance measures.

5. Plan of Action and Milestone (POA&M) management could be improved.

6. Certain TNet security procedures were not documented as required.

We are making 14 recommendations to Treasury's Chief Information Officer (CIO) to improve the security management of TNet.

In a written response to a draft copy of this report, the Treasury CIO agreed with our findings and recommendations and provided corrective action plans (see appendix 2). Treasury's planned corrective actions are responsive to the intent of our recommendations.

Background

TNet provides Treasury, its bureaus, and on-site contractors with telecommunication services. On September 21, 2007, Treasury procured TNet as a successor to the Treasury Communications System through the General Service Administration's Networx Universal Contract and selected AT&T as the vendor. At that time, TNet was estimated to cost $270 million. The total contract cost is

[2] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009).

now estimated at $449 million. Based on AT&T's proposal, implementation of TNet was to have started in October 2007. However, implementation under an interim authority to operate (ATO)[3] did not occur until August 2009. Furthermore, because of a number of security risks that needed to be remediated, TNet did not receive a full ATO until March 2011, more than a year and a half after the interim ATO.

The Internal Revenue Service Procurement Office was responsible for procurement, management, and administration of the TNet task order. On December 16, 2010, the Treasury Office of the CIO agreed to perform management oversight of TNet. The TNet PMO, which is located within the Office of the CIO, performs program oversight of the TNet contractor's operations. The TNet PMO also serves as an interface between Treasury and AT&T to monitor service level agreements (SLA) and manage invoices. TNet COR continues to work for the Internal Revenue Service and is responsible for, among other things, maintaining the complete contract working files.

We performed our audit at the TNet contractor, AT&T, facilities in Oakton and Ashburn, Virginia. AT&T's Enterprise Management Center located in Oakton, Virginia, is the primary facility that provides all network support, management, and maintenance for TNet. The backup facility is located in Durham, North Carolina. AT&T's IDC located in Ashburn, Virginia, is the primary facility that provides Treasury internet access through a Trusted Internet Connection. The backup IDC is located in Mesa, Arizona.

[3] ATO is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk associated with the system's operation. ATO can only be granted after the authorizing official has assessed the results of the certification and accreditation (a comprehensive assessment of the management, operational, and technical security controls for a system) package and deemed that the risk to agency operations, agency assets, or individuals is acceptable.

Findings and Recommendations

Finding 1 Weaknesses Existed in Physical Security Protection of TNet at AT&T's Primary IDC Site

We found weaknesses in physical security protection for TNet at AT&T's primary IDC site. Specifically, we found that some non-TNet AT&T personnel had physical access to TNet cages at the IDC without having undergone required background investigations. We also found that the IDC cages' power supply units were not locked. Finally, we found that 16 failed hard disk drives at the IDC were not properly labeled or tracked prior to destruction. It should be noted that after we informed Treasury officials of this matter, the TNet PMO told us that AT&T subsequently provided Treasury with the failed hard drives for destruction.

We found that AT&T technical support personnel working at the IDC had physical access to TNet's cages without having undergone a Treasury background investigation. The AT&T TNet IDC Architect informed us that AT&T granted physical access to these individuals for emergency purposes and that all AT&T technical support personnel undergo a background check as a condition of employment. However, AT&T was unable to provide us with any evidence that they performed a background investigation for the AT&T technical support personnel we identified. The TNet PMO stated that the IDC is not Treasury owned or controlled and that the persons lacking demonstrable security clearances were not involved in contracts that involve the design, operation, repair, or maintenance of information systems.

The TNet contract requires that AT&T adhere to all Treasury policies and procedures. Therefore, Treasury Directive Policy (TD P) 15-71[4] would apply to AT&T in this situation. This policy requires that all Federal employees, contractors, subcontractors, experts, consultants, and interns undergo a background investigation and favorable adjudication to determine their suitability and fitness for Treasury employment.

[4] TD P 15-71, "Treasury Security Manual, Chapter II section 2, Investigative Requirements for Federal Employees, Contractors, Subcontractors, Experts, Consultants and Paid/Unpaid Interns" (July 2011).

If non-TNet AT&T technical support personnel had physical access to TNet IDC cages without undergoing background investigation, there was an increased risk that individuals with unvetted backgrounds may have had physical access to Treasury assets without Treasury's consent. Accordingly, all personnel who need to have physical access to TNet's primary IDC cages, need to undergo background investigations.

We found that the IDC cages' power supply units were not locked even though AT&T TNet policy requires that all supporting infrastructure such as power, environmental conditioning, and security cages be protected.[5] According to the IDC Network Architect, the power supply units were left unlocked due to an oversight by AT&T technical support personnel. If power supply units for the IDC cages are not locked, the power could have been turned off by unauthorized individuals, which could have affected availability of service.

As mentioned above, we found a number of failed hard disk drives at the IDC that were not properly labeled or tracked prior to destruction. AT&T TNet policy requires that hard disk drives that cannot be cleared [wiped of content] because of a failure, be placed in a box marked "SENSITIVE BUT UNCLASSIFIED." Failed hard disk drives are to be released from the TNet environment only after they have been physically destroyed or degaussed using approved methods.[6]

The IDC Network Architect could not explain why the failed hard disk drives were not properly labeled or why they were not inventoried. Without an inventory of failed hard disk drives prior to destruction, missing or stolen drives could go undetected, which could allow for the inappropriate release of sensitive Treasury information. We have since been told that these disks were returned to Treasury for destruction.

[5] AT&T TNet policy, "Physical and Environmental Policy and Procedures," Version 2.0 (Apr. 2011).
[6] AT&T TNet policy, "Treasury Network Media Protection Policy and Procedures," Version 2.0 (Mar. 2011).

Recommendations

We recommend that the Treasury CIO do the following:

1. Ensure that a background investigation is performed for all AT&T personnel who need physical access to TNet's primary IDC cages.

Management Response

Treasury concurred with this recommendation. Treasury will send a contracts letter requiring AT&T to formally revoke physical access of any AT&T employee that does not have the requisite Treasury background investigation. It is anticipated that this planned corrective action will be completed by December 31, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

2. Remind AT&T to lock power supply units for TNet's primary IDC cages in accordance with AT&T TNet policy for physical and environmental controls.

Management Response

Treasury concurred with this recommendation. Treasury will send a contracts letter to AT&T, where the language in AT&T's Physical and Environmental Controls Policies and Procedures regarding secure access to all power supply units will be reiterated. It is anticipated that this planned corrective action will be completed by December 31, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

3. Amend TNet policy and procedures to require that failed hard disk drives be inventoried and destroyed promptly using a Treasury approved method.

Management Response

Treasury concurred with this recommendation. Treasury will direct AT&T to amend or modify its Media Protection Policy and Procedures so that failed hard disk drives are inventoried and destroyed using an approved method. It is anticipated that this planned corrective action will be completed by December 31, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

4. Ensure that failed hard disk drives at TNet's primary IDC are properly labeled and inventoried for tracking purposes and destroyed in a timely basis using a Treasury approved method.

Management Response

Treasury concurred with this recommendation. Treasury will require AT&T to provide quarterly hard drive destruction logs to ensure they are being labeled, inventoried, and destroyed in accordance with established policy. It is anticipated that this planned corrective action will be completed by June 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

Finding 2 Not All Security Controls Required by NIST SP 800-53, Revision 3, Were Tested and Implemented

We found that not all of the security controls required by NIST SP 800-53, Revision 3, dated August 2009, were tested and implemented for TNet. These security controls are the management, operational, and technical safeguards or countermeasures intended to protect the confidentiality, integrity, and availability of the system and its information.

The Treasury, AT&T TNet contract requires that AT&T comply with all National Institute of Standards and Technology (NIST) security policies as well as Treasury's information technology security policies, as these documents are modified and become available. Furthermore, Federal agencies are required to comply with NIST SPs within 1 year of the publication date unless otherwise directed by the Office of Management and Budget (OMB).[7] The 1 year compliance date applies to all new and/or revised NIST SPs.

According to the TNet PMO Director, in January 2011, a management decision was made to pursue an ATO for TNet which was to be based on compliance with security controls in NIST SP 800-53, Revision 2, dated December 2007 (under which significant work had already been performed), with the understanding that the security controls in NIST SP 800-53, Revision 3, dated August 2009, would be implemented sometime afterward. He also told us that a POA&M item was added to track compliance with NIST SP 800-53, Revision 3. We reviewed the 2012 POA&M, dated June 7, 2012, and found that an entry was made directing AT&T to comply with the most up-to-date NIST SP 800-53 guidance and prepare a revised TNet System Security Plan (SSP). We verified that the SSP was updated to incorporate the latest version of NIST SP 800-53. The TNet PMO later informed us that only one-third of the controls were tested.

[7] OMB Memorandum M-11-33, "FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," (Sept. 2011).

If all required security controls were not tested, TNet PMO could not ensure that the controls were in place and operating as intended. Therefore, safeguards or countermeasures intended to protect the confidentiality, integrity, and availability of TNet and its information could be ineffective.

Recommendation

5. We recommend that the Treasury CIO ensure that AT&T continue to test all NIST SP 800-53, Revision 3, security controls as soon as possible.

Management Response

Treasury concurred with this recommendation. Treasury will continue to test NIST SP 800-53 controls in accordance with Treasury policy. It is anticipated that this planned corrective action will be completed by June 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

Finding 3 TNet's Patch Management Process Was Not Fully Implemented

We found that TNet's patch management process was not fully implemented. Specifically, we found that the TNet flaw remediation process was incomplete. We also found that some of the quarterly vulnerability scans were not performed for all locations.

For the purposes of assessing the flaw remediation control, AT&T implemented 41 patches during calendar year 2011. According to the AT&T TNet Information System Security Manager (ISSM), TNet's flaw remediation process for fixing vulnerabilities consisted of the following five steps: (1) identification, (2) analysis, (3) technical review board, (4) testing, and (5) deployment. AT&T could not provide evidence that the five-step flaw remediation process was followed for the 41 patches. Furthermore, for calendar

year 2011, AT&T provided us evidence of some quarterly scanning for critical devices at its IDC in Ashburn, Virginia, and in Mesa, Arizona. Based on our review of the scan results provided from the Ashburn and Mesa locations, we found that a vulnerability discovered in the quarter one scan was reported again in the quarter two scan, indicating that the vulnerability had not been remediated in a timely manner. Additionally, we found that the quarter four scan for the Ashburn location was not performed.

NIST SP 800-53, Revisions 3, requires the following flaw remediation control procedures:

- The organization identifies, reports, and corrects information system flaws.
- The organization tests software updates related to flaw remediation for effectiveness before installation.
- The organization incorporates flaw remediation into the organizational configuration management process.

NIST SP 800-53, Revision 3, also requires the following vulnerability scanning control procedures:

- The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and/or the organization-defined process for random scans.
- The organization defines the response times for remediating legitimate vulnerabilities in accordance with an organizational assessment of risk.
- The organization remediates legitimate vulnerabilities in accordance with organization-defined response times.

NIST 800-53, Revision 3, provided up-to-date requirements for these controls; however, the majority of the controls were already required in Revision 2. AT&T TNet policy, "Patch and Vulnerability Management Policy and Procedures," Version 3.1, dated March 2011, requires that TNet Subject Matter Experts who specialize in and support a particular technology currently deployed within TNet do the following:

- Monitor vendor sites for their assigned technology for security patches and updates.
- Determine the impact of patches on the TNet environment and advise the TNet Technical Review Board.
- Test security patches prior to deployment.

AT&T TNet policy required that AT&T perform vulnerability scans on information systems and applications on a quarterly basis or when critical or high vulnerabilities are identified and reported. Critical vulnerabilities are required to be remediated within 72 hours of patch availability. However, AT&T TNet policy allowed for exceptions during system maintenance periods.

According to the AT&T TNet Information System Security Manager (ISSM), TNet's patch management process was not fully implemented during calendar year 2011. He said there was also a POA&M item related to this security weakness. He told us that Treasury officials had been made aware of this deficiency and that AT&T is working towards resolving the issue. Based on our review of the 2011 TNet POA&M, we confirmed that the item was entered into the POA&M.

AT&T was unable to explain why it did not follow the remediation process for all of the 41 patches it pushed through. Furthermore, AT&T was unable to tell us the why the vulnerability discovered in the quarter one scan was not addressed prior to the quarter two scan for the Ashburn and Mesa locations. Lastly, AT&T told us that the quarter four scan at the Ashburn location was not run due to technical issues.

By not fully implementing a comprehensive patch management process, TNet PMO cannot effectively manage the risks resulting from security vulnerabilities to TNet. If flaw remediation processes are not followed for all patches applied, patches may be deployed without approval and testing, which could render the system unavailable or inoperable. Furthermore, if missing patches are not identified and applied in a timely manner, the vulnerabilities resulting from these missing patches could put TNet at risk of exploitation, especially when TNet is facing the Internet. Lastly, TNet PMO is not fully compliant with NIST SP 800-53 and TNet policy for patch and vulnerability management.

Recommendations

We recommend that the Treasury CIO do the following:

6. Ensure that AT&T, in accordance with TNet PMO guidance, implements and documents all steps in the flaw remediation process for TNet.

Management Response

Treasury concurred with this recommendation. Treasury will require AT&T to provide Treasury with a flaw remediation process that has identifiable inputs, repeatable processes, tangible outputs, and mechanisms for communication. Treasury further stated that the process will be compliant with government and contractual requirements. It is anticipated that this planned corrective action will be completed by March 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

7. Ensure that quarterly vulnerability scans are performed and any discovered vulnerabilities are remediated within 72 hours of patch availability.

Management Response

Treasury concurred with this recommendation. Treasury will require AT&T to schedule quarterly vulnerability scans and provide evidence of completion, to include remediation of discovered vulnerabilities within 72 hours of patch availability. It is anticipated that this planned corrective action will be completed by December 31, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

Finding 4 The COR and TNet PMO Did Not Adequately Monitor TNet's Security Performance Measures

We found that the COR and TNet PMO did not adequately monitor AT&T's performance against the security performance measures provided for in its contract with Treasury. Specifically, the COR and TNet PMO did not ensure that all security-related performance measures were met during calendar years 2010 and 2011. The contract provided for the following security performance measures:

- The contractor is required to ensure that 75 percent of all TNet security controls comply satisfactorily with stated objectives as required by the NIST SPs and Treasury, prior to the biannual compliance verification.
- The contractor is required to implement within 36 hours United States Computer Emergency Readiness Team recommended patches or implement compensating controls to protect systems from the vulnerability the patch is intended to address until the patch can be tested to be effective and does not cause instability.
- The contractor is required to detect 100 percent of simulated intrusion attacks.
- The contractor is required to detect 100 percent of simulated denial of service (DoS) attacks.

However, we found that:

- AT&T did not perform the security control compliance testing in 2010. It should be noted that AT&T did perform security control compliance testing in 2011, with a 90 percent compliance rate.
- AT&T did not implement security patches within 36 hours of availability. Although we asked multiple times, neither the TNet PMO nor AT&T could provide a report indicating how long it took to implement patches.
- AT&T did not test TNet's security intrusion detection and DoS detection capability in 2011. It should be noted that AT&T did test for this in 2010 with no deficiencies identified.

While these performance measures were provided for in the contract, AT&T did not always meet them, and the COR and TNet

PMO did not independently monitor or evaluate AT&T's performance against them. As a result, the COR and TNet PMO did not notify the contracting officer about AT&T's failure to meet some of the required security performance measures.

Even if the contracting officer had been notified, we found that the TNet contract contained no penalties for not meeting the security performance measures discussed above. Treasury had an opportunity to incorporate penalties for not meeting these performance measures when the contract was amended in June 2011.

The TNet PMO told us that it only began to focus more on the security performance measures recently, seeing them as a low priority in the past. The TNet PMO told us that the security SLA, which are where the security performance measures discussed above are spelled out in the contract, were established as annual benchmarks or targets. According to the TNet PMO, only monthly SLAs had disincentives or penalties associated with them. Since the security SLAs had no associated disincentives, they were not priorities for the vendor. The TNet PMO also told us that the focus was on network stabilization, change management, and service delivery.

If security performance measures are not met, TNet may be vulnerable to attacks and compromises, including denial of service and other network intrusions. Furthermore, without effective monitoring and evaluation of the security related performance measures, the COR and TNet PMO may not be aware of AT&T's failure to comply with the required security performance measures in order to alert the CO. As a result, the CO may not be able to make informed decisions in administering the contract in the best interest to the government. Without penalties in the contract for the security related performance measures, Treasury may have no legal recourse to assess damages or apply disincentives against AT&T for the failure to meet the security performance measures.

Recommendations

We recommend that the Treasury CIO do the following:

8. Ensure that security control compliance testing is performed in accordance with the contract.

Management Response

Treasury concurred with this recommendation. Treasury will continue to track security control compliance testing in accordance with contractual requirements. It is anticipated that this planned corrective action will be completed by June 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

9. Ensure that security patches are implemented within 36 hours of availability in accordance with the contract.

Management Response

Treasury concurred with this recommendation. Treasury will require AT&T to provide Treasury with a contractually compliant flaw remediation process that has identifiable inputs, repeatable processes, tangible outputs, and mechanisms for communication. It is anticipated that this planned corrective action will be completed by March 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

10. Ensure that testing for intrusion detection and DoS detection is performed in accordance with the contract.

Management Response

Treasury concurred with this recommendation. Treasury will retain a new Trusted Internet Connection provider that will provide intrusion detection and denial of service detection. It is anticipated that this planned corrective action will be completed by March 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

11. Ensure that TNet PMO, in coordination with the contracting officer and COR, review all security performance measures in the contract, negotiate with AT&T the terms for when penalties are to be applied in the event a measure is not met, and amend the contract accordingly.

Management Response

Treasury concurred with this recommendation. Treasury will evaluate the utility, adequacy, and enforceability of existing SLAs and collaborate with AT&T to define security performance measures and negotiate possible penalties. It is anticipated that this planned corrective action will be completed by June 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

Finding 5 POA&M Management Could Be Improved

We found that certain security weaknesses were not always remediated on schedule, and that the POA&M was not always documented in accordance with OMB and NIST guidance. Based on our review of the 2011 TNet POA&M, we found that the TNet PMO did not ensure that 4 of 53 security weaknesses scheduled to be completed in 2010 were remediated on schedule. It took the

TNet PMO 18 to 26 months longer than the scheduled completion date to resolve these four security weaknesses. We also found that justifications for POA&M item delays, waivers, and cancellations were not always documented, and that the TNet POA&M sections, such as milestone changes and source of weaknesses, were not completed in accordance with OMB requirements.

OMB Memorandum 02-01[8] requires federal agencies to implement a POA&M process to identify tasks that are necessary to remediate identified security weaknesses. The POA&M is to include details of the weaknesses, point of contact, resources required, scheduled completion date, milestones with completion dates, changes to milestones, source of the identification of the weakness (i.e., audit report or other review), and status.

NIST SP 800-65[9] recommends, among other things, that changes to the milestones section of the POA&M, document any changes to timelines. It also recommends the POA&M's source of security weakness section, document where and how the weakness was identified (e.g., risk assessment). Lastly, the POA&M's comments section provides space for additional detail or clarification (e.g., causes for delays or potential factor that may impact weakness mitigation).

According to the TNet PMO Director, who was not with the TNet PMO at the time when the security weaknesses were recorded in the 2011 POA&M, the reason why the security weaknesses were not remediated in a more timely manner was due to higher priority efforts given to the transition of the wide-area-network from Treasury Communication System to TNet. With regard to not having justifications for POA&M item delays, waivers, and cancellations, the TNet PMO Director was unable to explain why these decisions were not documented in the POA&M.

If security weaknesses are not remediated in a timely manner, they could compromise the confidentiality, integrity, or availability of

[8] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (Oct. 17, 2001).
[9] NIST SP 800-65, Version 1.0, *Integrating IT Security into the Capital Planning and Investment Control Process* (Jan. 2005).

TNet's systems. Also, by not completing the POA&M's sections for changes to milestones, source of weakness, and comments, Treasury officials may not be able to effectively track the progress of corrective actions.

Recommendations

We recommend that the Treasury CIO do the following:

12. Ensure that security weaknesses are remediated on schedule and where there are delays, waivers, or cancellations, they be documented in the POA&M.

Management Response

Treasury concurred with this recommendation. Treasury will work toward remediating security weaknesses on schedule and ensure delays, waivers, cancellations, milestone changes, and the sources of security weaknesses are entered into Trusted Agent FISMA. It is anticipated that this planned corrective action will be completed by October 15, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

13. Ensure that the POA&M sections for milestone changes, source of security weakness, and comments are complete.

Management Response

Treasury concurred with this recommendation. Treasury will ensure delays, waivers, cancellations, milestone changes, and the sources of security weaknesses are entered into Trusted Agent FISMA. It is anticipated that this planned corrective action will be completed by October 15, 2012.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

Finding 6 Certain TNet Security Procedures Were Not Documented As Required

We found that certain other TNet procedures need to be more fully documented. For example, we found that AT&T's procedures for configuration management, security planning, and system and services acquisition were incomplete or missing information.

NIST SP 800-53, Revision 3, requires that:

- The organization configuration management procedures facilitate implementation of the configuration policy and associated configuration management controls.
- The organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls.
- The organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls.

NIST 800-53, Revision 3, contains up-to-date requirements for these procedures; however, these procedures were already required in Revision 2.

According to the AT&T TNet ISSM, all policy statements will not have corresponding procedures. He said that there are times when the policy statement is considered to be sufficiently explanatory. When this is the case, AT&T does not document step-by-step procedures. While we acknowledge the AT&T TNet ISSM's rationale, we believe that configuration management, security planning, and system and services acquisition need documented procedures in order to facilitate consistent conformance to technical requirements and practices. Also, as a result of the documentation issues noted above, AT&T TNet procedures are in non-compliance with NIST SP 800-53, Revision 3, requirements.

Procedures that contain incomplete or missing information increase the risk of inconsistent practices among AT&T personnel.

Recommendation

14. We recommend that the Treasury CIO ensure that AT&T's procedures for configuration management, security planning, and system and services acquisition are fully documented.

Management Response

Treasury concurred with this recommendation. Treasury will require AT&T to map each requirement to a corresponding procedure in the policy documents referenced. It is anticipated that this planned corrective action will be completed by March 1, 2013.

OIG Comment

Management's planned corrective action is responsive to our recommendation.

* * * * * *

I would like to extend my appreciation to the Office of the CIO and the TNet PMO for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Farbod Fakhrai, Information Technology Audit Manager, at (202) 927-5841. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Director of Information Technology Audits

The report represents the results of our audit of the Department of the Treasury's security management of Treasury Network (TNet). The objective of this audit was to determine whether Treasury ensured that TNet security controls met federal standards and guidelines. This audit was included in the *Office of Inspector General Annual Plan for 2012*.

To accomplish our objective, we reviewed and analyzed TNet's security related documentation including policies and procedures. We performed observation and testing at the TNet contractor, AT&T, facilities in Oakton and Ashburn, Virginia. We also interviewed Treasury and AT&T personnel responsible for the security management of TNet. We utilized National Institute of Standards and Technology guidelines to assess TNet's management, operational, and technical controls. We performed our fieldwork in the Washington, DC, metropolitan area from November 2011 through June 2012. The results of this audit may be used to support our work undertaken in accordance with the requirements of the Federal Information Security Management Act.

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.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SEP 21 2012

MEMORANDUM FOR TRAM J. DANG
AUDIT DIRECTOR
OFFICE OF THE INSPECTOR GENERAL

FROM: for Robyn East
Deputy Assistant Secretary for Information Systems
and Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – "Treasury's Security Management of the Treasury Network (TNet) Needs Improvement"

Thank you for the opportunity to comment on the draft audit report entitled "Treasury's Security Management of the Treasury Network (TNet) Needs Improvement". The objective of this audit was to determine whether Treasury ensured that TNet security controls met federal standards and guidelines.

Since being granted an Authority to Operate, security management has improved. TNet has hired a permanent Information Systems Security Manager to relieve the person on detail from the Internal Revenue Service. TNet has undergone multiple penetration tests and continuous monitoring assessments with no major findings. TNet has transitioned from NIST SP 800-53 Revision 2 to Revision 3 and is planning its transition to Revision 4. TNet has also migrated its Trusted Internet Connection (TIC) from a commercial provider to a government organization.

We have carefully reviewed the draft report and are in agreement with all findings and recommendations. It underscores a number of items we have identified and taken measures to correct. For example, our Plan of Actions and Milestones has items related to vulnerability management and control testing. Please refer to the attachment for further details on our planned corrective actions.

We appreciate the audit recommendations, as they will help improve our security posture. If you have any questions, please contact Scott Hill, Chief Information Security Officer for Departmental Offices at 202-622-4264.

Attachment

cc: Edward A. Roback, Associate Chief Information Officer for Cyber Security and Chief Information Security Officer

Management Response to OIG Recommendations

Note: The Department agrees with all findings and recommendations.

(U) OIG Finding 1: Weaknesses Existed in Physical Security Protection of TNet at AT&T's Primary IDC Site.

(U) OIG Recommendation 1: Ensure that a background investigation is performed for all AT&T personnel who need physical access to TNet's primary Internet Data Center (IDC) cages.
(U) Treasury Response: Treasury will send a contracts letter requiring AT&T, in accordance with Personnel Security requirements in Treasury Directive Publication (TD P) 15-71, to formally revoke physical access of any AT&T employee that does not possess the requisite Treasury background investigation. Target completion: December 31, 2012.
(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Recommendation 2: Remind AT&T to lock power supply units for TNet's primary IDC cages in accordance with AT&T TNet policy for physical and environmental controls.
(U) Treasury Response: Treasury will send a contracts letter to AT&T reiterating the language in their *Physical and Environmental Controls Policies and Procedures* and instructing them to secure access to all power supply units. Target completion: December 31, 2012.
(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Recommendation 3: Amend TNet policy and procedures to require that failed hard disk drives be inventoried and destroyed promptly using a Treasury approved method.
(U) Treasury Response: Treasury will direct AT&T to amend or modify its *Media Protection Policy and Procedures* so that failed hard disk drives are inventoried and destroyed using an approved method. Target completion: December 31, 2012.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Recommendation 4: Ensure that failed hard disk drives at TNet's primary IDC are properly labeled and inventoried for tracking purposes and destroyed promptly using a Treasury approved method.
(U) Treasury Response: Treasury will require AT&T to provide quarterly hard drive destruction logs to ensure they are being labeled, inventoried, and destroyed in accordance with established policy. Target completion: June 1, 2013.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Finding 2: Not All Security Controls Required by NIST SP 800-53, Revision 3, Were Tested and Implemented.

(U) OIG Recommendation 5: We recommend that the Treasury CIO ensure that AT&T continues to test all National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, security controls as soon as possible.
(U) Treasury Response: Treasury will continue to test NIST SP 800-53 controls in accordance with Treasury policy. Target completion: June 1, 2013.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Finding 3: TNet's Patch Management Process Was Not Fully Implemented.

(U) OIG Recommendation 6: Ensure that AT&T, in accordance with TNet Program Management Office (PMO) guidance, implements and documents all steps in the flaw remediation process for TNet.
(U) Treasury Response: Treasury will require AT&T to provide Treasury with a flaw remediation process that has identifiable inputs, repeatable processes, tangible outputs, and mechanisms for communication. The process will be compliant with government requirements (for example, SP 800-53r3) and contractual requirements. Target completion: March 1, 2013.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Recommendation 7: Ensure that quarterly vulnerability scans are performed and any discovered vulnerabilities are remediated within 72 hours of patch availability.
(U) Treasury Response: Treasury will require AT&T to schedule quarterly vulnerability scans and provide evidence of completion, to include remediation of discovered vulnerabilities within 72 hours of patch availability. Target completion: December 31, 2012.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Finding 4: The COR and TNet PMO Did Not Adequately Monitor TNet's Security Performance Measures.

(U) OIG Recommendation 8: Ensure that security control compliance testing is performed in accordance with the contract.
(U) Treasury Response: Treasury will continue to track security control compliance testing in accordance with contractual requirements. Target completion: June 1, 2013.

(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Recommendation 9: Ensure that security patches are implemented within 36 hours of availability in accordance with the contract.
(U) Treasury Response: Treasury will require AT&T to provide Treasury with a contractually compliant flaw remediation process that has identifiable inputs, repeatable processes, tangible outputs, and mechanisms for communication. Target completion: March 1, 2013.
(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Recommendation 10: Ensure that testing for intrusion detection and denial of service detection is performed in accordance with the contract.
(U) Treasury Response: Treasury will retain a new Trusted Internet Connection (TIC) provider that will provide intrusion detection and denial of service detection. Target completion: March 1, 2013.
(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Recommendation 11: Ensure that TNet PMO, in coordination with the contracting officer and contracting officer's representative, review all security performance measures in the

contract, negotiate with AT&T the terms for when penalties are to be applied in the event a measure is not met, and amend the contract accordingly.
(U) Treasury Response: Treasury will evaluate the utility, adequacy, and enforceability of existing Service Level Agreements (SLAs) and collaborate with AT&T to define security performance measures and negotiate possible penalties. Target completion: June 1, 2013.
(U) Responsible Official: TNet Contracting Officer's Representative

(U) OIG Finding 5: POA&M Management Could Be Improved.

(U) OIG Recommendation 12: Ensure that security weaknesses are remediated on schedule and where there are delays, waivers, or cancellations, they be documented in the POA&M.
(U) Treasury Response: Treasury will work toward remediating security weaknesses on schedule and ensure delays, waivers, cancellations, milestone changes, and the sources of security weaknesses are entered into Trusted Agent FISMA (TAF). Target completion: October 15, 2012.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Recommendation 13: Ensure that the POA&M sections for milestone changes, source of security weakness, and comments are complete.
(U) Treasury Response: Treasury will ensure delays, waivers, cancellations, milestone changes, and the sources of security weaknesses are entered into Trusted Agent FISMA (TAF). Target completion: October 15, 2012.
(U) Responsible Official: TNet Information Systems Security Manager

(U) OIG Finding 6: Certain TNet Security Procedures Were Not Documented As Required.

(U) OIG Recommendation 14: We recommend that the Treasury CIO ensure that AT&T's procedures for configuration management, security planning, and system and services acquisition are fully documented.
(U) Treasury Response: Treasury will require AT&T to map each requirement to a corresponding procedure in the policy documents referenced. Target completion: March 1, 2013.
(U) Responsible Official: TNet Information Systems Security Manager

Office of Information Technology (IT) Audits

Tram J. Dang, Audit Director
Farbod Fakhrai, IT Audit Manager
Abdirahman Salah, Former IT Audit Manager
Robert Kohn, Auditor-in-Charge
Kevin Mfume, IT Specialist
Don'te Kelley, IT Specialist
Mitul Patel, IT Specialist
Jason Beckwith, IT Specialist
Jason Madden, Referencer

Department of the Treasury

Office of the Chief Information Officer

Office of Strategic Planning and Performance Management

Office of the Deputy Chief Financial Officer, Risk and Control Group

Office of Management and Budget

Office of Inspector General Budget Examiner