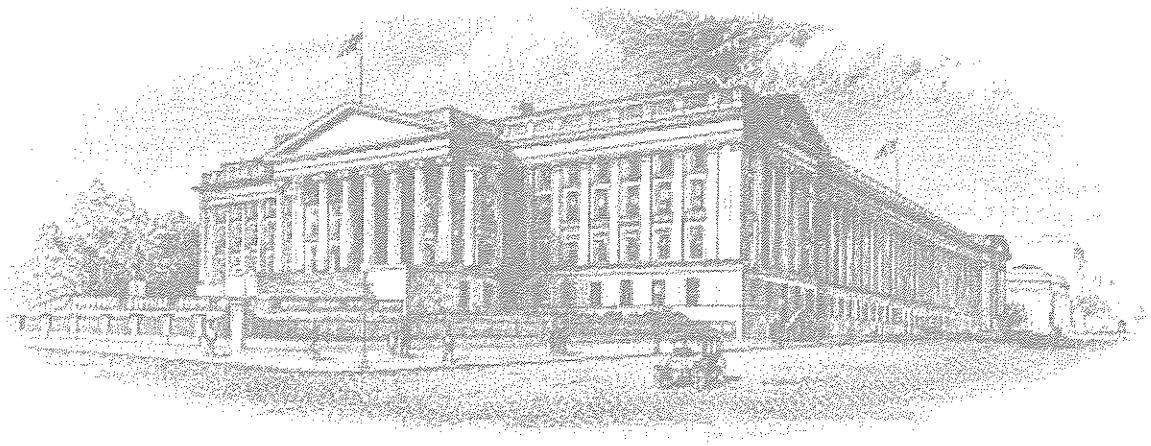
Evaluation Report



OIG-CA-07-001

INFORMATION TECHNOLOGY: Additional Actions Needed for System Inventory

October 2, 2006

Office of Inspector General

DEPARTMENT OF THE TREASURY

Contents

Contents

Abbreviations

GAO	Government Accountability Office
FISMA	Federal Information Security Management Act of 2002
IT	Information Technology
NSS	National Security Systems
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
Treasury	Department of the Treasury
TSI	Treasury System Inventory

Ira L. Hobbs
Chief Information Officer

We recently completed the evaluations for the year ended June 30, 2006, of Treasury's information security program and practices as required by the Federal Information Security Management Act of 2002 (FISMA). In addition to the three reports issued pertaining to these efforts,[1] we are issuing this report to address several matters relating to the FISMA inventory. These matters came to our attention during the course of our FISMA evaluations. We performed our work from June through September 2006. A detailed description of our objective, scope, and methodology is provided in appendix 1.

Results in Brief

We determined that despite notable progress, Treasury's information system inventory still needs improvement. Our evaluations disclosed the following matters:

(1) Several system categorization discrepancies existed between Treasury and bureau inventories.
(2) Numerous systems lacked required categorizations.
(3) One discrepancy existed between summary and component system categorizations.

[1] During 2006, we issued the following FISMA-related reports: *INFORMATION TECHNOLOGY: 2006 Evaluation of Treasury's FISMA Implementation for Its Intelligence Program* (OIG-CA-06-004, dated August 1, 2006), *INFORMATION TECHNOLOGY: Fiscal Year 2006 Evaluation of Treasury's FISMA Implementation for Its Non-Intelligence National Security Systems* (OIG-06-005, dated September 26, 2006), and *INFORMATION TECHNOLOGY: 2006 Evaluation of Treasury's FISMA Implementation* (OIG-CA-06-008, dated September 29, 2006).

(4) The Office of the Chief Information Officer's (OCIO) inventory review process needs improvement.

We recommend that the Chief Information Officer (CIO):

(1) Ensure that the OCIO reviews the system inventory periodically and in a timely manner. Such reviews should include identification, communication, and proposed resolution of discrepancies or missing information.
(2) Ensure the OCIO compliance reviews of bureau system security include procedures to address the completeness and consistency of the system inventory, as well as the proper security categorization of information systems.
(3) Ensure that OCIO reviews are properly documented to maintain an adequate audit trail.

We provided our findings and recommendations to management prior to the issuance of this report. Management generally concurred with all findings and recommendations.

Background

FISMA requires that Treasury report on its information security program and practices and maintain an inventory of major systems. In addition, FISMA requires that the OIG perform an independent evaluation of Treasury's information security program and practices.

The Office of Management and Budget (OMB) and the National Institute for Science and Technology (NIST) require that Treasury use NIST's Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize each Treasury system into one of three impact levels: high, moderate, or low. To determine a system's security categorization, FIPS 199 requires assigning an impact level to each system for each of three objectives: confidentiality, integrity, and availability. The overall categorization of a system is determined using the "high water"

mark (i.e., the highest impact level assigned to any of the three objectives.)

In 2005, we reported the following:[2]

- In 2004, the Treasury CIO's system inventory was inaccurate and incomplete. In addition, we found the OCIO had not assessed the consistency of the methodologies used by certain bureaus to re-categorize their inventories, nor had it assessed the impact of the inventory changes on the remainder of Treasury.
- Treasury was not fully in compliance with OMB's current requirement to include all systems in the FISMA report and to categorize these systems by FIPS 199 impact levels. In particular, we noted that the bureaus had inconsistent treatments for non-major applications. In many cases, non-major applications were not reported, or reported as part of a general support system or a major application.

Likewise, in 2004 we reported that Treasury's system inventory was not accurate, complete, or consistently reported. There have been major variances in the number of systems reported year-to-year, without adequate reconciliation. The number of systems reported in FISMA changed from 708 in FY 2003 to 237 in FY 2004. The change was largely due to IRS, which recategorized its systems in 2004.[3]

Using NIST guidance, Treasury issued two memorandums (dated September 12, 2005 and December 6, 2005) defining the Treasury system inventory (TSI). These memorandums defined general support systems, major applications, minor applications, major systems, "parent" systems, and "children" systems. In addition, these two memorandums together defined the TSI to include major general support systems, major applications, minor applications

[2] *INFORMATION TECHNOLOGY: Evaluation of Treasury's FISMA Implementation for Fiscal Year 2005* (Report No. OIG-CA-06-001, dated October 7, 2005)

[3] INFORMATION TECHNOLOGY: Evaluation of Treasury's FISMA Implementation for Fiscal year 2004 (Report No. OIG-CA-05-001, dated October 5, 2004)

that are not covered in a "parent" system, and minor applications that are "children" of another system.

Appendix 2 summarizes the fluctuations that have occurred in the Treasury system inventory since 2002.

Notable Improvements

For the year ending June 30, 2006, we noted the following improvements in the TSI:

(1) On September 12, 2005, the CIO issued the first of two memorandums defining the TSI and providing instructions to bureaus on what information to collect to develop the TSI. In this memo, the CIO also requested information on the identification of national security systems (NSS). Prior to issuance of this memorandum, the OCIO sought input from all Treasury bureaus and the OIG.
(2) On December 6, 2005, the CIO issued the second memorandum pertaining to the TSI. This memorandum expanded the inventory to include the identification of certain minor applications.
(3) During 2006, the OCIO met with several bureaus and the Office of Inspector General (OIG) to discuss the development of the current TSI, the responses obtained to the two TSI memorandums, and certain issues that had surfaced during the process.
(4) During 2006, the OCIO improved the inventory of intelligence program systems. This inventory is now complete.
(5) During 2006 and as a result of the improved inventory process, OCIO discovered and established an inventory of non-intelligence NSS.

Findings and Recommendations

Finding 1 — Several System Categorization Discrepancies Existed Between Treasury and Bureau Inventories

We noted several instances where FIPS 199 categories in the TSI did not agree with documentation maintained by the bureaus. For example:

- Two Departmental Offices (DO) systems were categorized as "high" in the TSI, but were categorized as "moderate" on DO's respective security plans.
- One DO system was categorized as "moderate" in the TSI, but should have been categorized as "low" based on DO's respective documentation that assigned a "low" impact level to all three FIPS 199 objectives.
- One DO system was categorized as "moderate" in the TSI, but based on DO's documentation should have been categorized as "high" due to the integrity objective.
- Seven Office of the Comptroller of the Currency (OCC) systems were categorized as "moderate" in the TSI, but were categorized as "high" in OCC's corresponding self assessments.
- One OCC system was categorized as "low" on the TSI but should have been categorized as "high" based on OCC's respective documentation that assigned a "high" impact level to the integrity objective.

OMB requires that agencies use FIPS 199 to categorize or assign impact levels to their inventories. If FIPS 199 is not properly followed, improper security categorizations may be assigned. Improper security categorizations may result in too few or too many security controls, inability to direct attention to more critical systems, and non-compliance with FISMA.

Finding 2 Numerous Systems Lacked Required Categorizations

We identified numerous instances where systems were not assigned a required FIPS 199 category (i.e., impact level). For example:

- OCC had 135 systems that were not assigned a FIPS 199 category by OCC or by OCIO.
- The Treasury Inspector General for Tax Administration (TIGTA) had four systems that did not have a FIPS 199 category assigned a FIPS 199 category by TIGTA or by OCIO.
- The Bureau of Engraving and Printing (BEP) had 61 systems that were not assigned a FIPS 199 category by BEP or OCIO.

OMB requires that agencies use FIPS 199 to categorize or assign impact levels to their inventories. If FIPS 199 is not properly followed, improper security categorizations may be assigned. Improper security categorizations may result in too few or too many security controls, inability to direct attention to more critical systems, and non-compliance with FISMA.

Finding 3 One Discrepancy Existed Between Summary and Component System Categorizations

We found one instance at the OCC where a discrepancy existed in OCC's internal documentation. Specifically, one system was assigned an overall "moderate" impact level. However, the system had a "high" impact level assigned to its integrity objective (one of the three components of the overall categorization). Based on FIPS 199's high water mark approach, the overall impact category should have been "high" due to the integrity objective.

FIPS 199 requires the use of the high water mark approach when assigning an overall security categorization. This approach requires assigning an impact level (high, moderate or low) to three components (i.e., the confidentiality, integrity and availability objectives). Once the three impact levels are assigned, the overall

security category should equal the highest impact level assigned to any of the three components. Improper assignment of the overall security categorization may result in the application of too few or too many security controls, inability to properly direct attention to more critical systems, and non-compliance with FISMA.

Finding 4 OCIO's Inventory Review Process Needs Improvement

We found that the OCIO inventory review process needed improvement. Specifically, we observed the following deficiencies:

- OCIO did not sufficiently or adequately review the inventories prepared by the bureaus. OCIO hired a contractor to perform this function; however, the procurement of this contract was not completed in a timely manner. The contract was awarded with an effective date of July 24, 2006, after the conclusion of the 2006 FISMA reporting period.
- Although the OCIO compiled the inventory as received from the bureaus, there was no evidence that an OCIO supervisor reviewed the compilation of the inventory.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states that internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. In addition, 44 U.S.C. 3505(c) requires the head of each agency develop and maintain an inventory of major information systems. FISMA and 44 U.S.C. 3506 further delegate this function and related responsibilities to the CIO. Without a properly developed, maintained or reviewed system inventory, the risks increases that the information security program and practices will be deficient.

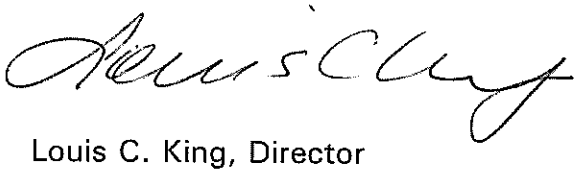
Recommendations

We recommend that the Chief Information Officer do the following:

(1) Ensure that the OCIO reviews the system inventory periodically and in a timely manner. Such reviews should include identification, communication, and proposed resolution of discrepancies or missing information.
(2) Ensure the OCIO compliance reviews of bureau system security include procedures to address the completeness and consistency of the system inventory, as well as the proper security categorization of information systems in accordance with FIPS 199.
(3) Ensure that OCIO reviews and those by its contractor are documented to maintain an adequate audit trail.

* * * * * *

I would like to extend my appreciation to the OCIO for the cooperation and courtesies extended to my staff during the evaluation. If you have any questions, please contact me, at (202) 927-5774, or Tram J. Dang, IT Project Manager, Office of Information Technology Audits, at (202) 927-5171. Major contributors to this report are listed in appendix 4.



Louis C. King, Director
Office of Information Technology Audits

Our primary objective was to evaluate Treasury's information security program and practices, as required by FISMA. To accomplish this objective, we divided the universe of information systems into three subsets:

- Intelligence Program Related NSS
- Other NSS
- Non-NSS

We performed the two evaluations pertaining to NSS[4]. We hired a contractor to perform the evaluation for non-NSS[5]. We reviewed the findings and recommendations developed by the contractor. As part of our work, we noted issues pertaining to the system inventory. However, our objective was not to perform a comprehensive review of the system inventory. Accordingly, we are not expressing a positive assurance opinion on the system inventory.

Our work covered the FISMA reporting period established by Treasury (i.e., the year ending June 30, 2006). We performed our work from June to September 2006 in Washington, D.C. We conducted our work in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

[4] These evaluations were included in the OIG's *Annual Plan Fiscal Year 2006* (page 30).
[5] This evaluation was included in the OIG's *Annual Plan Fiscal Year 2006* (page 29).

Figure 1 and Table 1 summarize the fluctuations in Treasury's system inventory since 2002.

Figure 1--Systems Reported for FISMA

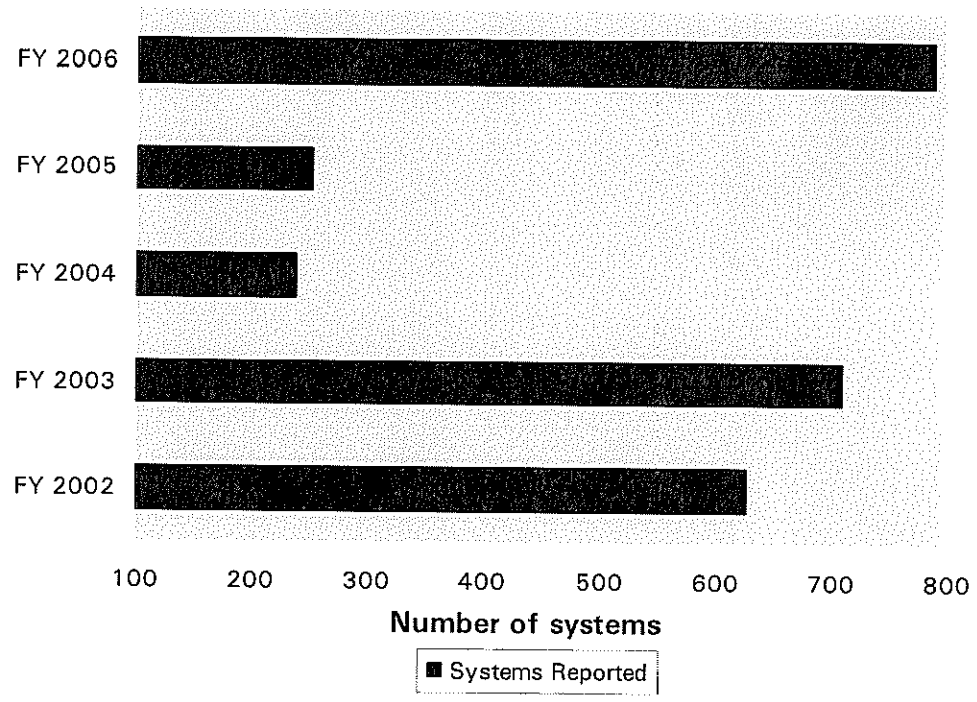


Table 1—Systems Reported For FISMA

	REPORTED	% CHANGE
FY 2002	626	--
FY 2003	708	13%
FY 2004	237	-67%
FY 2005	251	6%
FY 2006	787	213 %

Office of Information Technology Audits

Louis C. King, Director
Gerald Steere, IT Specialist

Department of the Treasury

Assistant Secretary for Management/Chief Financial Officer
Chief Information Officer
Chief Information Security Officer
Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management

OMB

Office of Inspector General Budget Examiner