Evaluation Report

OIG-CA-09-007

INFORMATION TECHNOLOGY: Treasury's Federal Desktop Core Configuration Deviation Tracking Process Is Inadequate

February 19, 2009

Office of Inspector General

Department of the Treasury

Contents

Evaluation Report 3

Results in Brief 3

Background 4

Finding and Recommendations 7

OCIO's FDCC Deviations Tracking Is Inadequate 7
Recommendations 8

OCIO's FDCC Deviations Tracking Policies Are Inconsistent 8
Recommendation 9

Appendices

Appendix 1: Objective, Scope, and Methodology 12
Appendix 2: Management Response 13
Appendix 3: Major Contributors 15
Appendix 4: Report Distribution 16

Abbreviations

CIO	chief information officer
FDCC	Federal Desktop Core Configuration
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Treasury Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	plan of action and milestones
TCIO	Treasury Chief Information Officer
TTB	Alcohol and Tobacco Tax and Trade Bureau

Michael D. Duffy
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Department of the Treasury

We recently completed the evaluation of the Department of the Treasury's Alcohol and Tobacco Tax and Trade Bureau (TTB) to determine whether sufficient protections exist to prevent intrusions into TTB's network and systems.[1] We also examined TTB's compliance with the requirement to implement the National Institute of Standards and Technology (NIST) Federal Desktop Core Configuration (FDCC).[2] During our evaluation, several matters relating to the Treasury Office of the Chief Information Officer's (OCIO) policies and procedures for tracking FDCC deviations came to our attention. We are issuing this report to address these matters.

We performed our fieldwork at TTB from January through July 2008. We performed subsequent follow-up work with OCIO through January 2009. Appendix 1 contains a detailed description of our objective, scope, and methodology.

Results in Brief

We determined that Treasury's FDCC deviation tracking policies and procedures need improvement. Specifically, we noted that while OCIO tracks the number of deviations reported by the bureaus on a monthly basis, it does not track or evaluate the

[1] *Information Technology: Network Security at the Alcohol and Tobacco Tax and Trade Bureau Could Be Improved*, OIG-CA-09-005 (Dec. 18, 2008).
[2] Office of Management and Budget Memorandum (OMB) M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" (Mar. 22, 2007), required agencies to implement common security configurations developed by NIST for Windows Vista and XP operating systems by February 1, 2008.

details associated with each deviation. For instance, OCIO does not keep track of the name of the FDCC setting that will not be implemented, description of the FDCC setting, bureau justification for not implementing the FDCC setting, and estimated remediation date for each deviation. In addition, we found that the Treasury Chief Information Officer's (TCIO) policies provide inconsistent instructions on tracking security weaknesses.

Our two overall findings are as follows:

1. OCIO's FDCC deviations tracking is inadequate.
2. OCIO's FDCC deviations tracking policies are inconsistent.

We are making the following three overall recommendations to the Treasury Chief Information Officer (CIO) to address the above issues:

1. Expand OCIO's FDCC deviation tracking to include the name of the FDCC setting that will not be implemented, description of the FDCC setting, bureau justification for not implementing the FDCC setting, and estimated remediation date for each deviation, if applicable.
2. Review and evaluate the legitimacy of the deviations reported by the bureaus.
3. Replace or update TCIO M-07-04 and M-08-04 to provide consistent guidance for tracking FDCC deviations.

Treasury CIO concurred with our findings and recommendations and provided plans for corrective actions (see appendix 2).

Background

Organized into bureaus and offices, Treasury encompasses a wide range of programs and operations. The Treasury bureaus include TTB, the Bureau of Engraving and Printing, the Bureau of the Public Debt, the Community Development Financial Institutions Fund, the Financial Crimes Enforcement Network, the Financial Management Service, the Internal Revenue Service, the Office of the Comptroller of the Currency, the Office of Inspector General, the Office of Thrift Supervision, the United States Mint, and the Treasury Inspector General for Tax Administration. The Treasury offices are composed of divisions headed by Assistant Secretaries and Under

Secretaries who are primarily responsible for policy formulation and overall management of Treasury. These offices are collectively known as Departmental Offices.

Office of Management and Budget (OMB) Memorandum 07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," required that agencies implement common security configurations developed by NIST for Windows Vista and XP operating systems by February 1, 2008.[3] Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. They allow agencies to improve system performance, decrease operating costs, and help ensure public confidence in the confidentiality, integrity, and availability of government information. OMB Memorandum 07-18, "Ensuring New Acquisitions Include Common Security Configurations," requires new acquisitions to include these configurations and information technology (IT) providers to certify that their products operate effectively using these configurations.[4]

OMB recognizes that some agencies may have difficulty implementing all the FDCC requirements because of technical issues. On March 20, 2007, OMB issued a memorandum instructing agencies to provide documentation to NIST of any deviations from the FDCC common security baseline and the rationale for such deviations.[5] Additionally, OMB instructed agencies to report FDCC compliance through their organization's CIO hierarchy. Compliance is expressed in terms of numbers of compliant versus noncompliant computers. For noncompliant computers, CIOs must provide a representative sample of Security Content Automation Protocol–based assessment reports.[6] This information should be sent to OMB with a copy to NIST, which will perform trend analysis on all federal data on noncompliant computers and present findings to OMB.

[3] OMB M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" (Mar. 22, 2007).
[4] OMB M-07-18, "Ensuring New Acquisitions Include Common Security Configurations" (June 1, 2007).
[5] Memorandum from Karen Evans, Administrator, Office of E-Government and Information Technology, to Chief Information Officers, "Managing Security Risk By Using Federal Desktop Core Configuration" (Mar. 22, 2007).
[6] The Security Content Automation Protocol is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., Federal Information Security Management Act compliance).

The Treasury CIO is responsible for implementing FDCC for Treasury and reporting compliance to OMB and NIST. OCIO policies relating common security configurations or FDCC are as follows:

- TCIO memorandum M-07-01, "Security Configuration and Vulnerability Management Policy" (January 30, 2007), requires Treasury bureaus and offices to use the NIST security configuration checklists repository. This memorandum was designed to address the finding in the 2006 Federal Information Security Management Act report that Treasury lacks agency-wide configuration management policy.

- TCIO memorandum M-07-04 requires bureaus to use the OMB-specified Windows XP and Vista configuration settings as the basis for deployed standard security configurations. TCIO M-07-04 also states that any security weaknesses identified during the development or execution of bureau plans regarding use of common security configurations should be entered in the plan of action and milestone (POA&M)[7] process as described in the TCIO memorandum M-06-01, "Improving the Department's Security Plan of Action and Milestone (POA&M) Process" (March 24, 2006).

- TCIO memorandum M-08-04 states that deviations from the FDCC baselines for Vista and XP (and other platforms as FDCC settings are established) are to be considered weaknesses and tracked for remediation via bureau POA&M process unless a bureau has documented a business requirement for the deviation(s) as an element of a modified FDCC baseline configuration. FDCC settings for Vista and XP are expected to change over time. A single POA&M entry can address one or multiple deviations, provided the deviations are broken out elsewhere to help ensure completeness and so that remediation can be tracked.

[7] Agency CIOs, working with other appropriate agency officials, are responsible for developing a POA&M for each program and system for which a weakness was identified. The purpose of a POA&M is to help agencies identify, assess, prioritize, and monitor progress of corrective efforts for security weaknesses in programs and systems.

Findings and Recommendations

Finding 1 OCIO's FDCC Deviations Tracking Process Is Inadequate

We determined that the OCIO's FDCC deviations tracking process is inadequate. Even though OCIO tracks the number of deviations reported by the bureaus on a monthly basis, it does not track the details associated with each deviation and the bureaus' rationale for the deviation. For example, during our review of TTB's FDCC compliance, we requested that OCIO provide us with a copy of TTB's deviation submission for April 2008. After reviewing TTB's submission to OCIO, we were able to verify that TTB had reported 11 deviations to OCIO. However, we were unable to verify the details of these deviations because OCIO does not track this information. Specifically, OCIO does not keep track of the FDCC setting name, description, and the justification for the deviated settings. Also, we could not determine whether OCIO was able to evaluate the justification for the deviation or whether the deviation reflected a reasonable business requirement.

In the March 20, 2007 memorandum to CIOs, OMB instructed agencies to provide documentation to NIST of any deviations from the FDCC common security baseline and the rationale for doing so. Additionally, OMB instructed agencies to report FDCC compliance through their organization's CIO hierarchy. The Treasury CIO is responsible for implementing FDCC for Treasury and reporting compliance to OMB and NIST.

It is vital to maintain complete records on all FDCC deviations, including deviation details such as the FDCC setting name and description, as well as any bureau rationale for the deviations. If the details of the deviations are not tracked, OCIO may not have an effective method of overseeing and reviewing the legitimacy of the reported deviations. In addition, OCIO cannot draw conclusions based solely on the number of deviations reported by bureaus; additional detail is necessary. Failure to maintain complete information on FDCC deviations could adversely affect the accuracy of Treasury's FDCC deviations submission to NIST for OMB reporting.

Recommendations

We recommend that the Treasury CIO

1. expand FDCC deviation tracking to include the name of the FDCC setting that will not be implemented, description of the FDCC setting, bureau justification for not implementing the FDCC setting, and estimated remediation date for each deviation, if applicable; and
2. review and evaluate the legitimacy of the deviations reported by the bureaus.

Finding 2 OCIO's FDDC Deviations Tracking Policies Are Inconsistent

During our evaluation at TTB, we found that the following two TCIO policies provide inconsistent instructions to the bureaus for tracking security weaknesses:

- TCIO M-07-04, "Implementation of Common Security Configurations for IT Systems Using Windows XP or Vista" (April 17, 2007)

- TCIO M-08-04, "Additional Cyber Security Controls and Recommended Practices," section CVM.11 (June 27, 2008)

On April 17, 2008, OCIO issued TCIO M-07-04 as its guidance to Treasury bureaus for implementing common security configurations for IT Systems using Windows XP or Vista. Specifically, TCIO M-07-04 also states, "consistent with the requirements set forth in OMB memorandums M-O7-11, the bureaus are to use the OMB-specified Windows XP and Vista configuration settings, as the basis for deployed standard security configuration." TCIO M-07-04 requires that "any security weaknesses identified during the development or execution of bureau plans regarding use of common security configurations should be entered into the POA&M process as described in the TCIO M-06-01." TCIO M-07-04 was issued to implement requirements in OMB-07-11 directing agencies with Windows XP deployed and/or that plan to upgrade to the Vista operating system to adopt the FDCC, also known as commonly accepted security configurations.

On June 27, 2008, OCIO issued TCIO memorandum M-08-04, stating that "deviations from the FDCC baselines for Vista and XP (and other platforms as FDCC settings are established) shall be considered weaknesses and tracked for remediation via bureau POA&M process unless a bureau has documented a business requirement for the deviation(s) as an element of a modified FDCC baseline configuration."

We contacted OCIO about the unclear guidance. According to OCIO, bureaus are not required to track an FDCC deviation as a security weakness in the POA&M process as long as they have documented the rationale for the deviation. However, TCIO M-08-04 does not contain any clause to nullify the policy requirement in TCIO M-07-04 that "any security weaknesses identified during the development or execution of bureau plans regarding use of common security configurations should be entered into the POA&M process."

The Treasury CIO is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as for oversight of a number of IT programs. Among these programs is Cyber Security, whose mission is to develop and implement IT security policies and provide policy compliance oversight for both unclassified and classified systems managed by each of Treasury's operating bureaus and offices. The Treasury CIO has given the Associate CIO for Cyber Security responsibility for managing and directing OCIO's Cyber Security program, as well as for ensuring compliance with applicable statues, regulations, policies, and guidance.

OCIO policies and guidance on tracking FDCC deviations tracking remain unclear and inconsistent and, as a result, subject to interpretation. Therefore, confusion may occur and compliance with IT security policy may be impossible to effectively enforce.

Recommendation

We recommend that Treasury CIO

3. replace or update TCIO M-07-04 and M-08-04 to provide consistent guidance for tracking FDCC deviations.

Management Response

As noted in appendix 2, OCIO agreed with our findings and recommendations, and will be implementing our recommendations by May 2009.

OIG Response

We agree that the formal steps OCIO has proposed are responsive to the intent of our findings and recommendations.

* * * * * *

If you have any questions, please contact me at (202) 927-5171 or Abdirahman Salah, IT Specialist, Office of Information Technology Audits, at (202) 927-5763. Major contributors to this report are listed in appendix 2.

/s/

Tram J. Dang, Director
Office of Information Technology Audits

We recently completed an evaluation to determine whether sufficient protections exist at the Alcohol and Tobacco Tax and Trade Bureau (TTB) to prevent intrusions into TTB's network and systems.[8] We also examined TTB's compliance with the requirement to implement the National Institute of Standards and Technology Federal Desktop Core Configuration (FDCC).[9] Our primary objective for this report was to address the matters that came to our attention during our evaluation at TTB relating to the Office of Chief Information Officer's (OCIO) policies and procedures for tracking FDCC deviations. To accomplish this objective, we analyzed documents received from TTB and OCIO relating to FDCC, reviewed Treasury Chief Information Officer policies, and contacted TTB and OCIO personnel for clarification.

We performed our fieldwork at TTB from January through July 2008. We performed subsequent follow-up work with OCIO through January 2009. Fieldwork was conducted at TTB headquarters and at OCIO in Washington, D.C.

[8] *Information Technology: Network Security at the Alcohol and Tobacco Tax and Trade Bureau Could Be Improved*, OIG-CA-09-005 (Dec. 18, 2008).

[9] Office of Management and Budget Memorandum (OMB) M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" (Mar. 22, 2007), required agencies to implement common security configurations developed by NIST for Windows Vista and XP operating systems by February 1, 2008.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

FEB 13 2009

MEMORANDUM FOR TRAM J. DANG
DIRECTOR, OFFICE OF INFORMATION TECHNOLOGY AUDIT

FROM: Michael D. Duffy
Deputy Assistant Secretary for Information Systems and Chief Information Officer

SUBJECT: Discussion Draft Report – *Federal Desktop Core Configuration (FDCC) Deviation Tracking Progress is Inadequate*

Management Response to Discussion Draft Audit Report *-- Federal Desktop Core Configuration Deviation Tracking Progress is Inadequate – February 5, 2009*

FINDING 1 – OCIO'S FDCC Deviations Tracking Process is Inadequate

Recommendation: We recommend that the Treasury CIO expand FDCC deviation tracking to include the name of the FDCC setting that will not be implemented, description of the FDCC setting, bureau justification for not implementing the FDCC setting, and estimated remediation date for each deviation, if applicable.

Treasury Response: We will obtain (and/or update current records as necessary) from Bureaus their FDCC deviations that will not be implemented for purposes of Department-wide tracking. This will include the name of the FDCC setting(s) that will not be implemented, description of the FDCC setting(s), bureau justification for not implementing the FDCC setting(s), and estimated remediation date for each deviation, if applicable.

Additionally, we plan to issue revised FDCC policy, as discussed below in response to the second finding regarding tracking of deviations within Plans of Action and Milestones (POA&Ms). Our intent is that this policy will also identify FDCC settings that the Treasury CIO has determined are impractical to implement within Treasury because of the adverse impact such settings would have on the ability to perform the Treasury business functions. We plan to institute a process for the Treasury CIO to make similar determinations for settings similarly affecting only a specific Bureau(s). Once published via policy, bureaus would no longer need to report these as "deviations." FDCC implementation will be considered complete at a Bureau when all other applicable FDCC settings are implemented.

Planned Completion Date: April 1, 2009

Recommendation: We recommend that the Treasury CIO review and evaluate the legitimacy of the deviations reported by the bureaus.

Treasury Response: The Treasury CIO will review and evaluate the legitimacy of the deviations reported by the bureaus. We will notify the Bureau whether the Treasury CIO has approved the Bureau deviation(s) in whole or in part. Please also see comment above regarding planned policy changes.

Planned Completion Date: May 1, 2009

FINDING 2 – OCIO's FDCC Deviations Tracking Policies are Inconsistent

Recommendation: We recommend that the Treasury CIO replace or update TCIO M-07-04 and M-08-04 to provide consistent guidance for tracking FDCC deviations.

Treasury Response: The Treasury CIO will update TCIO M-07-04 and M08-04 accordingly.

Planned Completion Date: May 1, 2009

If you have any questions on this matter, please contact Ed Roback, Associate CIO for Cyber Security at 202-622-2593.

Appendix 3
Major Contributors

Office of Information Technology Audits

Tram J. Dang, Director
Abdirahman M. Salah, IT Specialist (Lead)
Gerald J. Steere, IT Specialist
Jane Lee, IT Specialist
Larissa Klimpel, IT Specialist
Shiela S. Michel, Referencer

Appendix 4
Report Distribution

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management

Office of Management and Budget

Office of Inspector General Budget Examiner