Office of Inspector General
U.S. Government Accountability Office

SECURITY CLEARANCES

Actions Needed to Strengthen Controls over Top Secret Security Clearance Requirements

Serving the Congress and the Nation

OIG-13-3

Office of Inspector General
U.S. Government Accountability Office
Report Highlights

September 2013

SECURITY CLEARANCES

Actions Needed to Strengthen Controls over Top Secret Security Clearance Requirements

Objective

The Office of Inspector General (OIG) evaluated the extent to which the U.S. Government Accountability Office (GAO) has established effective policies and procedures (controls) to review and validate top secret security clearance requirements.

What OIG Found

While GAO has established a policy to review and validate security clearances, it does not provide detailed procedures for designating positions as sensitive (i.e., to require a security clearance). Our work showed that the Director, Office of Security (OS) grants and renews top secret security clearances solely based on security clearance requests from unit heads. OIG found that decisions by the Director, OS to grant or renew top secret clearances in fiscal year 2012 were, for the most part, made without justification to support employees' needs for access to top secret information. Without these controls, GAO has no reasonable assurance that only employees who need access to top secret information are granted top secret clearances.

What OIG Recommends

OIG recommends that the Comptroller General direct the Chief Administrative Officer to oversee the establishment and implementation of detailed procedures that define consistent criteria and processes to ensure that the agency's position designation and position sensitivity policies are carried out. OIG also recommends that GAO establish procedures to ensure that decisions to grant top secret security clearances are grounded in written justifications. Such documentation should include sufficient support to demonstrate each employee's need for access to top secret information. GAO agreed with OIG's recommendations.

Memorandum

Date: September 27, 2013

To: Comptroller General Gene L. Dodaro

From: Inspector General Adam R. Trzeciak

Subject: *Security Clearances: Actions Needed to Strengthen Controls over Top Secret Security Clearance Requirements*

The U.S. Government Accountability Office (GAO) conducts a wide range of financial and performance audits, program evaluations, management reviews, investigations, and legal services spanning a broad range of government programs and functions. Certain GAO work may involve access to classified information or facilities that require a security clearance for unescorted entry. Consistent with GAO's mission and national security interests, employees requiring access to classified information must have the appropriate security clearances. The Office of Inspector General (OIG) reviewed management controls in place to identify and validate top secret security clearance requirements.

Background

GAO has established policies to review and validate top secret security clearance requirements. According to GAO Order 0910.1, *GAO Security Program*, the Chief Administrative Officer is responsible for developing, implementing, and overseeing the GAO Security Program, including personnel security.[1] In addition, supervisors, including unit heads (e.g., managing directors and heads of mission support offices and staff offices), in consultation with the Chief Human Capital Officer and the Director, Office of Security (OS), are required to designate (i.e., label) every position under their jurisdiction as either a public trust position[2] or national security sensitive position.[3] When designating positions, unit heads are to ensure that a person's duties are consistent with the position designation and the personnel security requirements for the position.

[1]Personnel security is a program to ensure that all covered persons who have been granted access to information, property, or other assets or resources under the authority and control of GAO meet personnel security standards commensurate with the sensitivity of their positions.

[2]A public trust position (i.e., a position that does not require access to classified information) is a position in which an individual's action or inaction could diminish public confidence in, or otherwise have an adverse impact on, the integrity, efficiency, or effectiveness of GAO or other government activities.

[3]As outlined in Executive Order No. 10450, *Security Requirements for Government Employment* (Apr. 27, 1953 as amended) and Part 732 of Title 5 of the Code of Federal Regulations (CFR), a position should be designated sensitive based on an assessment of the nature of the position and degree of damage an individual, who occupies the sensitive position, could cause to national security. As defined in 5 C.F.R. § 732.102: a sensitive position (1) involves activities of the government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) *requires regular use of, or access to, classified information* (emphasis added).

The GAO order defines a national security sensitive position (i.e., sensitive position) as a position that requires access to (1) classified information; (2) a classified facility, which is any facility that requires a security clearance for admittance; or (3) a national security system.[4] If a position meets at least one of these requirements, the order calls for the unit head to designate the position as national security sensitive (i.e., to require a security clearance), consistent with Executive Order 10450 and Part 732 of Title 5, Code of Federal Regulations.

Once a position has been designated as sensitive, the Director of OS is required to assign a sensitivity level to the position. The sensitivity level determines whether the position requires a secret or top secret clearance. This assignment is based on an assessment of the degree of damage that an individual in that position could cause to a critical GAO or other government activity or interest, including national security. GAO's personnel security program Directive 0910.1-01, *Personnel Security Program*,[5] calls for sensitivity levels to be assigned as follows:

- *Non-critical sensitive*, which is any position involving potential serious impact or damage to national security. Non-critical sensitive positions include those involving access to confidential or secret information.
- *Critical sensitive*, which is any position that involves the potential for exceptionally grave impact or damage to national security. Critical sensitive positions include those involving access to top secret information.
- *Special-sensitive*, which is any position that is at a level higher than critical sensitive because of (1) the greater degree of damage to national security that an individual could effect by virtue of the position, or (2) special requirements applicable to comparable positions in the executive branch of the government that are governed by requirements over and above those of Executive Order 10450.

The Director, OS, or designee, is the single clearance-granting authority for GAO. The Director, OS, issues two levels of security clearances—top secret and secret, based on the sensitivity level.

When notified of a new employee appointment, OS will inform the relevant unit head by e-mail to request that the unit head confirm sensitivity level and security clearance requirements, based on the duties of the new employee's position.

Employees who are currently holding a security clearance are subject to reinvestigation. The level of security clearance determines the frequency of reinvestigation: for top secret clearance, a reinvestigation is required once every 5 years; for secret clearance, a reinvestigation is required once every 10 years. When a current employee's clearance is due for an update, OS will inform the relevant unit head by e-mail of the need to update the

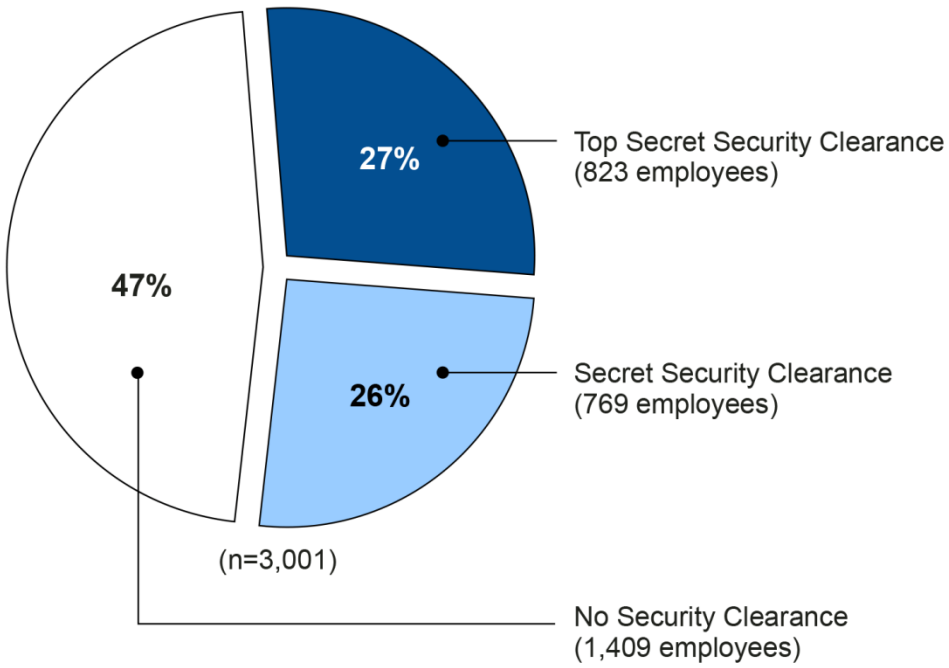
[4]A national security system is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which—(I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

[5]GAO Directive 0910.1-01, *Personnel Security Program* (July 1, 2013). This directive superseded GAO Directive 0910.1-01, *Personnel Security Program*, dated October 19, 2007, to reflect an organizational change.

investigation, and request that the unit head confirm continued position sensitivity level and security clearance requirements.

In fiscal year 2012, an initial top secret security investigation cost $2,836, and the 5-year reinvestigation cost $1,754. An initial secret clearance investigation cost $752, and the 10-year reinvestigation cost $228. From fiscal years 2007 through 2012, GAO spent, on average, about $500,000 annually on personnel security investigations. Based on data in GAO's central repository of personnel security determination records—known as the Security Clearance Online Tracking System (SCOTS)—as of November 19, 2012, more than half of GAO's employees, 27 percent and 26 percent, respectively, held top secret and secret security clearances (see figure 1).

Figure 1: GAO Employees' Security Clearance Profile, as of November 19, 2012



Source: OIG analysis of Office of Security personnel security data.

Objective, Scope and Methodology

This report addresses the extent to which GAO has established effective policies and procedures (controls) to review and validate top secret security clearance requirements to ensure that only employees with a need for regular access to top secret information are granted top secret clearances. To address the objective, we identified applicable policies and procedures and interviewed OS management officials who administer the personnel security program about the process for obtaining or renewing security clearances. In addition, we interviewed GAO's Chief Human Capital Officer and Deputy Chief Human Capital Officer, the Managing Director and Deputy Managing Director of Infrastructure Operations, and select mission team managing directors to obtain their perspectives on GAO policies and procedures for reviewing and validating top secret clearance requirements. We also reviewed executive orders, federal regulations, and GAO policies

and procedures related to the personnel security clearance process to identify clearance criteria and access requirements.

We analyzed clearance data from SCOTS, as of November 19, 2012, to determine the number of GAO employees who (1) were granted initial top secret clearances, and (2) had top secret clearances renewed in fiscal year 2012—the most recent year for which GAO-wide clearance data were available. We selected a simple random sample of 67 (of 213) top secret clearances granted or renewed in fiscal year 2012[6] to evaluate GAO's personnel security clearance policies, procedures, and practices against criteria in GAO's *Standards for Internal Control in the Federal Government*.[7] To assess the effectiveness of GAO's controls, the evaluation included a review of electronic SCOTS data files and hard copy personnel security records used by OS to capture personnel security clearance eligibility information. The results from our security clearance record reviews can be generalized to all 213 top secret security clearances granted or renewed in fiscal year 2012.[8]

We supplemented our work with a web-based survey of all GAO employees who had their top secret clearances renewed in fiscal year 2012—the most recent year for which GAO-wide clearance data were available—to obtain their perspectives about the need for clearances in the performance of their job duties and responsibilities in the last 5 years. Additional information on our scope and methodology is presented in attachment I, and the frequency of responses for selected survey questions is presented in attachment II.

We conducted this performance audit from September 2012 to September 2013 in accordance with generally accepted government auditing standards (GAGAS), except for the quality control and assurance standard requiring an external peer review of our audit organization every three years. The Inspector General is in the process of scheduling a peer review in fiscal year 2014. GAGAS requires 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 objective.

[6]We calculated the sample size of 67 clearances for a proportion estimate, assuming a population of 50 percent, to achieve a margin of error of 10 percentage points at the 95 percent confidence level.

[7]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999); GAO, *Internal Control Management and Evaluation* Tool, GAO-01-1008G (Washington, D.C.: August 2001).

[8]While our review looked at how security clearance requirements are documented, we did not revisit or "second guess" decisions to grant individual clearances. In addition, the scope of our review did not include the adjudication process for determining eligibility for access to classified information.

Internal Controls in the Clearance Process Do Not Provide Reasonable Assurance that Only Employees Who Need Access to Top Secret Information are Granted Top Secret Clearances

While GAO has an order[9] to set its policy for its personnel security program and a directive[10] to implement its order, GAO does not provide detailed procedures for designating sensitive positions, giving unit heads and OS discretion to decide how the policy should be implemented. Current agency practices do not reflect the stated policy. None of the positions occupied by the 1,592 employees who held security clearances (as of November 19, 2012) were designated as sensitive, including the 823 employees who held top secret security clearances. Our work showed that, in the absence of sensitive position designations, decisions to grant or renew top secret security clearances are solely based on requests from unit heads, not on OS's independent determination of sensitivity. That is, decisions to grant or renew top secret clearances in fiscal year 2012 were, for the most part, made without justification of employees' needs for access to top secret information. Without these controls, GAO has no reasonable assurance that only employees who need access to top secret information are granted top secret clearances.

In February 2008 and in subsequent reports examining personnel security clearance processes, GAO has highlighted the importance of a strong requirements-determination process in managing the workload and costs associated with the security clearance process.[11] GAO noted that, while having a large number of cleared personnel can give the military services, agencies, and industry a great deal of flexibility when assigning personnel, having unnecessary requirements for security clearances increases the investigative and adjudicative workloads that are required to provide the clearances and flexibility. GAO further noted that requests for clearances for positions that do not need a clearance or need a lower level of clearance increases costs unnecessarily.

Detailed Procedures Not Established for Designating Position Sensitivity

GAO has not established detailed procedures that define consistent criteria and processes to ensure that the agency's sensitive position designation policies are carried out. GAO's personnel security program directive requires unit heads to determine whether a given position requires access to classified information, and if access is required, to designate the position to require a security clearance. As of November 19, 2012, none of the 823 positions held by GAO employees with top secret clearances were designated as positions that required access to top secret information.[12] GAO's personnel security program directive also requires the Director of OS to assess and assign a sensitivity level to positions that require a security clearance; but, of the 823 positions that employees with top secret clearances held, none were assigned sensitivity levels.

---

[9]GAO Order 0910.1.

[10]GAO Directive 0910.1-01.

[11]GAO, *Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements*, GAO-12-800 (Washington, D.C.: July 12, 2012); *Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort*, GAO-12-815T (Washington, D.C.: June 21, 2012); *Personnel Clearances: Key Factors for Reforming the Security Clearance Process*, GAO-08-776T (Washington, D.C.: May 22, 2008); and *Personnel Clearances: Key Factors to Consider in Efforts to Reform Security Clearance Processes*, GAO-08-352T (Washington, D.C.: February 27, 2008).

[12]Based on data in GAO's central repository of personnel security determination records.

Unit heads provided various opinions on the reasons for not following GAO's position designation policy. For example, unit heads cited the need for flexibility in assigning staff to meet congressional mandates, the length of time necessary to complete a background investigation to support a top secret clearance, the nature of the way the team assigns staff to engagements, the increasing number of engagements that require access to classified information, and the unpredictability of the engagement work that needs to start immediately as reasons position designations are not practical.

Senior officials responsible for a range of administrative and operational support services said that unit heads are the appropriate agency officials for determining top secret security clearance requirements, and because OS has a mission support role, it is reluctant to question the security clearance requirements determined by the unit heads. These same officials also cited the nature of GAO's mission and congressional workload, declining staff resources to support congressional priorities, and the length of time it takes to issue a top secret clearance as obstacles to implementing GAO's position designation policy.

Further, senior GAO human capital officials said that the majority (56 percent) of the people at GAO who are engaged in mission work are in the agency's analyst job series (347), a job series unique to GAO. According to these officials, GAO's existing policy for position designations is difficult to apply to analyst positions because GAO's position description for the analyst job series is generic and covers a wide range of duties.

While flexibility is cited as one explanation for not designating positions, we have no evidence to suggest that following a designation process would reduce the flexibility to assign staff to engagements that require access to top secret information.

According to *Standards for Internal Control in the Federal Government*, management is responsible for developing detailed policies, procedures and practices to fit agency operations. According to OS officials, when GAO implemented its original position designation policy in 1994, the agency had well-defined procedures in place to help ensure consistent criteria for evaluating a position's need for a security clearance.[13] The original policy was implemented in part to reflect changes in executive branch policy, but also to address concerns about granting unnecessary security clearances. At the time, the new designation system was expected to result in a significant decrease in the number of security clearances.

Position designation was a key first step in GAO's security clearance eligibility process, and a position's duties and responsibilities, its impact on the efficiency of the federal service, and national security considerations were all factors in the position designation process. The designation process in 1994 required unit heads to apply some basic principles to position designations, which include the following:[14]

- "base designations on an assessment of an employee's actual duties and responsibilities, not on speculation about what kind of duties and responsibilities an employee might assume in the future, or what kind of information the employee might handle if the employee were to depart from the scope of his/her duties."
- "do not make a designation on the basis of whether a particular GAO employee has previously held or been eligible for a security clearance. Do not consider an incumbent's

[13]GAO Notice 0910.1 (A-94), *GAO Position Designation Procedure* (January 7, 1994), and GAO Notice 0910.1 (B-94), *Processing Procedures for Suitability and Clearability Determinations* (January 7, 1994).

[14]GAO Notice 0910.1 (A-94).

grade in the decision process; designating officials must focus on a person's job responsibilities and functions."

- "do not designate a position in a higher risk category that would require a more extensive investigation than is justified by the position."

The procedures reflected these principles and outlined criteria for following them. For example, the procedures noted that GAO designated each employee's position into one of two categories—national security position (i.e., a position requiring access to classified information) or public trust position. The duties and responsibilities of a national security position required access to classified information. In addition, the procedures indicated that for background investigation and clearance purposes, as a next step, GAO had to decide whether the position required access to top secret information or to secret or confidential information. Personnel security action requests containing such information as the name of the employee, position title, job series (e.g., analyst job series 347) were then submitted to OS for review and validation.

According to OS officials, GAO stopped using these procedures in 2007 when the agency implemented its current personnel security order. In the absence of detailed procedures for designating sensitive positions, our work showed that the Director, OS, grants and renews top secret security clearances based solely on security clearance requests from unit heads.

Top Secret Clearances Generally Granted without Justification to Support Need

OIG found that decisions by the Director, OS, to grant or renew top secret clearances in fiscal year 2012 were, for the most part, made without justification to support employees' needs for access to top secret clearances. GAO's personnel security policy and procedures do not require unit heads to submit, or OS to maintain, sufficient written justification to support the need for access to top secret information. As a result, an important system of checks and balances, the separation of duties, is not effectively implemented.

Federal standards for internal control and associated guidance state that agencies should document key decisions in a way that allows decisions to be traced from initiation, through processing, to after completion. Federal standards for internal control and associated guidance also state that agencies should document key activities in such a way to maintain the relevance, value, and usefulness of these activities to management in controlling operations and making decisions. GAO's personnel security directive instructs OS to e-mail unit heads to request (1) position sensitivity level and (2) security clearance requirements based on the duties of each new employee's position. For clearance renewals, the directive instructs OS to confirm continued position sensitivity level and security clearance requirements, or information regarding change in status. According to the directive, "the type of investigation required depends on the unit head's response."[15]

Based on our sample of 67 recently granted or renewed top secret security clearances, we estimate that about 76 percent of 213 personnel security records did not contain any documentation regarding the position sensitivity level and security clearance requirements to support the needs for top secret clearances.[16] In addition, we estimate that 13 percent of 213 records included information to support the needs for top secret clearances and 11 percent of them included limited information to support the needs for top secret clearances.

[15]GAO Directive 0910.1-01.

[16]Because we selected a simple random sample of top secret clearances for review, the results from our security clearance record review can be generalized to all 213 top secret security clearances granted or renewed in fiscal year 2012. Each estimate has a margin of error of plus or minus 12 percentage points or fewer.

Example e-mail exchanges and other documentation shown in figure 2 illustrate the more detailed justification unit heads provided to OS confirming their top secret security clearance requirements for employee positions.

Figure 2: Examples of Records That Included Information to Support Employees' Needs for Top Secret Clearances That Were Granted or Renewed in Fiscal Year 2012

"_____ currently has a secret security clearance. She has been staffed to an engagement that I will be co-AICing. In the course of this engagement we will definitely be operating with secret level documents, and will likely also review documents and/or conduct interviews at the top secret level. The director for the engagement has validated the need for _____ to have her security clearance upgraded from secret to top secret. Please advise as to next steps so that we can start this process."

E-mail from an analyst (not a unit head) to OS

"Your approval is requested to obtain SCI clearance with SI, TK, G, and HCS accesses for the following individuals_____. These individuals will be working on engagements involving _____. They will require access to SCI information with SI, TK, G, and HCS information to conduct these engagements."

Memorandum from a unit head to the Comptroller General[a]

"I am requesting a top secret clearance for _____. I have just assigned _____ as the AIC on our review. _____ currently possesses a secret level clearance. Given the nature of the work (and where we will be conducting the work), the possession of a TS clearance would be essential to our access to facilities, and, of course, any necessary information we may need that is classified at the TS level."

E-mail from a unit head to OS

Source: GAO Office of Security.

[a]The unit head submitted a request to the Comptroller General to obtain a sensitive compartmented information (SCI) clearance for an employee. According to an OS official, the employee did not have a top secret clearance at the time the SCI request was submitted. The investigative requirement for access to top secret and SCI is a favorably adjudicated single scope background investigation. According to an OS official, OS first granted the employee a top secret security clearance and then processed the request for the SCI clearance.

As shown in figure 3, however, the e-mail exchanges and other documentation represent the more limited information unit heads provided to OS confirming their top secret security clearance requirements for employee positions.

Figure 3: Examples of Records That Included Limited Information to Support Employees' Needs for Top Secret Clearances That Were Granted or Renewed in Fiscal Year 2012

"___ would like to request a top secret clearance for _____." "Please let me know if additional information is needed."

E-mail from an Assistant Director to OS

"As requested, below are the names of ___staff who we want to put in for top secret clearances. We could prioritize these if necessary as we discussed. Please reply to all with your approval/disapproval."

"Approved. These folks are all permanent ___staff and will need a top secret clearance."

E-mail from a Director to a unit head and the unit head's response forwarded to OS

"Needs TS per _____"

Annotation in GAO's central repository of personnel security determination records—known as the Security Clearance Online Tracking System

Source: GAO Office of Security.

OS officials acknowledged that clearance records intended to support security clearance decisions to grant or renew top secret security clearances generally do not contain sufficient justification regarding employees' needs for access to top secret information primarily because GAO's personnel security program policy and directive do not explicitly require it. Senior officials responsible for a range of administrative and operational support services and OS officials stated that OS is reluctant to question unit head responses because they believe that the unit heads are in the best position to make determinations regarding which employees require a top secret clearance. Without documentation, however, OS is not positioned to confirm employees' top secret security clearance needs. The Director of OS's decisions to grant or renew top secret security clearances, based on little or no information from unit heads to support top secret security clearance requirements, could potentially lead to unnecessary top secret clearances.

Our survey of GAO employees who had their top secret security clearances renewed in fiscal year 2012 showed that GAO renewed top secret security clearances that were not needed over the past 5 years, or were granted at a level higher than needed. Specifically, almost one-third of survey respondents (31 of 108) indicated that they did not use their top secret clearances at all in the last 5 years. Twenty-six of the 31 survey respondents reported that they only needed to access information classified lower than top secret in the performance of their job duties or responsibilities in the last 5 years, and the remaining 5 survey respondents reported that they did not need a top secret or secret clearance at all in the last 5 years.[17]

[17]For purposes of our survey, information lower than top secret is defined as (1) secret or confidential information that require protection against unauthorized disclosure in the interest of national security and (2) sensitive information under the authority or control of GAO that is not classified information, but that requires protection to ensure that it is not released to the public or any other individual or organization not under the authority or control of GAO without further review because it may be exempted from such disclosure.

In response to an open-ended question asking survey respondents to provide any additional comments about their job duties or responsibilities, one respondent stated that he or she had to access top secret information only once in a 23-year career. Although another respondent had not used his or her clearance, the respondent stated that having the clearance provides the respondent's mission team the flexibility to staff him or her to engagements which may require it.

Survey results also offer insights into whether clearance decisions are based on demonstrated needs for access to top secret information. In responding to a survey question about what best describes the reason that their top secret security clearances were renewed in fiscal year 2012, 43 percent of respondents (46 of 108) cited that their job duties or responsibilities require access to top secret information; 57 percent of survey respondents (61 of 108) cited that their job duties or responsibilities may require access to top secret information at a future date; and one survey respondent reported that he or she was unsure about the reason his or her top secret clearance was renewed.

In providing additional comments about their job duties or responsibilities requiring a top secret clearance, one respondent indicated that his or her current job duties typically do not require access to top secret information, and they have not required this kind of access in the last 5 years. The respondent further indicated that several years ago he or she accessed top secret information, and given the current position and the nature of the portfolio of work, he or she can never be sure when an engagement may be assigned that would require top secret access. In addition, another respondent stated that in some agencies and locations, a lack of a top secret clearance will prevent GAO from access to officials or information in a reasonable time frame in the conduct of an audit. The respondent also said that therefore, it is very useful to have top secret clearances for at least some mission team analysts and auditors in case the clearances are needed. A different respondent indicated that, at this time, it is not clear when or how their clearance would be used.

Conclusions

Consistent with GAO's mission and national security interests, GAO requires employees who need access to classified information to have the appropriate security clearances. GAO has established policies to review and validate top secret security clearance requirements, but a lack of detailed procedures has led to agency practices—specifically, granting security clearance requests for positions that have not been designated as national security sensitive—that do not reflect those policies.

In addition, while we believe that unit heads are in the best position to know their employees' clearance requirements, their requests currently lack the documentation that would allow OS to independently validate employee needs. Without these controls, there is no reasonable assurance that only employees who need access to top secret information are granted top secret clearances.

Recommendations

1. The OIG recommends that the Comptroller General direct the Chief Administrative Officer to oversee the establishment and implementation of detailed procedures that define consistent criteria and processes to ensure that the agency's position designation and position sensitivity policies are carried out.

2. We also recommend that the Comptroller General direct the Chief Administrative Officer to establish procedures to ensure that decisions to grant top secret security clearances are grounded in written justifications. Such documentation should include sufficient support to demonstrate each employee's need for access to top secret information.

Agency Comments

The Inspector General provided GAO with a draft of this report for review and comment. GAO provided written comments, which are reprinted in attachment III. GAO agreed with our recommendations and described actions planned to address them. Specifically, GAO stated that the security clearance issuance and renewal process needs to be revised to ensure that GAO Order 0910.1, policies and procedures are current and to ensure that adequate documentation is in place to justify a need for a clearance. In addition, GAO has assembled a team of key senior managers to evaluate the agency's current policies and procedures to determine what changes are needed to improve oversight and monitoring of the security clearance issuance and renewal process.

Actions taken in response to our recommendations are expected to be reported to our office within 60 days.

We are sending copies of this report to the other members of GAO's Executive Committee (the Chief Operating Officer, Acting Chief Administrative Officer/Chief Financial Officer, and General Counsel), GAO's Audit Advisory Committee, and other key managers. The report is also available on the GAO website at http://www.gao.gov/about/workforce/ig.html.

If you or your staff have any questions about this report, please contact me at (202) 512-5748 or trzeciaka@gao.gov. Contact point for GAO's Public Affairs may be found on the last page of this report. Key contributors to this report were Sandra Burrell; James Ashley; Cathy Helm; Cynthia Hogue; Jill Lacey; and Michael Volpe.

Attachments (3)

Attachment I: Objective, Scope and Methodology

This report addresses the extent to which GAO has established effective policies and procedures (controls) to review and validate top secret security clearance requirements to ensure that only employees with a need for regular access to top secret clearance information are granted top secret clearances. To address the objective, we identified applicable policies and procedures and interviewed OS management officials who administer the personnel security program about the process for obtaining or renewing security clearances. In addition, we interviewed GAO's Chief Human Capital Officer and Deputy Chief Human Capital Officer, the Managing Director and Deputy Managing Director of Infrastructure Operations, and select mission team managing directors to obtain their perspectives on GAO policies and procedures for reviewing and validated top secret clearance requirements. We also reviewed executive branch orders, federal regulations, and GAO policies and procedures related to the personnel security clearance process to identify clearance criteria and access requirements.

We analyzed clearance data from GAO's central repository of personnel security determination records, known as the Security Clearance Online Tracking system (SCOTS), as of November 19, 2012, to determine the number of GAO employees who (1) were granted initial top secret clearances, and (2) had top secret clearances renewed in fiscal year 2012—the most recent year for which GAO-wide clearance data were available. We identified 213 employees and selected a simple random sample of 67 (of 213) top secret clearances granted or renewed in fiscal year 2012[18] to evaluate GAO's personnel security clearance policies, procedures, and practices against criteria in GAO's *Standards for Internal Control in the Federal Government*.[19] To assess the effectiveness of GAO's controls, the evaluation included a review of electronic SCOTS data files and hard copy personnel security records used by OS to capture personnel security clearance eligibility information. The results from our security clearance record reviews can be generalized to all 213 top secret security clearances granted or renewed in fiscal year 2012.[20] On the basis of information from and discussions with OS management officials related to the controls in place to maintain the integrity of clearance data, we determined that the information in SCOTS was sufficiently reliable for the purposes of defining our audit population and selecting a sample for further review.

We supplemented our work with a web-based survey of all GAO employees who had their top secret clearances renewed in fiscal year 2012—the most recent year for which GAO-wide clearance data were available—to obtain their perspectives about the need for top secret clearances in the performance of their job duties and responsibilities in the last 5 years. Based on information on top secret security clearances provided by the OS, we identified 154 employees who had their top secret clearances renewed in fiscal year 2012 that would serve as the population for this survey. We later identified 11 employees that were out of scope, including those who retired or left GAO in fiscal year 2013. We sent the survey to 143 employees. We received responses from 108 of the 143 surveyed GAO

[18]We calculated the sample size of 67 clearances for a proportion estimate, assuming a population of 50 percent, to achieve a margin of error of 10 percentage points at the 95 percent confidence level.

[19]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[20]While our review looked at how security clearance requirements are documented, we did not revisit or "second guess" decisions to grant individual clearances. In addition, the scope of our review did not include the adjudication process for determining eligibility for access to classified information.

employees—a 76 percent response rate. The web-based survey was administered from March 13, 2013, to March 29, 2013. Respondents were sent an e-mail invitation to complete the survey on a GAO web server using a unique username and password. During the data collection period, we sent reminder e-mails to nonresponding employees. Because this was not a sample survey, it has no sampling errors. The practical difficulties of conducting any survey may also introduce nonsampling errors, such as difficulties interpreting a particular question, which can introduce unwanted variability into the survey results. We took steps to minimize nonsampling errors by pretesting the questionnaire in person with seven GAO employees in various audit and research teams, at various grade levels, based at headquarters in Washington, D.C. and in various field offices across the country. We conducted pretests to make sure that the questions were clear and unbiased, the information was readily obtainable, and the questionnaire did not place an undue burden on respondents. An independent reviewer also reviewed a draft of the questionnaire prior to its administration. We made appropriate revisions to the content and format of the questionnaire after the pretests and independent review. All data analysis programs used to generate survey results were independently verified for accuracy. Additionally, in reviewing the answers from GAO employees, we confirmed that they had correctly bypassed inapplicable questions (skip patterns). Based on our findings, we determined that the survey data are sufficiently reliable for the purposes of this engagement.

We conducted this performance audit from September 2012 to September 2013 in accordance with generally accepted government auditing standards (GAGAS), except for the quality control and assurance standard requiring an external peer review of our audit organization every three years. The Inspector General is in the process of scheduling a peer review in fiscal year 2014. GAGAS requires 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 objective.

Attachment II: Responses to Questions from OIG's Survey on GAO Personnel Security Clearances

We supplemented our work with a web-based survey of all GAO employees who had their top secret clearances renewed in fiscal year 2012 to obtain their perspectives about their job duties and responsibilities requiring top secret security clearances. We received responses from 108 (76 percent) of the 143 surveyed employees. For more information about our methodology for designing and distributing the survey, see attachment I.

Tables 1 through 16 show the responses to questions from the survey.

Table 1: Have you needed to use your GAO top secret security clearance to access top secret information in the performance of your job duties or responsibilities in the last 5 years?

Question	Yes	No	Don't know	Total
Number of Reponses	61	43	4	108

Source: OIG survey results.

Note: A top secret clearance is defined as a clearance that gives you access to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. For purposes of this survey, a top secret clearance may be required to access certain Special Category Information that has additional security requirements. The following list of Special Category Information types and definitions appeared in a hyperlinked pop-up box:

- **Special Access Program (SAP)**. SAPs are programs employing enhanced security measures exceeding those normally required for classified information of the same classification level.
- **Sensitive Compartmented Information (SCI)**. SCI is classified information concerning, or derived from, intelligence sources, methods, or analytical processes that must be handled within formal access control systems established by the Director, Central Intelligence Agency.
- **Restricted Data (RD).** RD is classified information overseen by the Department of Energy (DOE) concerning the design, manufacture, or utilization of nuclear weapons; production of special nuclear material; or use of special nuclear material in the production of energy, not including data declassified or removed from the RD category (i.e., Formerly Restricted Data).
- **Formerly Restricted Data (FRD).** FRD is classified information overseen by DOE and DOD relating to military utilization of atomic weapons that has been removed from the RD category.
- **Critical Nuclear Weapon Design Information (CNWDI).** CNWDI is Top Secret RD or Secret RD overseen by DOE and/or DOD that reveals the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device.
- **North Atlantic Treaty Organization (NATO) Information.** NATO classified information is information that is circulated within and by member countries of NATO, and is classified by a NATO member, entered into the NATO security system, and is accessible by any NATO member.

Table 2: When was the last time you needed to use your GAO top secret security clearance to access top secret information in the performance of your job duties or responsibilities?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Unsure	Total
Number of Reponses	32	15	7	3	3	1	61

Source: OIG survey results.

Notes: Results reflect the responses of those that answered "Yes" to the question, "Have you needed to use your GAO top secret security clearance to access top secret information in the performance of your job duties or responsibilities in the last 5 years?"

Respondents were also asked to provide a brief description of the top secret information they last accessed and how it related to their job duties or responsibilities.

Table 3: Have you used your GAO top secret security clearance to access a facility that requires at least a top secret security clearance for entry to, or ease of movement within, controlled areas in the last 5 years?

Question	Yes	No	Don't know	Total
Number of Reponses	48	53	7	108

Source: OIG survey results.

Table 4: When was the last time you needed to use your GAO top secret security clearance to access a facility that requires at least a top secret security clearance for entry to, or ease of movement within, controlled areas?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Total
Number of Reponses	27	8	6	6	1	48

Source: OIG survey results.

Notes: Results reflect the responses of those that answered "Yes" to the question, "Have you used your GAO top secret security clearance to access a facility that requires at least a top secret security clearance for entry to, or ease of movement within, controlled areas in the least 5 years?"

Respondents were asked to provide a brief description of the purpose for their most recent visit when they used their GAO top secret security clearance to access a facility that requires at least a top secret clearance for entry to, or ease of movement within controlled areas.

Table 5: Have you used your GAO top secret security clearance to access a national security system in the performance of your job duties or responsibilities in the last 5 years?

Question	Yes	No	Don't know	Total
Number of Responses	27	78	3	108

Source: OIG survey results.

Notes: Examples of national security systems include: secure telephone units (STU-III/STE) approved to discuss top secret information; security telephone equipment (STU-III/STE) approved to transmit top secret information; and designated computers authorized to process top secret information.

Examples of national security systems do not include: the Secure Internet Protocol Router Network (SIPRNet); and Department of Defense's Non-secure Internet Protocol Router Network (NIPRNet).

The following information on national security systems appeared in a hyperlinked pop-up box:

A **national security system** is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which— (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Table 6: When was the last time you needed to use your GAO top secret security clearance to access a national security system in the performance of your job duties or responsibilities?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Total
Number of Reponses	16	6	3	2	0	27

Source: OIG survey results.

Notes: Results reflect the responses of those that answered "Yes" to the question, "Have you used your GAO top secret security clearance to access a national security system in the performance of your job duties or responsibilities in the last 5 years?"

Respondents were asked to provide a brief description of the national security system they last accessed and a description of the top secret information accessed on the system.

Table 7: Have you needed to access information lower than top secret in the performance of your job duties or responsibilities in the last 5 years?

Question	Yes	No	Not checked	Total
Number of Reponses	99	8	1	108

Source: OIG survey results.

Note: For purposes of this survey, information lower than top secret is defined as (1) secret or confidential information that require protection against unauthorized disclosure in the interest of national security and (2) sensitive information under the authority or control of GAO that is not classified information, but that requires protection to ensure that it is not released to the public or any other individual or organization not under the authority or control of GAO without further review because it may be exempted from such disclosure. Sensitive information includes Sensitive But Unclassified (SBU). The following information on SBU appeared in a hyperlinked pop-up box:

Sensitive But Unclassified (SBU) information. SBU information is unclassified information an executive branch agency (or an individual or component within such an agency) has designated as information that should be protected from unauthorized disclosure. The term "SBU" is used both as a specific designation and a general category, which includes:

- administrative designations such as "For Official Use Only" (FOUO), "Limited Official Use Only" (LOUO), and "Law Enforcement Sensitive" (LES), that executive branch agencies may use to describe unclassified information that may be exempt from public disclosure
- statutory designations of unclassified information that should not be released to the public, such as transportation-related sensitive security information (SSI), unclassified controlled nuclear information (UCNI), and taxpayer data protected.

Table 8: What was the type of information you accessed in the performance of your job duties or responsibilities in the last 5 years?

Question	Secret	Confidential	Sensitive but unclassified	Other	Unsure
Number of Responses	84	66	87	13	2

Source: OIG survey results.

Notes: Eighty-seven of 99 survey respondents who indicated that they needed to access information lower than top secret in the performance of their job duties or responsibilities in the last 5 years provided responses to the survey question in the table above. The total number or responses across all categories does not equal the total number of respondents (87) because respondents could have selected more than one category.

Examples of "Other" responses included proprietary and business confidential information, procurement sensitive information, competition sensitive information, GAO work papers, and personally identifiable information.

Table 9: When was the last time you needed to access information lower than top secret in the performance of your job duties or responsibilities?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Total
Number of Reponses	85	10	2	1	1	99

Source: OIG survey results.

Notes: Results reflect the responses of those that answered "Yes" to the question, "Have you needed to access information lower than top secret in the performance of your job duties or responsibilities in the last 5 years?"

Table 10: Have you accessed a facility that requires a security clearance lower than top secret for entry to, or ease of movement within, controlled areas in the last 5 years?

Question	Yes	No	Don't know	Not checked	Total
Number of Reponses	67	33	6	2	108

Source: OIG survey results.

Table 11: When was the last time you accessed a facility that requires a security clearance lower than top secret for entry to, or ease of movement within, controlled areas?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Unsure	Total
Number of Responses	55	5	4	2	0	1	67

Source: OIG survey results.

Note: Results reflect the responses of those that answered "Yes" to the question, "Have you accessed a facility that requires a security clearance lower than top secret for entry to, or ease of movement within, controlled areas in the last 5 years?"

Table 12: Have you accessed a national security system that requires a clearance lower than top secret in the performance of your job duties or responsibilities in the last 5 years?

Question	Yes	No	Don't know	Total
Number of Reponses	64	41	3	108

Source: OIG survey results.

Note: Examples of national security systems include Secure Internet Protocol Router Network (SIPRNet) and designated computers authorized to process classified information. The following information on national security systems appeared in a hyperlinked pop-up box:

A **national security system** is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which— (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Table 13: When was the last time you accessed a national security system that requires a security clearance lower than top secret in the performance of your job duties or responsibilities?

Question	Within the last 12 months	1 to 2 years ago	More than 2 years to 3 years ago	More than 3 years to 4 years ago	More than 4 years ago	Unsure	Total
Number of Responses	50	4	5	1	2	2	64

Source: OIG survey results.

Note: Results reflect the responses of those that answered "Yes" to the question, "Have you accessed a national security system that requires a clearance lower than top secret in the performance of your job duties or responsibilities in the last 5 years?"

Table 14: Have you used your GAO top secret security clearance to perform any other job duties or responsibilities in the last 5 years not already identified?

Question	Yes	No	Don't know	Total
Number of Reponses	19	85	4	108

Source: OIG survey results.

Note: Respondents were asked to provide a brief explanation of how they used their GAO top secret security clearance to perform any other assigned duties or responsibilities.

Table 15: Based on your need to use your GAO top secret security clearance to perform your job duties or responsibilities in the last 5 years, which of the following best describes your need for a top security clearance?

Question:	My job duties or responsibilities required a top secret security clearance	My job duties or responsibilities required a lower than top secret security clearance	My job duties or responsibilities did not require a security clearance	Unsure	Total
Number of Responses	68	32	4	4	108

Source: OIG survey results.

Table 16: To the best of your knowledge, which of the following best describes the reason that your top secret security clearance was renewed in fiscal year 2012?

Question:	My current job duties or responsibilities do require access to top secret information	My current job duties or responsibilities may require access to top secret information at a future date	Unsure	Total
Number of Responses	46	61	1	108

Source: OIG survey results.

Note: Respondents were asked to provide additional comments they had about their job duties or responsibilities requiring a top secret clearance.

Attachment III: Comments from the U.S. Government Accountability Office

Comptroller General of the United States

United States Government Accountability Office
Washington, DC 20548

September 23, 2013

Adam Trzeciak
Inspector General

Thank you for the opportunity to review your draft report OIG-13-3, *Actions Needed to Strengthen Controls over Top Secret Security Clearance Requirements*. Overall, the Executive Committee agrees with the two recommendations contained in your report and we offer the following comments on the current process at GAO.

To be efficient and produce high quality products, it remains a top priority of agency management to be able to quickly mobilize staff to work on engagements with minimal to no delay and to ensure that staff have access to the right site (location), personnel and records. This often means already having the appropriate top secret or a secret security clearance in place. As noted in the OIG report, agency management values having this flexibility when needed and we believe the Managing Director designation is at the appropriate level of authority to make such a determination. To that end, we agree that the security clearance issuance and renewal process needs to be revised to ensure that our GAO Order 0910.1, policies and procedures are current and to ensure that adequate documentation is in place to justify the need for a clearance.

For your information, I have assembled a team of key senior managers to evaluate our current policies and procedures to determine what changes are needed to improve oversight and monitoring of the security clearance issuance and renewal process.

In closing, we appreciate your work in this area and for identifying actions to take to strengthen controls over issuing security clearances while continuing to meet the goals and objectives of GAO and our mission, including quickly mobilizing staff to work on engagements and be able to carry out work without delay or roadblocks.

As required, and within 60 days of your published report, we will provide you with a summary of actions taken to date or planned actions for each recommendation. If you have any questions, please contact me at 512-5800.

Cheryl Whitaker
Acting Chief Administrative Officer/
Chief Financial Officer

cc: Pat Dalton, Chief Operating Officer
Terry Dorn, Office of Infrastructure Operations
Carolyn Taylor, Chief Human Capital Officer
Bill Anderson, Controller
Cathy Helm, Office of the Inspector General

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud, waste, and abuse in GAO's internal operations, do one of the following. (You may do so anonymously.)

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Online at: https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimony

To obtain copies of OIG reports and testimony, go to GAO's Web site: www.gao.gov/about/workforce/ig.html.

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149,
Washington, DC 20548