Audit Report

OIG-15-040

OSP Needs to Promptly Inform OIG of Potential Illegal Activity and Improve Other Processes

July 27, 2015

Office of Inspector General

Department of the Treasury

Contents

Abbreviations

ABIS	Automated Background Investigation System
CATS	Case Adjudication Tracking System
CVS	Central Verification System
DoD	Department of Defense
e-QIP	Electronic Questionnaires for Investigations Processing
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive 12
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IRS	Internal Revenue Service
OCIO	Office of the Chief Information Officer
OIG	Treasury Office of Inspector General
OPM	Office of Personnel Management
OPM-FIS	Office of Personnel Management, Federal Investigative Services
OSP	Office of Security Programs
PSS	Personnel Security System
ROI	Report of Investigation
SF	Standard Form
SOPs	standard operating procedures
TD P	Treasury Directive Publication

July 27, 2015

S. Leslie Ireland
Assistant Secretary for Intelligence and Analysis

This report provides the results of our audit of the security clearance process performed by the Department of the Treasury's (Treasury) Office of Security Programs (OSP). This audit was included in the *Office of Inspector General Fiscal Year 2013 Annual Plan*. Additionally, our office had noted differences in the Office of Inspector General (OIG) employee security clearance information maintained in OSP's Personnel Security System (PSS) database and Office of Personnel Management's (OPM) Central Verification System (CVS).[1]

Federal regulations require employees and contractors to receive a favorable eligibility determination before holding sensitive positions or accessing classified information. Organizationally located within Treasury's Departmental Offices, OSP directs personnel security as part of the Office of Intelligence and Analysis.[2] OSP has the authority to determine employee eligibility to receive security clearances and consequently, OSP may grant, deny, and revoke security clearances and suspend access to classified information of

[1] Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 (Dec. 17, 2004), required the OPM Director to establish, operate, and maintain an integrated, secure database where data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel would be entered from all authorized investigative and adjudicative agencies. However, the Performance Accountability Council established by Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008), elected to leverage OPM's existing system, CVS, to enable access to records on investigations and adjudications.

[2] The Office of Intelligence and Analysis was established by Public Law 108-177, Intelligence Authorization Act for Fiscal Year 2004 (Dec. 13, 2003), and is headed by the Assistant Secretary for Intelligence and Analysis who is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of Treasury.

Departmental Offices personnel, Treasury bureau personnel, and presidential appointees. OSP also interprets security policy and procedures and provides written security guidance to the Departmental Offices and bureaus.

Our audit objectives were to determine whether OSP (1) implemented an effective program to ensure that the activities to grant employees and contractors access to classified information were conducted in a timely and appropriate manner and (2) ensured security-related documents were accurate and secured. To address these objectives, we reviewed activities related to initial background investigations and periodic reinvestigations,[3] the adjudication process,[4] reporting requirements to OIG and OPM, and the granting of physical access to Treasury facilities. We did not include in our testing OSP actions and documents related to personnel of the Internal Revenue Service (IRS), OIG, the Special Inspector General for the Troubled Asset Relief Program, or the Treasury Inspector General for Tax Administration.

During our audit, we learned of two incidents where OPM Reports of Investigation (ROI) in OSP personnel security files contained information that revealed illegal activity on the part the subjects of investigations. W**e** therefore expanded our audit to determine the circumstances surrounding these two incidents and issued a separate, classified memorandum to management.[5] We conducted our fieldwork from November 2012 to June 2015. Appendix 1 contains a more detailed description of our audit objectives, scope, and methodology.

[3] Periodic reinvestigations are required when employees need continued access to classified information. Reinvestigations are conducted every 5 years for access to information classified at the top secret level, every 10 years for information classified at the secret level, and every 15 years for access to information classified at the confidential level.

[4] The adjudication process examines a sufficient period of a person's life, including the results of the OPM background investigation, to determine whether the person is eligible to (1) serve in a designated public trust position or (2) have access to classified information.

[5] OIG-CA-15-022; issued July 27, 2015.

Results in Brief

We found that OSP did not (1) promptly report to OIG as required by Treasury Directive 40-01,[6] two incidents that involved illegal activities on the part of the subjects which were disclosed in OPM's ROIs; (2) provide Treasury employees' security clearance information in OPM's CVS; (3) timely initiate periodic reinvestigations; (4) communicate well with its clients; and (5) always follow its standard operating procedures (SOPs) for the security clearance process. With respect to the adjudication process, our review of a sample of 45 new background investigations processed in fiscal year 2012 showed that OSP adjudicated these investigations in an average of 11 days, well within the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) requirement.[7] We also found that the Treasury employees' personnel security files maintained at the OSP office were accurate, physically secured, and contained all the documentation required by the Treasury Security Manual.

In this report, we are recommending that the Assistant Secretary for Intelligence and Analysis (1) direct OSP to notify OIG immediately when the office becomes aware that any employee, former employee, contractor, subcontractor, or potential contractor that may have engaged in improper or illegal activities; (2) conduct, in conjunction with the Treasury Office of the Chief Information Officer (OCIO), a resource analysis of OSP to determine the proper information technology support needed to comply with CVS requirements; (3) ensure that OSP works with OCIO and OPM, as appropriate, to resolve OSP system and data issues with CVS so that Treasury employee security clearance data in CVS is accurate; (4) ensure that periodic reinvestigations continue to be initiated within required timeframes; (5) instruct OSP to work with its client

[6] Treasury Directive 40-01, Responsibilities of and to the Inspector General (Sept. 16, 2011)

[7] IRTPA requires agencies authorized to grant national security information clearances to complete at least 90 percent of clearances within an average of 60 days. Agencies have 40 days to complete the background investigation and 20 days to adjudicate the clearance. Effective in fiscal year 2013, the number of days to complete the single scope background investigation increased to 80 days. The original 60-day requirement remains in effect for confidential/secret investigations. A single scope background investigation covers the past 7 years of a person's history and includes, among other things, verification of citizenship, date and place of birth, national agency records checks, and face-to-face interviews of the person subject to the investigation and selected references.

offices to identify ways to improve communications as to the status of security clearances and the need for assistance to facilitate the security clearance process; (6) improve the security clearance process guidance by streamlining the Treasury Security Manual and other related sources by, for example, including a roles and responsibilities matrix/cross-index of all the parties involved in the security clearance process; and (7) ensure that OSP develops and implements comprehensive SOPs for the security clearance process.

In a written response, the Assistant Secretary for Intelligence and Analysis provided the corrective actions taken and planned to in response to the recommendations in this report. The management response is summarized in the Findings and Recommendations section of the report and the text of the response is included as appendix 6. We believe the corrective actions are responsive to our recommendations.

Other Matters

On December 17, 2014, OIG provided drafts of this report and the above referenced separate, classified memorandum to management for comment. We recommended in the draft classified memorandum that OSP review its files and inquire of its staff to identify any information about illegal and/or improper activities by Treasury employees and contractor personnel and report to the Treasury OIG Office of Investigations on the results of its search and inquiries. Management initially responded to the draft classified memorandum on February 10, 2015, with a planned corrective action that we considered insufficient. After much discussion, management provided a supplemental response on July 23, 2015, with a planned corrective action that meets the intent of the recommendation.

In a letter dated, February 27, 2015, the Chairman of the Senate Committee on Homeland Security and the Chairman of the Senate Committee on the Judiciary requested our office provide certain information semiannually, to include: “A narrative description of all audits, evaluations, and investigations provided to the agency for comment but not responded to within 60 days.” In that the supplemental management response was received over 7 months

after we issued the draft classified memorandum for comment, we plan to include this audit in our next reply to the Chairmen. That reply is due in October 2015.

Background

Executive Order 12968 established a uniform Federal personnel security program for employees who require access to classified information, detailed the investigative and adjudicative requirements for each level of access, and defined reciprocity procedures between Federal agencies.[8] Within Treasury, OSP is responsible for (1) setting Department-wide personnel security policies, which are published in the Treasury Security Manual;[9] (2) verifying the security clearance information for Treasury contractor employees, whose clearances are processed by the National Industrial Security Program (NISP);[10] and (3) implementing the security program throughout Treasury. In addition, OSP adjudicates background investigations for (1) most positions in the Departmental Offices, including all Departmental Offices presidential appointees requiring Senate confirmation; (2) some positions within the bureaus, including all bureau presidential appointees requiring Senate confirmation, other bureau heads, and their first deputies; (3) all personnel security officers and any official with delegated authority to grant security clearances;[11] and (4) personal services contractors.[12]

OSP must report its adjudicative decisions on security clearance investigations to OPM.[13] OPM provides investigative products and

[8] Executive Order 12968, Access to Classified Information (Aug. 4, 1995)

[9] Treasury Security Manual, Treasury Directive Publication (TD P) 15-71 (June 17, 2011)

[10] Executive Order 12829, National Industrial Security Program (Jan. 3, 1993), established the National Industrial Security Program to achieve cost savings and protect classified information held by contractors, licensees, and grantees of the U. S. Government. The Department of Defense's (DoD) Defense Security Service manages this program and is responsible for the contractor security clearance process.

[11] TD P 15-71, Chapter I, Section 2, Issuing Clearances and Granting Access to Classified Information (Jan. 3, 2012), gives the OSP Director authority to determine the eligibility for access to classified information for these positions.

[12] Personal services contractors are consultants or experts who contract directly with Departmental Offices and bureaus and are subject to the same requirements as Treasury employees for determining position sensitivity, risk designation, and investigative requirements.

[13] 5 CFR §732.302(b), Reporting to OPM (Apr. 23, 1991)

services for Federal agencies' determination of suitability and security clearances as required by executive orders and other rules and regulations. OPM uses CVS, an integrated, secure database, to collect and share data necessary for Federal agencies to make reciprocal determinations on existing security clearances,[14] background investigations, suitability, fitness, and Homeland Security Presidential Directive 12 (HSPD-12) secured identification credentialing.[15] In short, CVS provides real-time security clearance information to most Federal agencies.

Sensitivity Levels and Risk Designation

Before security clearances can be granted, employees must undergo investigations by OPM or an agency with delegated authority from OPM to conduct investigations. According to 5 CFR §731.106, all Federal government positions must be assigned a level of risk and a sensitivity designation that determines the type of investigation for the positions.[16] In general, a position designated with a higher risk or greater sensitivity requires a more comprehensive background investigation. Furthermore, the type of investigation required also depends on the level of access to classified national security information[17] needed by the employee.

Access to Classified Information

A security clearance is a determination that an individual is eligible to access a particular level of classified information. Actual access

[14] A reciprocal determination is the process of accepting the background investigations and eligibility determinations conducted by other government agencies unless the employee does not meet the standards of Executive Order 12968.

[15] Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 27, 2004), established a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors.

[16] According to 5 CFR §731.106, Designation of public trust positions and investigative requirements, the position level of risk can be high, moderate, or low and can have a sensitivity designation of special, critical, or non-critical.

[17] Executive Order 13526, Classified National Security Information (Dec. 29, 2009), defines national security information as any knowledge of U. S. defense or foreign relations that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by produced by or for, or is under the control of the U. S. Government.

to levels of classified information is only granted on a "need-to-know"[18] basis. Executive Order 13526 categorizes classified information in three levels: top secret, secret, and confidential. Individuals in positions that require access to a particular level of classified information are only granted access after a successful investigation and adjudication. Individuals who do not require access to classified information but who may be involved in policymaking, major program responsibility, or other sensitive roles are typically considered to be in public trust positions and are generally identified at the high or moderate risk levels.[19] See appendix 4 for a list of the standard form types required for specific position designations and the related background investigation.

The Security Clearance Process

The first phase of the security clearance process is initiation—the applicant completes an application, by providing general and historical information and required documentation, in OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system. The remaining two phases are the actual investigation and the subsequent adjudication. In fiscal year 2012, at the government-wide level, IRTPA required agencies authorized to grant national security information clearances to complete at least 90 percent of the clearances within an average of 60 days. Agencies had 40 days to complete the background investigation and 20 days to adjudicate the clearance.[20]

Treasury uses OPM to conduct employee background investigations and reinvestigations. OPM is responsible for the timeliness of the investigative phase. In fiscal year 2012, OSP adjudicated 254 background investigations for persons employed by Departmental Offices. We used a non-statistical sampling methodology and randomly selected and reviewed 90

[18] A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information to perform or assist in a lawful and authorized governmental function.

[19] 5 CFR §731.106(b)

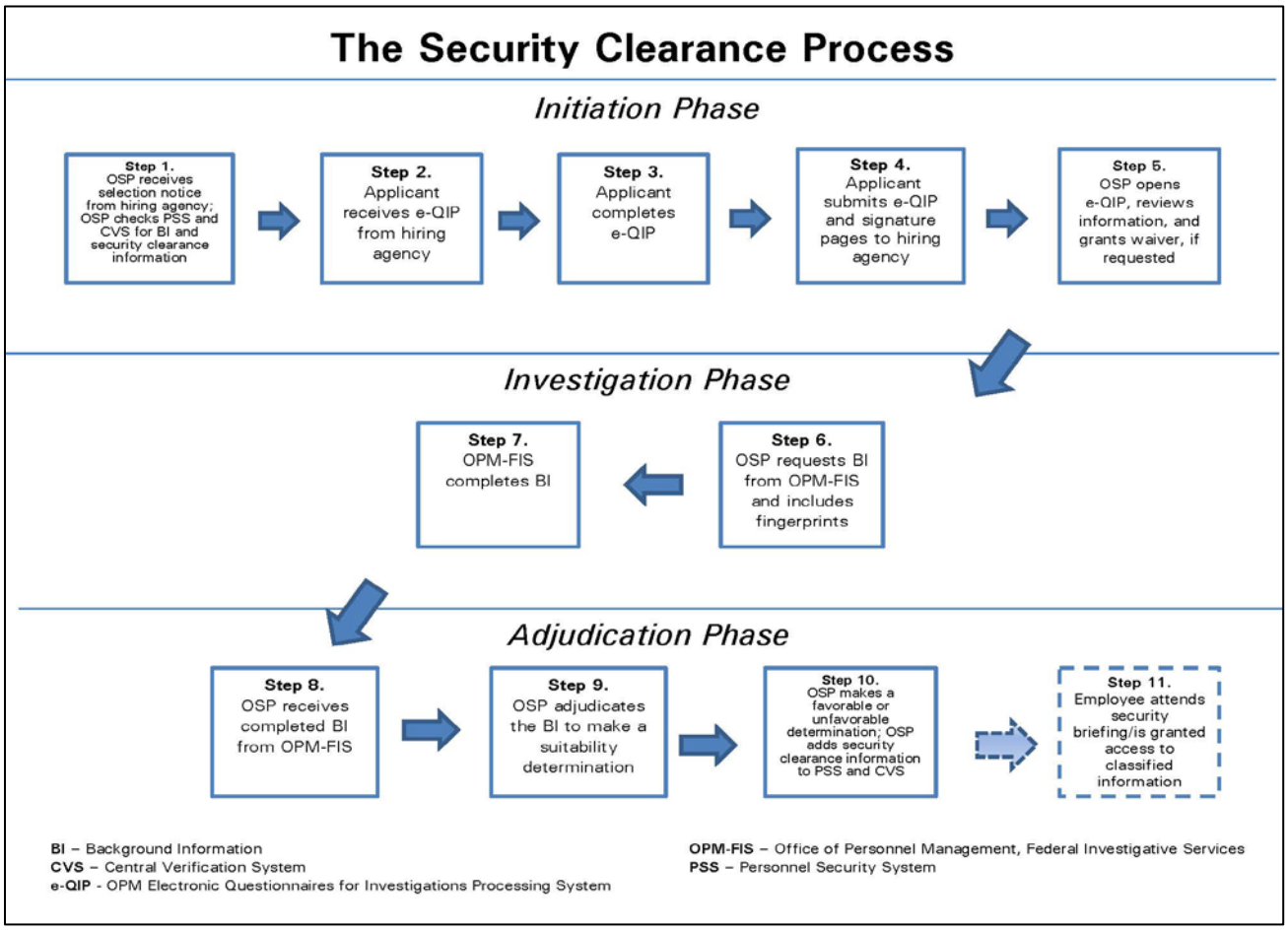
[20] Effective in fiscal year 2013, the number of days to complete the single scope background investigation increased to 80 days. The original 60-day requirement remained in effect for confidential/secret investigations.

adjudications. Of those, 45 were for new background investigations, 24 were for periodic reinvestigations, and 21 were for reciprocity determinations. Of the sampled items, we found that OPM completed 90 percent of the Treasury employee background investigations and reinvestigations in an average of 62 days, which exceeded the IRTPA 40-day requirement. After OSP received the completed background investigation files from OPM, OSP adjudicated 90 percent of the background investigations and reinvestigations in an average of 11 days, well within the 20-day requirement.[21]

Figure 1 provides an overview of the specific steps of the security clearance process. A more detailed description of each step is included as appendix 2.

[21] IRTPA, Title III, Security Clearances, Sec. 3001(g), Reduction in the Length of Security Clearance Process

Figure 1: Security Clearance Process



Source: Federal and Treasury security clearance documentation

Personnel Security Files

According to the Treasury Security Manual, personnel security files shall contain the following documentation:[22]

- The type of investigation completed.
- The investigative agency that conducted the investigation, investigative date, and investigative results.
- Results of the security and suitability adjudications/ determinations.
- Security clearance decisions.

[22] TD P 15-71, Chapter I, Section 4, Personnel Security Operations (Jan. 3, 2012)

- Any significant personnel security or suitability information developed during employment.

OSP is responsible for retaining the Departmental Offices and bureaus personnel security files for the duration of an individual's employment with Treasury in accordance with Treasury Directive 80-05, Records and Information Management Program,[23] and National Archives and Records Administration requirements.[24] The Treasury Security Manual also requires that personnel security files and related documents be properly destroyed or transferred to a Federal Records Center[25] upon notification of an employee's death or after employment separation or transfer from Treasury.[26]

Findings and Recommendations

Finding 1 OSP Did Not Promptly Report Required Activity to OIG

During fiscal year 2013, OSP did not promptly report to OIG two incidents that involved illegal activities on the part of the subjects, which were disclosed in OPM's ROIs. Treasury Directive 40-01 requires Treasury officials, officers, and employees to promptly report to OIG any information or allegation that a Treasury employee, former employee, contractor, subcontractor, or potential contractor, may have engaged in improper or illegal activities, including but not limited to:

- a criminal or other illegal act;
- a violation of the Standards of Conduct or other Federal regulation;
- a prohibited personnel practice or violation of merit system principles; and

[23] Treasury Directive 80-05, Records and Information Management Program (June 26, 2002). This directive also authorized the issuance of TD P 80-05, Records and Information Management (RIM) Manual, which included additional policy guidance for specific categories of records.

[24] National Archives and Records Administration, General Records Schedule 18, Items 21 – 24, Security and Protective Services Records, Personnel Security Clearance Records (Apr. 2010)

[25] The National Archives and Records Administration manages the Federal Records Centers Program, which ensures the protection and access of U.S. records for their scheduled life.

[26] TD P 15-71, Chapter I, Section 4, Personnel Security Operations (Jan. 3, 2012)

- any act which creates a specific danger to the public health and safety.

In addition to Treasury Directive 40-01, a Treasury General Counsel memorandum provided clarification on reporting allegations of misconduct to OIG.[27]

For these two incidents, OSP became aware of the illegal activities after the investigation phase. However, OSP did not report these incidents to OIG until as late as 3 months later.

As previously noted, we issued a separate, classified memorandum to management on these two incidents. [28]

Neither individual involved had a security clearance.

Recommendation

We recommend that the Assistant Secretary for Intelligence and Analysis direct OSP to notify OIG immediately when the office becomes aware of any employee, former employee, contractor, subcontractor, or potential contractor that may have engaged in improper or illegal activities.

Management Response

OSP management provided the OSP workforce with a copy of Treasury Directive 40-01 and reminded them of their obligations. OSP is working with OIG, its counsel, and the Office of General Counsel to clarify the notification requirements of Treasury Directive 40-01 as applied to the range of information to which OSP has access as a result of its role in the security clearance process.

[27] General Counsel Memorandum for All Departmental Offices and Bureau Heads*, Reporting Allegations of Misconduct to the Inspector General* (Sept. 25, 2009). The memorandum is provided as part of appendix 3.

[28] OIG-CA-15-022; issued July 27, 2015.

OIG Comment

Management's corrective actions meet the intent of our recommendation.

Finding 2 Security Clearance Information Was Not Provided to OPM's Central Verification System

IRTPA required OPM to establish, operate, and maintain an integrated, secure database into which granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.[29] OPM leveraged CVS to maintain Federal employees' security clearance information.[30]

According to OPM Federal Investigations Notice No. 10-04, agencies are required to do the following in CVS:

- Submit daily updates to security clearance information to report any changes, such as adding new clearances, noting revocations, denials, suspensions, and those clearances, which were administratively withdrawn.
- Fully refresh, or update, CVS clearance data at least monthly.

OSP did not maintain accurate security clearance information in CVS. We obtained CVS print-screens for the 90 adjudications selected for review. Based on these CVS print-screens, we determined that the security clearance information was current for only 12 Treasury employees. The security clearance data for the remaining 78 adjudications (87 percent) was shown as "unknown" or OSP staff could not access the data in CVS.

[29] IRTPA, Sec. 3001(e)(1), Security Clearances, Database on Security Clearances

[30] According to OPM, Federal Investigations Notice No. 10-04, Enhancements to the Central Verification System (CVS) for Reciprocity (Mar. 18, 2010), OPM initially called the database the Clearance Verification System but later changed the name to the Central Verification System because it better represented the scope of information contained in the system (e.g., reciprocity of security clearances, suitability and fitness determinations).

OPM-Federal Investigative Services (OPM-FIS) Agency Oversight[31] staff provided us with data on the Departmental Offices and bureaus employee security clearances maintained in CVS. As of March 8, 2014, according to the CVS data, there were no active Departmental Offices and bureaus employee security clearances in CVS. CVS had a total of 1,449 Departmental Offices and bureaus employee security clearance records; however, of these, 1,254 records were shown as "unknown" and 195 records were inactive.

OSP management told us about two issues the office had encountered with using CVS. First, OSP's PSS database was not compatible with CVS;[32] consequently, OSP staff would have had to manually enter data into CVS. Second, OSP could not access a CVS error report to correct the OSP data in CVS. OSP management told us they had communicated these CVS issues to OPM.

At the start of our audit, the OSP Director in place at the time[33] told us that OSP planned to replace PSS with another database, the Automated Background Investigation System (ABIS). OSP hired a contractor to install ABIS in 2012. The ABIS contractor was paid about $454,000 as of May 2014.[34] With ABIS, OSP expected to resolve most, if not all of its CVS issues.

In March 2014, the then OSP Director[35] told us that she elected to abandon ABIS. She decided, instead, to implement the DoD's Case Adjudication Tracking System (CATS) by the end of fiscal year

[31] OPM-FIS Agency Oversight conducts program reviews of Federal agencies' Personnel Suitability and Security Programs, including the evaluation of the Federal agencies' use of CVS and compliance with the OPM issuances. OPM-FIS Agency Oversight started its review of OSP in June 2013 and suspended the review until October 2013 at the former OSP Director's request because, among other things, OSP resources were needed to support our audit. OPM-FIS Agency Oversight completed its program review at OSP in January 2014 and issued its final report in March 2015.

[32] OPM-FIS Agency Oversight staff told us that only the DoD Joint Personnel Adjudication System interfaces with CVS. Non-DoD agencies must submit revalidation files to CVS through a flat file format by manually uploading the flat file to OPM through the OPM portal, or directly through the agencies' case management system.

[33] This OSP Director retired from Federal service in July 2013.

[34] According to the former OSP Director, IRS used ABIS for the past 10 years. OSP hired Data Source, Inc., IRS's ABIS contractor, to install ABIS.

[35] This OSP Director's tenure at Treasury was July 2013 to May 2014.

2014. This OSP Director told us that CATS was cheaper than ABIS and required fewer information technology staff.

Current OSP management has decided to work with the OCIO to resolve the PSS compatibility issues with CVS. OSP also hired a consultant to analyze ABIS and CATS to determine which database to implement.

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis:

1. Conduct, in conjunction with OCIO, a resource analysis of OSP to determine the proper information technology software, equipment, and support needed to comply with CVS requirements.

   Management Response

   On November 7, 2014, the OSP Director in conjunction with OCIO finalized a support agreement with the Defense Logistics Agency to implement CATS, upon completion of a resource analysis of required technology. This agreement formalized the participation in, and use of Defense Information System for Security (DISS) by OSP and sets forth the responsibilities of the parties associated with OSP's receipt and use of Personal Security Investigation electronic reports from OPM by OSP DISS. Computers and monitors have also been ordered through OCIO to support CATS implementation. These initiatives should allow OSP to comply with CVS requirements. OSP will continue to collaborate with OCIO on technology, software, equipment and support to ensure CVS compliance. OSP anticipates CATS will be implemented by the end of fiscal year 2015.

   OIG Comment

   Management's corrective actions meet the intent of our recommendation.

2. Ensure that OSP works with OCIO and OPM, as appropriate, to resolve OSP system and data issues with CVS so that Treasury employee security clearance data is provided to and maintained

in CVS on a complete, current, and accurate basis going forward.

Management Response

The implementation of CATS should resolve interoperability issues within CVS. As a result of the audit, OSP identified CATS as the enterprise tool to address the requirement to maintain clearance data in a complete, current, and accurate basis going forward. OSP anticipates CATS will be implemented by the end of fiscal year 2015.

OIG Comment

Management's corrective action meets the intent of our recommendation.

Finding 3 Periodic Reinvestigations Were Not Always Initiated Timely

IRTPA requires each Federal agency to perform periodic reinvestigations on existing security clearance holders to verify that they should still have access to classified information. IRTPA established reinvestigation requirements as follows: (a) every 5 years for continued access to information classified at the top secret level or access to a highly sensitive program, (b) every 10 years for continued access to information classified at the secret level, and (c) every 15 years for continued access to information classified at the confidential level.[36]

As discussed in the Background section of this report, in fiscal year 2012, OSP adjudicated 254 background investigations for Departmental Offices. Of those, we randomly selected and reviewed 90 adjudications. Of the sampled items, 45 were for new background investigations, 24 were for periodic reinvestigations, and 21 were for reciprocity determinations.

We found that OSP did not initiate 14 of the 24 periodic reinvestigations (58 percent) within the required timeframe. The 14

[36] IRTPA, Title III, Security Clearances, Sec. 3001(a)(7), Definitions

late periodic reinvestigations included 13 top secret clearances, of which 3 were initiated over a year after they first became due. The other late periodic reinvestigation was for a secret clearance; it was also initiated over a year after it first became due.

OSP personnel told us that resource and budget shortages contributed to periodic reinvestigation delays; and that they had been trying to bring the periodic reinvestigation process into compliance with IRTPA. To help reduce these delays, OSP obtained temporary resources to initiate and adjudicate the periodic reinvestigations. At the exit conference for this audit, OSP management stated that periodic reinvestigations were current. We did not validate that information.

Recommendation

We recommend that the Assistant Secretary for Intelligence and Analysis ensure that periodic reinvestigations continue to be initiated within required timeframes.

Management Response

OSP recently implemented a new policy process to ensure reinvestigations are initiated within required timeframes. Under this process, OSP will prioritize the initiation of periodic reinvestigations based on the direction issued in a September 26, 2014, memorandum from the Director of National Intelligence.

OIG Comment

Management's corrective action meets the intent of our recommendation.

Finding 4 OSP Communications with Clients Could Be Improved

According to Government Accountability Office (GAO) standards for internal control, for an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal, as well as, external events. Information is needed throughout the agency to achieve all of its objectives. Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In additional to

internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals.[37]

We sent a survey to 17 offices within Departmental Offices to gauge OSP's working relationships with its clients. Our survey instrument is included as appendix 5. Eleven (11) of the 17 offices responded, stating they were generally satisfied with OSP's services. Since our survey response rate was only 65 percent (11 of 17 offices), we interviewed personnel within two (2) offices that together accounted for 85 percent of the fiscal year 2012 security clearance requests.

The interviewees told us that OSP could improve communications. For example, they suggested that OSP provide defined process timelines with milestone updates. They also suggested that their offices be included on OSP's administrative communications with the applicant. The interviewees understood that they could not be involved in the adjudication process; however, they believed they could expedite the security clearance process by assisting OSP with administrative matters such as ensuring applicants complete the e-QIP application and attend security briefings in a timely manner.

The interviewees also expressed concerns about their roles and responsibilities in the security clearance process. For example, they told us that there was no clear policy for people to report significant life events (e.g., marriage to a foreign national). The Treasury Security Manual does address employee information changes, including marriage or cohabitation reporting requirements, but the interviewees stated that staff is not familiar with the guidance because information is contained in multiple sources (e.g., Federal regulations, executive orders, Treasury Security Manual, and Treasury directives) rather than in a single guide. In this regard, we noted that the 400-plus page Treasury Security Manual, excluding appendices, did not clearly set out the roles and responsibilities for all parties involved in the security clearance process.

[37] GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Nov. 1999)

Recommendations

We recommend that the Assistant Secretary for Intelligence and Analysis:

1. Take into consideration the results of our survey and interviews and instruct OSP to work with its client offices to identify ways to improve communications as to the status of security clearances and the need for assistance to facilitate the security clearance process.

   Management Response

   OSP will collaborate with client offices to identify Personnel Security Liaisons to facilitate communication between OSP and the client office. OSP will meet with Personnel Security Liaisons and identify ways to improve communications and facilitate real time status inquiries. This collaboration is ongoing, and we will meet with all affected offices by the end of calendar year 2015.

   OIG Comment

   Management's corrective actions meet the intent of our recommendation.

2. Improve the security clearance process guidance by streamlining the Treasury Security Manual and other related sources by, for example, including a roles and responsibilities matrix/cross-index of all the parties involved in the security clearance process.

   Management Response

   The Treasury Security Manual is under review to include updating of written guidance and instructions for compliance with applicable laws, regulations and OPM issuances. As part of the review, OSP will consider areas to streamline, elaborate, explain, and provide illustrative guidance on the processes. OSP anticipates completing this review by end of calendar year 2015.

OIG Comment

Management's corrective action meets the intent of our recommendation.

Finding 5 Standard Operating Procedures for the Security Clearance Process Were Incomplete and Not Always Followed

According to GAO standards for internal control, control activities occur at all levels and functions of the entity and are an integral part of an entity's planning, implementing, reviewing and accountability for stewardship of government resources and achieving effective results. Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

OSP did not have comprehensive SOPs for the security clearance process. Documented procedures did not exist for (1) access and oversight of the personnel security files, (2) communications with clients and OPM, (3) tracking periodic reinvestigations, and (4) management of electronic records.

The Treasury Security Manual details the security clearance processes for new, transferring, and current employees. OSP also provided its critical-sensitive and non-critical sensitive processes to us.[38] When we compared the documented processes to security clearance practice, we found inconsistencies. For example, OSP's written procedures stated that after an employee is favorably adjudicated, the employee is invited to attend a security briefing as soon as the employee begins work. In practice, security briefings were not conducted when the employee began work because access to classified information was not always required at that time. Security briefings are conducted on a "need-to-know" basis. OSP management stated that the security briefings were

[38] OSP, Process for Cases Types Handled by Treasury DO Office of Security Programs

conducted when necessary but acknowledged that the procedures did not always represent its processes.

According to OSP management, OSP had limited staffing and the documentation and maintenance of the SOPs was not a priority. However, we believe that it is important for OSP to develop and maintain SOPs to reduce the risk for inaccuracies and increase accountability for the security clearance process. In addition, without written policies and procedures, the loss of key personnel could result in lapses and errors in required procedures for processing security clearances.

Recommendation

We recommend that the Assistant Secretary for Intelligence and Analysis ensure that OSP develops and implements comprehensive SOPs for the security clearance process.

Management Response

OSP is reviewing its written guidance and instructions for compliance with applicable laws, regulations and OPM issuances. OSP recently hired a Policy and Personnel Security Specialist who is charged with completing SOPs detailing the security clearance process and procedures including the four areas described above for Treasury security specialists. OSP anticipates completing the SOPs by end of calendar year 2015.

OIG Comment

Management's corrective action meets the intent of our recommendation.

******

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 7. A distribution list for this report is included as appendix 8. If you wish to discuss this report, you may contact me at (202) 927-5400 or Kieu T. Rubb, Audit Director, at (202) 927-5904.

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

Our audit objectives were to determine whether the Department of the Treasury's (Treasury) Office of Security Programs (OSP) (1) implemented an effective program to ensure that the activities to grant employees and contractors access to classified information were conducted in a timely and appropriate manner and (2) ensured security-related documents were accurate and secured. This audit was included in the *Office of Inspector General Fiscal Year 2013 Annual Plan*. Our office had also noted that the Office of Inspector General (OIG) employee security clearance information was not accurate or complete in OSP's Personnel Security System (PSS) database and Office of Personnel Management's (OPM) Central Verification System (CVS). We last reviewed OSP's operations in fiscal year 2002.[39]

During our audit, we learned of two incidents where OPM Reports of Investigation (ROI) in OSP personnel security files contained information that revealed illegal activity on the part of the subjects of investigations. We therefore expanded our audit to determine the circumstances surrounding these two incidents. We also expanded our work into 2015 because OSP delayed providing us information that it had in its possession for six months.

To accomplish these objectives, we conducted fieldwork from November 2012 to June 2015 at Treasury offices in Washington, D.C. Our fieldwork consisted of these steps:

- We reviewed Federal and Treasury rules, regulations, policies and procedures, and internal controls including:

    - Intelligence Authorization Act for Fiscal Year 2004, Public Law 108-177 (Dec. 13, 2003)
    - Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 27, 2004)

[39] *General Management: Timeliness of Departmental Offices' Security Clearances Can Be Improved*, OIG-CA-02-006 (June 25, 2002), and *General Management: Investment in Information Technology May Speed Security Clearances*, OIG-CA-02-007 (June 25, 2002). In the reports, we stated that the Personnel Security Branch, the predecessor to OSP, needed to increase coordination with the Office of Personnel Resources and individual hiring offices to improve the timeliness of security clearances. Occasional delays in the security clearance process occurred due to applicants not understanding the security forms.

- Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458 (Dec. 17, 2004)
- 5 CFR §732.202(a)(2)(i), Waivers and exceptions to investigative requirements, Specific waiver requirements (Apr. 23, 1991)
- 5 CFR §732.302 (b), Reporting to OPM (Apr. 23, 1991).
- 5 CFR §731.106, Designation of public trust positions and investigative requirements (Apr. 15, 2008)
- Executive Order 10450, Security requirements for Government employment (Apr. 27, 1953)
- Executive Order 12829, National Industrial Security Program (Jan. 6, 1993)
- Executive Order 12968, Access to Classified Information (Aug. 2, 1995)
- Executive Order 13381, Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information (June 27, 2005)
- Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008)
- Executive Order 13526, Classified National Security Information (Dec. 29, 2009)
- Treasury Security Manual, Treasury Directive Publication TD P 15-71 (June 17, 2011)
- Treasury Directive 80-05, Records and Information Management Program (June 26, 2002)
- Treasury General Counsel Memorandum for All Departmental Offices and Bureau Heads, *Reporting Allegations of Misconduct to the Inspector General* (Sept. 25, 2009)
- Treasury Directive 40-01, Responsibilities of and to the Inspector General (Sept. 16, 2011)
- Office of Security Programs, Process for Cases Types Handled by Treasury DO Office of Security Programs
- Office of Management and Budget, Memorandum for Deputies of Executive Departments and Agencies, Reciprocal Recognition of Existing Personnel Security Clearances (Dec. 12, 2005)
- Office of Personnel Management, Federal Investigations Notice No. 10-04, Enhancements to the Central Verification System (CVS) for Reciprocity (Mar. 18, 2010)

  - Office of Personnel Management, Federal Investigative Services, Requesting OPM Personnel Investigations (Apr. 2012)
  - National Archives and Records Administration, General Records Schedule 18, Security and Protective Services Records (Apr. 2010)
  - Government Accountability Office, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Nov. 1999)

- We interviewed OSP management and staff involved with the security clearance process.

- We sent a survey to 17 offices within Treasury's Departmental Offices to gauge OSP's working relationships with its clients. Our survey instrument is included as appendix 5. Eleven (11) of the 17 offices responded to our survey. We also interviewed personnel within two (2) offices that together accounted for 85 percent of the fiscal year 2012 security clearance requests. The Departmental Offices staff we interviewed included a senior advisor to the undersecretary, a deputy director for business operations, a disclosure coordinator information analyst, a recruitment/contracting coordinator, and program analysts.

- We used a non-statistical sampling methodology and randomly selected and reviewed 90 of the 254 background investigations adjudicated by OSP in fiscal year 2012. We reviewed the related 90 personnel security files to determine OSP's (1) adherence to Federal and Treasury security documentation standards, (2) timeliness of background investigation and periodic reinvestigation adjudications, and (3) compliance with CVS requirements. Because of our sampling methodology, we did not project the results.

- We interviewed OPM-Federal Investigative Services program staff and oversight agency inspectors to gain insight into Federal agency CVS use and to obtain OSP's security clearance record history in CVS.

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.

The Department of the Treasury (Treasury) security clearance process has three phases: initiation, investigation, and adjudication. The steps below detail the procedures for the security clearance process. Step 1 through Step 10 summarizes the determination that an applicant is eligible to access a particular level of classified information. Step 11 describes the granting of a security clearance to an employee to have access to "need-to-know" classified information.

Initiation Phase

Step 1 - The Office of Security Programs (OSP) receives a selection notification from the hiring Treasury Departmental Office or bureau for a new applicant. OSP checks its Personnel Security System (PSS) database for an existing record for the applicant. If OSP does not have a record in PSS for the applicant, then OSP checks Office of Personnel Management's (OPM) Central Verification System (CVS) for a background investigation and security clearance information.

Step 2 - If the applicant does not have any record of a security clearance, the hiring Departmental Office or bureau emails a request to the applicant to register for access to the OPM Electronic Questionnaires for Investigations Processing (e-QIP) system. e-QIP is a secure web-based automated system that collects data from the applicant based on the appropriate investigative questionnaire. See appendix 4 for a list of the standard form (SF) types required for specific position designations and the related background investigation.

Step 3 - Within e-QIP, the applicant completes the appropriate investigative questionnaire based on the position's level of risk and sensitivity designation.

Step 4 - The applicant submits the e-QIP, including the required attachments to the hiring Departmental Office or bureau. In addition, the applicant signs the signature release forms and returns them to the hiring agency by fax, mail, or uploads them into e-QIP.

Step 5 - The OSP Director retrieves the e-QIP and reviews the information provided and the Request for Pre-Appointment Security Investigative Waiver, if requested.[40] The pre-appointment investigation requirement may not be waived for appointment to positions designated as special sensitive.[41]

Investigation Phase (40 Days)[42]

Step 6 - All initial investigations sent to OPM require electronic or paper fingerprint submissions.[43] OSP initiates the appropriate background investigation with OPM-Federal Investigative Services (OPM-FIS) and selects the applicable fingerprint submission type and method.

Step 7 - OPM-FIS uses the applicant's e-QIP information to conduct its background investigation. Investigations to support a secret level security clearance include automated and manual checks of criminal history, terrorist activities, credit history, and foreign activities and influence. When the checks identify issues of concern, additional checks, including interviews and other manual efforts are conducted, as needed. Top secret investigations add non-automated checks, including interviews of the applicant, employers, and social references, and collect information related to foreign influence and foreign preference.

---

[40] Executive Order 10450, Security requirements for Government employment (Apr. 27, 1953) provides that in case of emergency, a sensitive position may be filled for a limited period by a person with respect to whom a full field pre-appointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

[41] 5 CFR §732.202(a)(2)(i), Waivers and exceptions to investigative requirements, Specific waiver requirements (Apr. 23, 1991)

[42] Intelligence Reform and Terrorism Prevention Act of 2004 requires agencies authorized to grant national security information clearances to complete at least 90 percent of clearances within an average of 60 days. Agencies have 40 days to complete the background investigation and 20 days to adjudicate the clearance. Effective in fiscal year 2013, the number of days to complete the single scope background investigation increased to 80 days. The original 60-day requirement remains in effect for confidential/secret investigations.

[43] Fingerprints are electronically submitted to OPM's Fingerprint Transaction System by an FBI approved Live-Scan System or Fingerprint Card Scan System that uses OPM-approved software. Alternatively, OPM may also receive paper fingerprint submission on the SF 87, Fingerprint Chart for Federal and Military Positions.

Adjudication Phase (20 Days)

Step 8 - OSP receives the completed background investigation file by mail from OPM-FIS for adjudication.

Step 9 - An OSP personnel security specialist adjudicates the applicant's background investigation. The adjudication process examines a sufficient period of a person's life to determine whether the person is eligible for access to classified information or to serve in a public trust position. The process includes the careful weighing of a number of variables known as the "whole person concept." Available, reliable information about a person's past and present, favorable and unfavorable, are considered when making a suitability determination.

Step 10 - If the adjudication is favorable, the applicant is *eligible* for a security clearance. OSP staff manually adds the security clearance information to its PSS database, and notifies the applicant and the hiring Departmental Office or bureau by email. OSP reports its adjudicative decision on the OPM background investigation in CVS and by completing INV FORM 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations.

If the adjudication is not favorable, the OSP personnel security specialist forwards the background investigation file to the OSP Chief of Personnel Security Branch to initiate the denial process and give the applicant an opportunity to appeal the decision.

Step 11 - If the employee needs access to classified information, as determined by the hiring Departmental Office or bureau, OSP invites the employee to an OSP security briefing and then requests a signed SF 312, Classified Information Nondisclosure Agreement, from the employee. OSP then completes the Treasury Department Form 15-03.2, Certificate of Clearance and/or Security Determination, which includes the level of security clearance granted and whether it was granted on an interim or final basis.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

GENERAL COUNSEL

September 25, 2009

MEMORANDUM FOR ASSISTANT GENERAL COUNSELS, CHIEF COUNSELS AND LEGAL COUNSELS

FROM: George W. Madison
General Counsel

SUBJECT: Reporting Allegations of Misconduct to the Inspector General

Please read the attached memorandum from Inspector General Eric Thorson regarding our continuing obligation to report misconduct. The OIG has the statutory mandate to conduct independent and objective investigations into the Department's programs and operations. In addition, each of us has the duty to report to the IG all allegations of misconduct. The attached memorandum from me to all Departmental Offices and Bureau Heads further explains these important responsibilities.

I have invited Rich Delmar, Counsel to the IG, to attend our staff meeting on Friday, October 2, 2009 at 3:30 p.m. so that he can explain these responsibilities to us and answer any questions that you may have. Please make arrangements to attend this meeting.

Attachments
Memorandum for all Departmental Offices and Bureau Heads
Memorandum from IG

cc: Eric Thorson
Rich Delmar

ATTACHMENT 1

GENERAL COUNSEL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

September 25, 2009

MEMORANDUM FOR ALL DEPARTMENTAL OFFICES AND BUREAU HEADS

FROM: George W. Madison
General Counsel

SUBJECT: Reporting Allegations of Misconduct to the Inspector General

As you are aware, Treasury Directive 40-01 requires all Treasury employees to report any known or suspected act of misconduct to the Office of the Inspector General (OIG). I have received the attached memorandum from the Inspector General Eric Thorson clarifying the types of allegations and incidents that should be reported.

Circumstances that must be reported to OIG include, but are not limited to: all allegations of workers' compensation fraud, all instances of loss, theft, or compromise of personally identifiable, classified, or sensitive information or of government-owned or leased property, and all breaches of government-occupied office or other space. Further, all apparent instances of violation of the Hatch Act, the Treasury Employee Rules of Conduct and the Executive Branch Standards of Conduct must be reported.

Issues of the following types need not be reported to OIG and should be addressed by the appropriate manager:

- Leave issues such as tardiness, AWOL, etc. (However, time & attendance fraud must be reported to OIG);
- Performance and productivity related issues, such as disagreements as to how work assignments should be handled, assignment of work, insubordination, poor quality of work, etc;
- Appearance, personal hygiene and dress issues;
- Work atmosphere issues such as loud music, talking, or reading newspapers. However, fundraising or canvassing in the workplace (other than authorized Combined Federal Campaign events) should be reported;
- Minor personality conflicts (not involving assaults or harassment); and
- Minor traffic infractions. However, all arrests must be reported.

This is not an exclusive list of minor issues that need not be reported. However, to the extent doubt may exist, issues should be reported. OIG will make an evaluation and, if appropriate, refer the issue back to management for resolution.

All allegations are to be reported to the OIG Complaints Management Office, via email at OIGIntake@oig.treas.gov. The OIG Complaints Management Office will respond to each notification and provide a reply stating whether OIG will assume responsibility for the investigation or allegation or return it to the reporting bureau or office for resolution by management. Urgent after hours matters should be reported to the OIG Duty Agent, who is available through the following number: (202) 927-5260.

Many issues of the types discussed above involve potential Treasury liability in addition to misconduct within OIG's jurisdiction. Although seeking legal counsel does not substitute for, and should not be permitted to delay, reporting to the OIG, please do not hesitate to contact me or an Assistant General Counsel when such issues arise, or any time legal advice may be needed or appropriate.

Attachment
Memorandum from IG

cc: Eric Thorson
Rich Delmar

ATTACHMENT 2

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SEP 21 2009

MEMORANDUM FOR GEORGE W. MADISON
GENERAL COUNSEL

FROM: Eric M. Thorson
Inspector General

SUBJECT: Guidance for Reporting Allegations of Misconduct

As you and my Counsel, Rich Delmar discussed last week, the Office of Inspector General (OIG) seeks to re-state and clarify to all Treasury bureaus and offices its jurisdiction and their obligation to report incidents, problems, and apparent violations of law, rule, or regulation. You have agreed to forward this memo to all concerned officials, and to invite Mr. Delmar to brief Legal Division officials about it. I greatly appreciate your support.

The OIG is tasked by statute and Treasury Order to conduct independent and objective investigations into the Department's programs and operations, to detect fraud and abuse, promote economy and efficiency, and keep the Secretary and the Congress informed about problems and deficiencies. In keeping with this mandate, and in furtherance of transparency and accountability, the OIG must be fully informed of all events that potentially constitute violations of law, rules, or regulations. To accomplish this duty, the OIG must be informed of the full range of misconduct and inefficiency suspected in the Department and the various bureaus.

The OIG recognizes that most minor conduct violations should continue to be addressed by bureau/Departmental Office management and will be returned to bureaus and offices for resolution by management staff. However, the OIG also recognizes the need to become involved in certain violations as well as monitor emerging trends and patterns within the bureaus. To that end, a better balance in reporting needs to be established in order to promote the operations and efficiency of both the bureaus and the OIG.

The OIG requires bureaus and offices to refer all allegations of administrative misconduct with only minimum exceptions. This includes, but is not limited to, all allegations of workmen's compensation fraud, all instances of loss, theft or compromise of personally identifiable information (PII), classified or sensitive information, government-owned or leased property, and breaches of government-occupied offices or other space. In addition, all apparent instances of violation of the Hatch Act, the Treasury Employee Rules of Conduct and the Executive Branch Standards of Conduct must be reported, for OIG review and consideration.

The following types of issues need **not** be reported to the OIG and should be handled directly by your bureau/DO management:

- Leave issues such as tardiness, AWOL, etc., (However, time & attendance fraud must be reported to the OIG).
- Performance and productivity related issues, such as disagreements as to how work assignments should be handled, assignment of work, insubordination, poor quality of work, etc.
- Appearance, personal hygiene and dress issues.
- Workplace atmosphere issues such as loud music or talking, reading newspapers. However, fundraisers or canvassing in the workplace should be reported for assessment.
- Minor personality conflicts (not involving assaults or harassment).
- Minor traffic infractions however, **all arrests** must be reported.

This list is not all-inclusive and is provided as a guideline. Should there arise a question as to whether a particular issue is reportable, we recommend that it be reported to the OIG and allow us to evaluate it and, if appropriate, refer it back to management for resolution.

All allegations are to be reported to the OIG Complaints Management Office, via email at OIGIntake@oig.treas.gov. The OIG Complaints Management Office will respond to each notification and provide a reply whether the OIG will assume responsibility for the investigation of an allegation or return it to the reporting bureau or office for resolution by management. Urgent after hours matters should be reported to the OIG Duty Agent, who is available by calling the Office of Investigations main number, (202) 927-5260.

The OIG is committed to serving the needs of the Department and the performance of its statutory responsibilities efficiently. Any questions concerning this guidance can be addressed to Assistant Inspector General for Investigations (Acting) P. Brian Crane on (202) 927-0365, or to Mr. Delmar, on (202) 927-3973.

Thank you again for your cooperation and support.

The Office of Personnel Management (OPM) requires an applicant to submit an Electronic Questionnaires for Investigations Processing (e-QIP) application, using different forms, based on the position designation as shown below:

Form Type	Position Designation	Background Investigation Type
Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions	Non-Sensitive Position Low Risk and/or Homeland Security Presidential Directive 12 (HSPD-12) Credential (with no other designation)	National Agency Check and Inquiries (NACI)
SF 85P, Questionnaire for Public Trust Positions	Moderate Risk Public Trust Position (No national security sensitivity)	Moderate Risk Background Investigation (MBI)
	Reinvestigation for Moderate Risk Public Trust Position (No national security sensitivity)	National Agency Check with Law and Credit (NACLC)
	High Risk Public Trust Position (No national security sensitivity)	Background Investigation (BI)
	Reinvestigation for High Risk Public Trust Position (No national security sensitivity)	Periodic Reinvestigation (PRI)
SF 86, Questionnaire for National Security Positions	Secret/Confidential (Undesignated – e.g., Military/Contractor) or Reinvestigation for Noncritical Sensitive Position and/or Secret/Confidential Eligibility/Clearance	National Agency Check with Law and Credit (NACLC)
	Noncritical Sensitive Position and/or Secret/Confidential Security Eligibility/Clearance (Low Risk)	Access National Agency Check and Inquiries (ANACI)
	Noncritical Sensitive Position and/or Secret/Confidential Security Eligibility/Clearance (Moderate Risk)	Moderate Risk Background Investigation (MBI)
	Critical Sensitive Position and/or Top Secret (TS) Security Eligibility/Clearance (Any level of risk) or Special Sensitive Position and/or Top Secret with Sensitive Compartmented Information (SCI) (Any level of risk)	Single Scope Background Investigation (SSBI)
	High Risk Public Trust with any level of Position Sensitivity	Single Scope Background Investigation (SSBI)
	Reinvestigation for Critical Sensitive Position or Special Sensitive Position And/or Top Secret or Top Secret with SCI or High Risk Public Trust with any level of Position Sensitivity	SSBI Periodic Reinvestigation (SSBI-PR) or Phased Periodic Reinvestigation (PPR)

Source: OPM Federal Investigative Services, *Requesting OPM Personnel Investigations* (Apr. 2012)

We sent the following survey to the Department of the Treasury Departmental Offices to gauge Office of Security Programs' working relationships with its clients.

OSP Client Survey

Name: _____ **Position:** _____

Departmental Office: _____

Contact Email: _____ **Contact Telephone:** _____

PLEASE HIGHLIGHT YOUR RESPONSES TO THE QUESTIONS BELOW

1. **Did you request suitability investigations or other security actions from the Office of Security Programs (OSP) during July 1, 2011 - September 30, 2012?**

   a) Yes
   b) No

2. **What kind and how many investigations did you request?**

   a) Secret = _____

   b) Top Secret = _____

   c) Other Requests = _____

   PLEASE PROVIDE COPIES OF ALL CORRESPONDENCE RELATED TO THE ABOVE REQUESTS WITH YOUR COMPLETED SURVEY.

3. **Do you believe that your requests were/are handled efficiently?**

   a) Yes
   b) No Please Explain _____

4. **How do you receive information from OSP?**

   a) Phone Calls
   b) Emails
   c) Other Please Define _____

5. **Do you receive quick responses from OSP staff when you have problems or concerns?**

   a) Yes
   b) No

6. **Are you able to obtain security clearance information when needed?**

   a) Always
   b) Sometimes
   c) Never

7. **How much do you pay for OSP services?**

   _____

8. **Do you have any suggestions for improvements in the security clearance process?**

   _____
   _____

Source: OIG audit workpapers.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

February 10, 2015

MEMORANDUM FOR MARLA FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: S. Leslie Ireland /s/
Assistant Secretary
Office of Intelligence and Analysis

SUBJECT: Management Response to Draft Report – Security Clearance Process Performed by the Department of the Treasury's Office of Security Programs

Thank you for the opportunity to review the Office of Inspector General's (OIG) draft report on the security clearance process performed by the Department of the Treasury's Office of Security Programs (OSP). The report makes several recommendations which are addressed below.

Finding 1, Recommendation: Office of Security Programs management provided the OSP workforce a copy of Treasury Directive 40-01 and reminded them of their obligations. OSP is working with OIG, its counsel, and OGC, to clarify the notification requirements of TD 40-01 standards as applied to the range of information to which OSP has access as a result of its role in the security clearance process.

Finding 2, Recommendation 1: Director, OSP in conjunction with Office of Chief Information Officer (OCIO) finalized the Defense Logistics Agency (DLA) support agreement for implementation of the Case Adjudication Tracking System (CATS) on November 7, 2014, upon completion of a resource analysis of required technology. This agreement formalized the participation in, and use of Defense Information System for Security (DISS) by Treasury OSP and sets forth the responsibilities of the parties associated with OSP's receipt and use of Personal Security Investigation (PSI) electronic reports from the Office of Personnel Management (OPM) via OSP DISS. Computers and monitors have also been ordered through OCIO to support CATS implementation. These initiatives should allow OSP to comply with CVS requirements. OSP will continue to collaborate with OCIO on technology, software, equipment and support in order to ensure compliance. OSP anticipates CATS will be implemented by the end of fiscal year 2015.

Finding 2, Recommendation 2: Implementation of the CATS should resolve interoperability issues within the Clearance Verification System (CVS). As a result of the audit, OSP identified CATS as the enterprise tool in order to address the requirement to maintain clearance data in a complete, current, and accurate basis going forward. OSP anticipates CATS will be implemented by the end of fiscal year 2015.

Finding 3, Recommendation: OSP recently implemented a new policy process to ensure reinvestigations are initiated within required timeframes. Under this process, OSP will prioritize the initiation of periodic reinvestigations based on direction issued in a September 26, 2014 memorandum from the Director of National Intelligence.

Finding 4, Recommendation 1: OSP will collaborate with client offices to identify Personnel Security Liaisons in order to facilitate communication between OSP and the client office. OSP will meet with office liaisons and identify ways to improve communications and facilitate real time status inquiries. This collaboration is ongoing, and we will meet with all affected offices by the end of calendar year 2015.

Finding 4, Recommendation 2: The Treasury Security Manual TD P 15-71 is under review to include updating of written guidance and instructions for compliance with applicable laws, regulations and OPM issuances. As part of the review, OSP will consider areas to streamline, elaborate, explain, and provide illustrative guidance on the processes. OSP anticipates completing this by end of calendar year 2015.

Finding 5, Recommendation: OSP is reviewing its written guidance and instructions for compliance with applicable laws, regulations and OPM issuances. OSP recently hired a Policy and Personnel Security Specialist charged with completion of Standard Operating Procedures (SOPs) detailing the security clearance process and procedures including the four areas described above for Treasury security specialists. OSP anticipates completing this by end of calendar year 2015.

If you have any questions, please feel free to contact Michael W. Mason, Acting Deputy Assistant Secretary for Security, at (202) 622-6583.

Kieu T. Rubb, Audit Director
Katherine E. Johnson, Audit Manager
Cecilia K. Howland, Auditor-In-Charge
Justin D. Summers, Program Analyst
John N. Tomasetti, Referencer

Department of the Treasury

Deputy Secretary
General Counsel
Under Secretary for Terrorism and Financial Intelligence
Deputy Assistant Secretary for Security
Director, Office of Security Programs
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

OIG Budget Examiner