Description of document:	Department of the Treasury Office of the Inspector General (OIG) Reducing Over-Classification Act evaluation report, 2013
Request date:	07-October-2013
Released date:	18-October-2013
Posted date:	01-September-2014
Source of document:	FOIA Request Department of the Treasury Washington, DC 20220 Fax: 202-622-3895 FOIA Online Request Form

From: "Delmar, Richard K."
Date: Oct 18, 2013 1:17:54 PM
Subject: FOIA request - Treasury OIG - Reducing Over-Classification Act evaluation report

Per your 10/7/13 FOIA request (received today), here is the report you requested.

I view this as fully responsive to your request. Please advise if you believe it is not fully responsive.

Rich Delmar
Counsel to the Inspector General
Department of the Treasury

Evaluation Report

OIG-13-055

GENERAL MANAGEMENT: Treasury Has Policies and Procedures to Safeguard Classified Information But Implementation Needs to Be Improved

September 27, 2013

Office of
Inspector General

DEPARTMENT OF THE TREASURY

Contents

Abbreviations

ISOO	Information Security Oversight Office
OFAC	Office of Foreign Assets Control
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
OSP	Office of Security Programs
SF	Standard Form

This Page Intentionally Left Blank.

September 27, 2013

S. Leslie Ireland
Assistant Secretary for Intelligence and Analysis

This report provides the results of our first evaluation, pursuant to Public Law 111-258, *Reducing Over-Classification Act*, of the Department of the Treasury's (Treasury) classification program. The act requires the Inspectors General of each department or agency of the United States with an officer or employee who is authorized to make original classification[1] decisions to evaluate the agency's classification program and identify practices that may contribute to the persistent misclassification[2] of material. Our first evaluation under this requirement is to be completed by September 30, 2013. A second evaluation is to be completed by September 30, 2016.

In accordance with the act, the evaluation objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within Treasury; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material. In performing our work, we used applicable portions of an evaluation guide that was prepared by a working group of participating Offices of Inspector General (OIG) on behalf of the Council of the Inspectors General on Integrity and Efficiency.[3] We performed our fieldwork from March 2013 to August 2013. Appendix 1 contains

[1] Original classification is the determination by an authorized official that information within specifically designated categories requires protection against unauthorized disclosure in the interest of national security. Individuals authorized to make this original determination have original classification authority and are authorized in writing, either by the President, the Vice President, agency heads, or other officials designated by the President. Treasury has 13 officials with original classification authority.

[2] **Auditor Note**: In the context of this report, misclassification is the act of incorrectly classifying, either over- or under-classifying, information.

[3] Department of Defense OIG, *A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the Reducing Over-Classification Act* (Jan. 22, 2013).

a more detailed description of our evaluation objectives, scope, and methodology.

In brief, we concluded that Treasury has policies and procedures in place to safeguard classified materials,[4] but the implementation of these policies and procedures needs improvement. Heightened attention should be given to (1) marking classified emails; [5] (2) completing the annual Standard Form (SF) 311, *Agency Security Classification Management Program Data*;[6] and (3) complying with self-inspection requirements.[7] We are making three recommendations to improve the classification management process.

In a written response, the Assistant Secretary for Intelligence and Analysis provided corrective actions taken and planned to implement the above recommendations. The management response is summarized in the Recommendations section of the report and the text of the response is included as appendix 2. We believe the corrective actions, taken and planned, are responsive to our recommendations.

Background

In December 2009, the President signed Executive Order 13526, *Classified National Security Information,* which updated classification principles, policies, and procedures and prescribed a

[4] The *Treasury Security Manual*, *General Information, Treasury-wide Security Programs*, describes the process of safeguarding classified materials as identifying, marking, handling, processing, storing, transmitting, accounting, tracking, and destroying.
[5] Marking is the act of properly labeling sections of classified documents, whether paper copies or electronic, to indicate (1) the overall level of classification, (2) the paragraph/portion classification, (3) the name or personal identifier of the classifier, (4) the reason or source of the classification, and (5) the date or event for declassification.
[6] The SF311 is used to collect data from Executive branch agencies that create and/or handle classified national security information. Information to be reported includes the number of (1) individuals designated with original classification authority, (2) original and derivative classification decisions, (3) mandatory declassification review requests and appeals, (4) pages of decisions declassified, (5) internal oversight activities including self-inspections conducted, and (6) classification guides created and used. Classification decisions refer to any recorded information, including documents and e-mails.
[7] Self-inspections are internal reviews and evaluations conducted by agency management for activities related to classified information. For the Treasury classification management program, the Office of Security Programs conducts self-inspections of Treasury's Departmental Offices. Bureau personnel are responsible for conducting self-inspections of the bureaus' classification management programs.

uniform system for classifying, safeguarding, and declassifying[8] national security information. The executive order requires heads of agencies that have employees with original classification authority or who handle classified information to designate a senior agency official who is responsible for the classification management process. Within Treasury, the designated senior agency official is the Deputy Assistant Secretary for Security.[9] The Deputy Assistant Secretary has oversight of the Office of Security Programs (OSP), which is located within Treasury's Office of Intelligence and Analysis (OIA).[10]

OSP is responsible for establishing Treasury policies and procedures for classification management based on Executive Order 13526 and other federal sources. The June 2011 update to the *Treasury Security Manual*[11] defines and implements the Department's classification management policies. OSP is also responsible for (1) developing security training programs, (2) monitoring compliance by Treasury's Departmental Offices and bureaus with federal and Treasury requirements for classified information, (3) reporting on Treasury's information security programs to the Information Security Oversight Office (ISOO),[12] and (4) representing Treasury interests on interagency forums.

Public Law 111-258, *Reducing Over-Classification Act*, which became law on October 7, 2010, was intended to address issues highlighted by the *9/11 Commission Report.* This report concluded that over-classification and inadequate information sharing contributed to the government's failure to prevent the attacks of 9/11. The report also stated that security requirements nurtured over-classification and excessive compartmentalization of information among agencies.

[8] Declassification is the authorized change in the status of information from classified to unclassified based on the duration of the national security sensitivity of the information.
[9] Treasury Order 105-19, *Delegation of Original Classification Authority; Requirements for Downgrading and Declassification* (June 27, 2011)
[10] OIA was established within Treasury by Public Law 108-177, *Intelligence Authorization Act for Fiscal Year 2004* (Dec. 13, 2003). The office, which is headed by the Assistant Secretary for Intelligence and Analysis, is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of Treasury.
[11] Treasury Directive Publication 15-71 (June 17, 2011)
[12] ISOO is an office within the National Archives and Records Administration responsible for policy and oversight of the Government-wide security classification system.

Findings

Finding 1 Classified Emails Were Often Improperly Marked

According to the *Treasury Security Manual*, classifiers must ensure that the application of required markings on electronic documents include (1) subject line and paragraph/portion markings, (2) the overall classification on the top and bottom of each page, and (3) the completion of the classification authority block.[13]

In the first half of fiscal year 2013, OSP personnel conducted two self-inspections that included 330 derivatively classified emails and attachments generated by 38 OIA employees. As shown in Table 1, OSP found that 4 percent of reviewed classified emails had all of the required markings and were considered properly marked. However, OSP noted that 31 percent of the emails did not contain portion markings[14] and 63 percent of the emails were categorized as "did not appear to be classified." OSP personnel told us that this category included classified email strings with unclassified information that did not have portion markings to indicate that unclassified information was discussed. The OSP reviews also disclosed that 2 percent of the documents had markings that were not easily categorized into the other 3 descriptions.

Table 1. Results of OSP's Self-Inspections of Derivatively Classified Emails and Attachments

	Number of Documents (Percent)				
Date of Self-Inspection Report	Reviewed	Properly Marked	Lacked Required Portion Markings	Included Information that Did Not Appear to Be Classified	Included Other Errors
11/01/2012	121	10 (8%)	40 (33%)	64 (53%)	7 (6%)
04/05/2013	209	4 (2%)	62 (30%)	143 (68%)	0 (0%)
Total	330	14 (4%)	102 (31%)	207 (63%)	7 (2%)

Source: OIG's summary of OSP's self-inspection reports

[13] The classification authority block consists of (1) a "Classified By" line to identify who prepared the document, (2) the "Reason for" or "Derived from" classification line, and (3) a "Declassify On" line that indicates the length of the classification.

[14] The *Treasury Security Manual*, Chapter 3, Section 6, requires portion markings on a subject line, paragraph, or portion of all classified documents, whether paper or electronic, to indicate whether they are classified and the specific level of classification.

OSP personnel told us that the incomplete markings found during the self-inspections may have resulted from employees (1) not taking the time to properly mark the emails, (2) not believing that the markings were important, or (3) unintentionally "replying to" or "forwarding" an email without realizing that such actions were classification decisions. To address these issues, OSP developed a handout to remind employees that classification markings must appear on all emails.

Treasury is responsible for ensuring that classified information is properly safeguarded. The lack of proper classification markings makes it difficult for the recipient of an email to determine the proper classification level for the information in that email.

Finding 2 Treasury's SF311 Reporting to the Information Security Oversight Office Was Incomplete and Inaccurate

ISOO uses data collected on the SF311 from Executive branch agencies that handle and generate classified national security information to report statistics in its annual report to the President. For fiscal years 2011 and 2012, OSP did not provide ISOO with a complete and accurate count of Treasury's overall derivative and original classification decisions on the SF311.

For fiscal year 2011, OSP reported 12,733 derivative classification decisions to ISOO. However, when we performed a mathematical check of the internally submitted data by Treasury's Departmental Offices and bureaus to OSP,[15] we found that the total was much smaller, only 6,123 decisions. For fiscal year 2012, Treasury reported 20,179 derivative classification decisions to ISOO, but we recalculated the internally submitted reports to OSP and found that the total was 20,076 decisions. In addition to these differences, we found that the Treasury totals reported to ISOO for these fiscal years also did not include derivative classification decision counts for the Office of Foreign Assets Control (OFAC), a Treasury office that regularly handles classified information.

[15] Treasury's Departmental Offices and bureaus are required to provide their SF311 to OSP by November 1st of each year for inclusion in Treasury's consolidated SF311 report to ISOO. The consolidated SF311 report is to be submitted to ISOO by November 15th.

When we asked about the differences between the number of reported derivative classification decisions to ISOO and those internally submitted by Treasury's Departmental Offices and bureaus, OSP personnel could not provide an explanation as to why there were discrepancies. With respect to the omission of OFAC's derivative classification decisions, OSP personnel told us that multiple requests were made to OFAC, but the data was not submitted. During an interview, an OFAC employee told us that he thought OFAC had filed a report for fiscal year 2011 because he recalled completing the document count. However, when we asked for a copy of the submission to OSP, neither OFAC nor OSP had a copy. For fiscal year 2012, OFAC personnel told us that the OSP request was overlooked. OFAC subsequently reported to OSP, in May 2013, after we made the inquiry, that it made 7,358 derivative classification decisions during fiscal year 2012.

In addition to reporting incomplete derivative classification decision counts in the fiscal year 2012 SF311 to ISOO, Treasury reported four original classification decisions. But when we reviewed these reports and supporting documentation with Treasury's Departmental Offices and bureaus that reported the information, we found that there were no original classification decisions for the fiscal year. In fact, the two original classification decisions were actually made in fiscal year 2013, not fiscal year 2012; and the other two original classification decisions were misreported. Neither were original classification decisions; they were both derivative classification decisions and should have been reported as such. An OSP representative told us that he questioned three of the four decisions that were reported, but was assured by the reporting bureau that the information was correct. OSP accepted the other reported original decision as reasonably reported by the bureau.

Finding 3 Treasury's Self-Inspection Program Needs Improvement

Prescribed by the *Treasury Security Manual*, the annual self-inspection process is a key control within Treasury to ensure the protection of classified information. The manual delegates the methodology for conducting these self-inspections to officials

within Departmental Offices and bureaus.[16] These officials are required to:

- Document their findings and recommendations for improvement or enhancement.
- Indicate that all reviewed records, documents, briefings, and activities complied with Executive Order 13526 and applicable implementing directives.
- Identify noted discrepancies and indicate whether corrective action will be or have been taken.
- Conduct and document follow-up actions taken where individual self-inspections have identified such a particular need.
- Provide copies of corrective actions to address noted discrepancies to the Director, OSP, as necessary.
- Conduct at least one self-inspection annually that includes document reviews if the office generates classified information.

Overall, OSP is responsible for managing Treasury's classified program and is required by the *Treasury Security Manual* to monitor Treasury's compliance with federal and Treasury mandates for classified information.

For fiscal years 2011 and 2012, we found that one Treasury bureau that generated classified information properly completed the required self-inspections while four others either did not complete the self-inspections or completed the inspections but did not retain documentation. OSP performed and documented self-inspections for those offices within Treasury's Departmental Offices that generated classified information, but the scope of those inspections only included emails and attachments. OSP did not review classified documents generated outside of the electronic environment and this report is based on a review of OSP's findings.

OSP personnel told us they assume that bureaus are properly performing self-inspections because the bureaus should know their

[16] The *Treasury Security Manual* provides examples of procedures that could be taken to conduct a self-inspection. Examples include, but not limited to, (1) reviewing relevant security directives, guidelines, and instructions for currency and applicability; (2) reviewing access and control records and procedures; (3) sampling actual and electronically processed original and derivative classified documents; and (4) evaluating employee training, and if needed, modifying the training.

responsibilities. OSP personnel also told us that they get involved only when they become aware that a bureau is not following procedures. We believe a more proactive approach by OSP is necessary to ensure that OSP and bureaus are performing and documenting self-inspections in accordance with the *Treasury Security Manual*.

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis direct the Deputy Assistant Secretary for Security to:

1. Remind employees who work with classified information about the requirement in the *Treasury Security Manual* to properly mark classified emails and provide initial training on marking requirements when an employee is first given access to Treasury classified email systems and periodic refresher training thereafter.

   Management Comments

   Training on properly marking classified information is routinely provided to employees both initially when receiving their security clearance and annually through refresher training about required markings. OSP strives to develop comprehensive and tailored training and will work more closely with Treasury's Departmental Offices when developing training modules and ensure that training is accessible in some form to all bureau personnel. The referenced training serves to remind employees authorized access to classified information of their obligations to properly mark and safeguard that information. OSP will review Treasury Directive Publication 15-71 with respect to marking electronic media to determine whether it should allow for the same flexibility authorized by ISOO in their implementing regulation.[17]

[17] **Auditor Note:** 32 CFR Part 2001, *Classified National Security Information*, states that classified national security information in the electronic environment shall be marked with proper classification markings to the extent that such marking is practical including portion marking, overall classification, and the classification authority block.

OIG Comment

Management's action, taken and planned, meets the intent of our recommendation. Management will need to record an estimated date for completing its planned actions in the Joint Audit Management Enterprise System (JAMES), Treasury's audit recommendation tracking system.

2. Implement controls to ensure that an accurate and complete Treasury consolidated SF311 is submitted to ISOO. OSP should review Treasury's Departmental Offices' and bureaus' internally reported information on classification decisions and other classification information for reasonableness. OSP should also ensure that those offices expected to have classification information submit the required information for the consolidated SF311.

   Management Comments

   OSP requests clarification when Departmental Offices and bureaus submit questionable SF311 information. One office, for their fiscal year 2013 reporting, agreed to use a 2-week sampling to extrapolate their classification volume. Assuming meaningful results come from the 2-week sampling, OSP will suggest it for the largest Treasury components that generate classified information starting with the fiscal year 2014 report, as well as provide appropriate training to their employees on the sampling requirement and methodology.

   OIG Comment

   Management's action, taken and planned, meets the intent of our recommendation. Management will need to record an estimated date for completing its planned actions in JAMES.

3. Implement controls to ensure that Treasury bureaus with employees who handle and generate classified information conduct annual self-inspections in accordance with the *Treasury Security Manual*, document the results, and submit reports to the Director of OSP. In this regard, the scope of inspections

performed by OSP should include reviews of both emails and documents created outside the electronic environment.

Management Comments

OSP performs self-inspections in Departmental Offices each quarter. These include both physical and information security aspects. In fiscal year 2014, OSP will start cross-training within OSP to have an additional person fully trained in the information security discipline. OSP will require copies of self-inspection reports when they are reported by bureaus, and include this requirement in Treasury Directive Publication 15-71. In addition, OSP is taking steps to increase its personnel resources in the information security discipline to ensure oversight of bureau self-inspection and reporting requirements. OSP will also consider revising the directive to clarify the responsibilities of those components with few or no classified holdings, where internal access procedures equate to performing daily self-inspections and to have them self-inspect on other aspects of their individual information security program.

OIG Comment

Management's action, taken and planned, meets the intent of our recommendation. Treasury will need to record an estimated date for completing its planned actions in JAMES.

* * * * * *

We appreciate the courtesies and cooperation extended by your staff as we inquired about these matters. Major contributors to this report are listed in appendix 3. A distribution list for this report is provided as appendix 4. If you wish to discuss this report, you may contact me at (202) 927-5400 or Kieu Rubb, Audit Director, at (202) 927-5904.

/s/
Marla A. Freedman
Assistant Inspector General for Audit

Public Law 111-258, *Reducing Over-Classification Act,* Section 6(b), requires the Inspector General of each department or agency with an officer or employee who is authorized to make original classifications to (1) assess whether applicable classification policies, procedures, rules, regulations have been adopted, followed, and effectively administered; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material. The act called for two evaluations, this first to be completed by September 30, 2013, and the second evaluation to be completed by September 30, 2016.

The focus of this evaluation was the Department of the Treasury's (Treasury) policies and procedures related to classification training, self-inspections, and the completion of the Standard Form (SF) 311, *Agency Security Classification Management Program Data*.

We conducted fieldwork in Washington, DC, at the Office of Terrorism and Financial Intelligence, [18] the Office of General Counsel, the Office of International Affairs, the Office of Management, the Office of Inspector General, the Bureau of Engraving and Printing, the U.S. Mint, and the Bureau of the Fiscal Service.[19] We also conducted fieldwork in Vienna, Virginia at the Financial Crimes Enforcement Network. Our evaluation did not include the Internal Revenue Service.[20] Our evaluation scope covered the period from October 2010 to May 2013. We conducted our fieldwork from March 2013 through August 2013.

To accomplish our objectives we

- reviewed federal and Treasury rules, regulations, policies, and procedures, including:

[18] Treasury's Departmental Offices and bureaus reporting to the Office of Terrorism and Financial Intelligence include the Financial Crimes Enforcement Network, the Office of Terrorist Financing and Financial Crimes, the Office of Intelligence and Analysis, and the Office of Foreign Assets Control.
[19] Our evaluation focused on the legacy Bureau of the Public Debt which in October 2012 was consolidated with the legacy Financial Management Service and redesignated as the Bureau of the Fiscal Service.
[20] The Internal Revenue Service, under the jurisdictional oversight of the Treasury Inspector General for Tax Administration, does not have an individual designated with an original classification authority. Furthermore, our review of the Treasury SF311 process disclosed that the Internal Revenue Service reported zero derivative classification decisions for fiscal years 2011 and 2012.

  - Executive Order 13526, *Classified National Security Information* (Dec. 29, 2009)
  - 32 CFR Part 2001, *Classified National Security Information* (June 28, 2010)
  - Public Law 111-258, *Reducing Over-Classification Act* (Oct. 7, 2010)
  - *Treasury Security Manual*, Treasury Directive Publication 15-71 (June 17, 2011)
  - Treasury Order 105-19, *Delegation of Original Classification Authority; Requirements for Downgrading and Declassification* (June 27, 2011).

- interviewed the Deputy Assistant Secretary of Security and Office of Security Programs (OSP) employees who are responsible for directing and guiding the protection of personnel, information, facilities, and assets; and promoting security awareness within Treasury.
- interviewed personnel at the various bureaus who are responsible for security and training.
- reviewed training materials posted on Treasury's internal websites and paper copies of training documents and obtained the 2011 and 2012 training records of Treasury officials with original classification authority.
- reviewed OSP's quarterly self-inspection reports on Treasury's Departmental Offices from January 2011 through March 2013 and the Financial Crimes Enforcement Network's self-inspection reports from fiscal years 2011 and 2012.
- reviewed Treasury's SF311 for fiscal years 2011 and 2012 prepared by OSP, and related data on original classification decisions and derivative classification decisions provided to OSP by Treasury's Departmental Offices and bureaus. We interviewed Treasury personnel with responsibilities for completing the SF311.

As directed by the act, we coordinated our evaluation with other Offices of Inspector General with the intent of ensuring that our evaluations followed a consistent methodology to allow for cross-agency comparisons. In performing our work, we used applicable portions of an evaluation guide that was prepared by the working

group of participating Offices of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency.

We conducted this evaluation in accordance with Quality Standards for Inspections and Evaluations issued by the Council of the Inspectors General on Integrity and Efficiency.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

September 24, 2013

MEMORANDUM FOR: MARLA A. FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: S. LESLIE IRELAND
ASSISTANT SECRETARY FOR INTELLIGENCE AND ANALYSIS

SUBJECT: Treasury Response to Draft Office of the Inspector General (OIG) Report Required by Public Law 111-58, Reducing Over-Classification Act

Below are the Treasury Department comments to OIG's three recommendations in the above subject report. The Office of Security Programs (OSP) oversees the Department's classification management program and thus responds to the OIG recommendations below.

OIG Recommendations - We recommend that the Assistant Secretary for Intelligence and Analysis direct OSP to:

1. **Remind employees about the requirement to properly mark classified emails and provide initial training on marking requirements when an employee is first given access to Treasury classified email systems and periodic refresher training thereafter.**

   Training on properly marking classified information is routinely provided to employees, both initially when receiving their security clearance for access to classified information as well as remind employees annually in refresher training (in hard copy and electronic formats) about required markings. OSP strives to develop comprehensive and tailored training for our varied DO/bureau clients and to post DO training on the OSP. We will work more closely with DO TLMS officials when developing training modules and ensure that training is accessible in some form to all bureau personnel. All the above referenced training serves to remind employees authorized access to classified information of their obligations to properly mark and safeguard that information. OSP will review TD P 15-71 policy with respect to marking electronic media to determine whether it should allow for the same flexibility authorized by the Information Security Oversight Office in their implementing regulation.

2. **Implement controls to ensure that an accurate and complete Treasury consolidated SF 311 is submitted to ISOO. OSP should review Treasury components' internally reported information on classification decisions and other classification information for reasonableness. OSP should also ensure that components expected to have classification information submit the required SF 311 information for the consolidated SF 311.**

Where reported information in DO/bureau SF311 submissions has appeared to be questionable, OSP has requested clarification as we noted for this report (Finding 2) above. With one DO office in particular (for their FY 2013 report) we have their agreement to use a 2-week sampling to extrapolate their classification volume. Assuming meaningful results come from the 2-week sampling we will suggest it for the largest Treasury components that generate classified information starting with the FY 2014 report i.e., Office of Terrorism and Financial Intelligence, Office of Intelligence and Analysis, Office of International Affairs and FinCEN and provide appropriate training to their employees on the sampling requirement and methodology.

3. **Implement controls to ensure Treasury components that handle and generate classified information conduct annual self inspections in accordance with the Treasury Security Manual, document the results, and submit reports to the Director of OSP. In this regard, the scope of inspections performed by OSP should include reviews of both emails and documents created outside the electronic environment.**

   OSP performs self-inspections in DO each quarter. These include both physical and information security aspects. The former consist of examination of offices (and use of approved IT equipment) for handling, processing, storing, locking, and preparation of classified information for actual on-site destruction. The information security aspect of document reviews (markings) is one-person deep yet in FY 2014 we will start cross-training within OSP to have an additional FTE fully trained in the information security discipline – to be more prepared to review of actual documents regardless of environment and in keeping with the existing quarterly schedule.

   OSP will now require copies of self-inspection reports when they are reported by bureaus on the SF311 as having been accomplished and include this requirement in TD P 15-71. In addition, OSP is taking steps to increase its personnel resources in the information security discipline to ensure oversight of bureau self-inspection and reporting requirements. OSP will consider revising TD P 15-71's to clarify the responsibilities of those components with few or no classified holdings, where internal access procedures equate to performing daily self-inspections and to have them self-inspect on other aspects of their individual information security program.

Kieu T. Rubb, Audit Director
Gregory J. Sullivan Jr., Audit Manager
Regina A. Morrison, Auditor-in-Charge
Brigit A. Hoover, Auditor
Alex M. Taubinger, Referencer

Department of the Treasury

Secretary of the Treasury
Deputy Secretary
Under Secretary for Terrorism and
Financial Intelligence
Deputy Assistant Secretary for Security
Director, Office of Security Programs

Information Security Oversight Office

Director

Office of Management and Budget

OIG Budget Examiner

United States Senate

Chairman and Ranking Member
Committee on Homeland Security and Government Affairs

Chairman and Vice Chairman
Select Committee on Intelligence

Chairman and Ranking Member
Committee on Finance

Chairwoman and Vice Chairman
Committee on Appropriations

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations

U.S. House of Representatives

Chairman and Ranking Member
Committee on Homeland Security

Chairman and Ranking Member
Permanent Select Committee on Intelligence

Chairman and Ranking Member
Committee on Oversight and Government Reform

Chairman and Ranking Member
Committee on Financial Services

Chairman and Ranking Member
Committee on Appropriations

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations