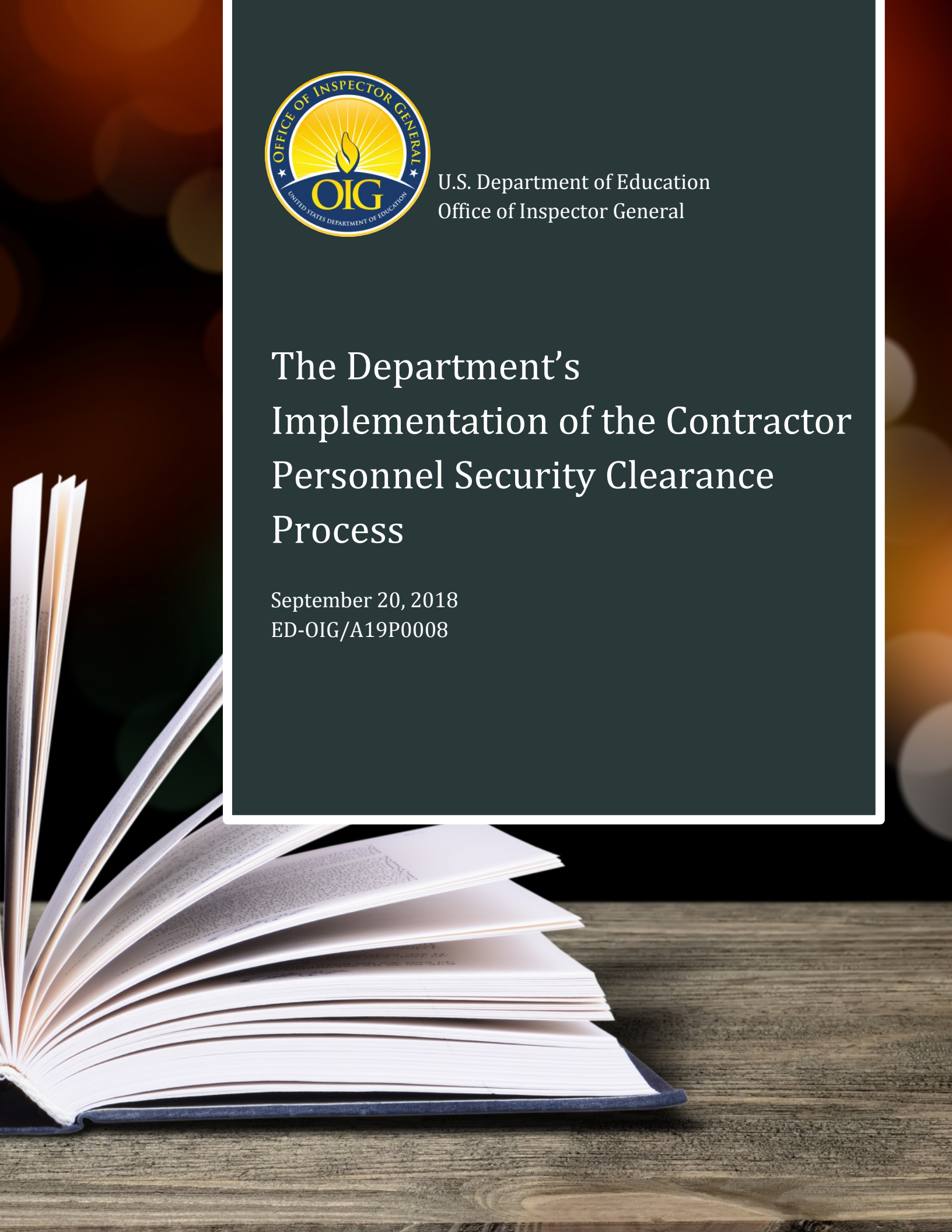

U.S. Department of Education
Office of Inspector General

The Department's Implementation of the Contractor Personnel Security Clearance Process

September 20, 2018
ED-OIG/A19P0008

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. The appropriate Department of Education officials will determine what corrective actions should be taken.

In accordance with the Freedom of Information Act (Title 5, United States Code, Section 552), reports that the Office of Inspector General issues are available to members of the press and general public to the extent information they contain is not subject to exemptions in the Act.

September 20, 2018

TO: Denise L. Carter
Acting Assistant Secretary
Office of Management

FROM: Bryon S. Gordon /s/
Assistant Inspector General for Audit

SUBJECT: Final Audit Report, "The Department's Implementation of the Contractor Personnel Security Clearance Process," Control Number ED-OIG/A19P0008

Attached is the subject final audit report that consolidates the results of our review of the Department's contractor personnel security screening process. We have provided an electronic copy to your audit liaison officer. We received your comments, including corrective actions planned or implemented in response to each of the recommendations included in our draft report.

U.S. Department of Education policy requires that you develop a final corrective action plan within 30 days of the issuance of this report. The corrective action plan should set forth the specific action items and targeted completion dates necessary to implement final corrective actions on the findings and recommendations contained in this final audit report. Corrective actions that your office proposes and implements will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after 6 months from the date of issuance.

We appreciate your cooperation during this review. If you have any questions, please contact Michele Weaver-Dugan at (202) 245-6941 or Michele.Weaver-Dugan@ed.gov.

Attachment

Table of Contents

Results in Brief 1

Introduction 3

Finding. The Department Did Not Effectively Implement Requirements for the Contractor Personnel Security Screening Process 6

Appendix A. Scope and Methodology 28

Appendix B: Contracts Reviewed in this Audit 30

Appendix C. Updated OPM Background Investigation and Reinvestigation Requirements 31

Appendix D: Position Designation Record Template 32

Appendix E. Acronyms and Abbreviations 33

Appendix F. OM Response to the Draft Report 34

Results in Brief

What We Did

The objective of our audit was to determine whether the Department of Education (Department) has effectively implemented the requirements for contractor personnel security screenings. This report presents the results of our review of the Office of Management (OM), the office responsible for Department-wide oversight of the contractor personnel security screening process. It combines the results of work conducted within OM and two principal offices (PO) — the Institute of Education Sciences (IES) and Federal Student Aid (FSA). In conducting this audit, separate reports were issued to IES (ED-OIG/A19R0002) and FSA (ED-OIG/A19R0003) related to their responsibilities within their respective offices pertaining to the contractor personnel security screening process. A listing of the contracts selected for review in each PO is included as Appendix B.

What We Found

We found that the Department has not effectively implemented requirements for the contractor personnel security screening process. Specifically, we found that OM did not provide adequate guidance or oversight of the process to ensure that key requirements of OM Directive: 5-101, Contractor Employee Personnel Security Screenings (Directive), dated July 16, 2010, were implemented and that contractors had appropriate screenings. OM did not ensure the Directive was updated to reflect Federal requirements and Department practices established subsequent to the issuance of the Directive. Additionally, OM did not comply with its own requirements in the Directive, to include ensuring POs submitted to OM PO-specific procedures for complying with the Directive, providing notice to POs of final adjudication determinations, and coordinating with POs with regard to contract position and risk designation.

We also found that OM did not ensure the timeliness of security screening activities; ensure contractor employee screening information maintained was accurate and reliable; or provide adequate training to POs with regard to process requirements and PO responsibilities.

As a result, the Department's ability to effectively implement the requirements for the contractor personnel security screening process may be hindered, to include ensuring key staff involved in the security screening process are aware of their expected responsibilities, ensuring consistency in PO processes, and ensuring compliance with government-wide policies.

In our review of both POs included in this audit, we found that staff and officials involved in the process were generally unaware of Department requirements and their related responsibilities for processing contractor employees' security screenings. Of the 191 contractor employees reviewed in these POs required to have a security screening, we identified at least 66 contractor employees (35 percent) that did not have evidence of an appropriate screening. This lessens the Department's assurance that contractor employees with access to Department-controlled facilities and systems, unclassified sensitive information, and/or school children are suitable for the level of access granted to them. The Department's information and systems might be vulnerable to unauthorized access, inappropriate disclosure, and abuse by contractor employees who may not meet security standards, including those in positions with the potential for moderate to serious impact on the efficiency of the Department.

What We Recommend

We made several recommendations to improve internal controls over the Department's contractor personnel security screening process. We recommend that the Assistant Secretary for Management ensure that OM develops and distributes written policies and procedures for the contractor personnel security screening process that reflect current Federal and Department requirements for the process and existing Department practices, and ensure that OM periodically reviews the security screening process and assesses the need to update policy accordingly. We also recommend that OM require POs to develop and submit internal procedures for the contractor personnel security screening process.

In addition, we recommend that OM develop a process to ensure POs receive notification of all final adjudication determinations, ensure that security screening activities are completed within required timeframes, ensure the accuracy and reliability of security screening data, and provide comprehensive training on the contractor personnel security screening process to all applicable staff.

We provided a draft of this report to OM for comment. OM did not disagree with the finding or recommendations. It noted it was taking proactive steps to resolve the issues and will continue to improve the agency's personnel security program. OM added that as a result of these ongoing improvement efforts, many of the audit recommendations have been implemented or are in the process of being implemented. OM's comments are summarized at the end of the finding. OM also provided technical comments that we considered and addressed, as appropriate, in the body of the report. We did not make any substantive changes to the audit finding or the related recommendations as a result of OM's comments. The full text of OM's response is included as Appendix F to this report.

Introduction

Background

Within the Department, OM is responsible for overseeing personnel security functions. The Personnel Security and Emergency Preparedness Division (Personnel Security) within OM's Office of Security, Facilities, and Logistics Services develops policies, procedures, and guidelines for OM's personnel security function in accordance with applicable Federal laws, regulations, and Executive Orders. In addition, Personnel Security initiates background investigations with the Office of Personnel Management (OPM) for applicants, appointees, employees, and contractor employees. Personnel Security staff also adjudicate[1] the results of OPM background investigations for employees and contractor employees for (1) security clearances or to occupy sensitive positions; and (2) suitability to occupy a position of trust not requiring a security clearance. OM has six staff authorized to perform adjudications.

OM has established the Department's requirements for the contractor personnel security screening process in the Directive. The purpose of the Directive is to establish the Department's policies regarding personnel security screening requirements for contractor employees and to ensure that all contractor employees undergo personnel security screenings if required for performance under a contract. The Department requires all contractor and subcontractor employees to undergo personnel security screenings if they will require an identification badge granting unescorted access to Department facilities, require information technology (IT) system access, require access to unclassified sensitive information, or perform duties in a school or location where children are present.

The Department's processing of contractor employee security screenings involves two information systems: OPM's Electronic Questionnaires for Investigations Processing (e-QIP) system and the Department's Security Manager system.[2] E-QIP is a web-based

[1] An adjudication is an evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is suitable for Government employment; eligible for logical and physical access; eligible for access to classified information; eligible to hold a sensitive position; or fit to perform work for or on behalf of the Government as a Federal employee, contractor, or non-appropriated fund employee.

[2] Security Manager is a web-based system that is owned and operated by a private company. The Department has a contract with this company for general Security Manager system administration such as IT support, specialized reports, and data back-ups.

automated system that OPM uses to process standard investigative forms used when conducting background investigations for Federal security, suitability, fitness, and credentialing purposes. The Department uses e-QIP to electronically enter, update, and transmit contractor employees' personal investigative data to OPM for background investigations. Security Manager is part of the Department's official system of records for the Department's security screening process and is the internal system for processing and tracking contractor employee security screenings.[3] OM uses Security Manager to conduct all aspects of the security screening process including documentation review and maintenance and adjudication of OPM background investigation information.

Processing a contractor employee's security screening generally involves coordination between the contractor employee, the contractor company, OPM, OM, and PO staff, such as Contracting Officer's Representatives (COR), Information System Security Officers, and PO internal security teams. The process begins when a contractor company submits a contractor employee's security screening information to PO staff to inform the PO of the contractor employee's assignment to the contract and to initiate the security screening. PO staff are expected to review the information in a security screening package for accuracy and completeness and, if any errors are detected, assist the contractor company and employee with submitting the required information. A complete security screening package includes a Request for Security Officer Action form, fingerprint documents, and required signature pages. After PO staff have determined that a contractor employee's security package has been completed appropriately, PO staff should release the contractor employee's e-QIP security screening information to OM or directly to OPM. OM initiates security screenings for contractor employees from all POs with the exception of FSA contractor employees in positions designated as Low or Moderate Risk.[4]

---

[3] Security Manager is a subsystem within the Department's Education Security Tracking and Reporting System and interfaces with the other subsystems within that system. The Education Security Tracking and Reporting System maintains records for the purpose of identification verification, adjudication determinations concerning suitability for Federal employment and contract positions, decisions concerning access to the Department's facilities and information systems, and issuance of personal identification verification cards.

[4] FSA initiates screenings directly with OPM for contractor employees in positions designated as Low and Moderate Risk. OM only initiates screenings for FSA contractor employees in positions designated as High Risk.

Contractor employees whose positions are not designated as High Risk can start working under a Department contract as soon as their complete security screening package is submitted through e-QIP to the PO overseeing their contract. Contractor employees whose positions are designated as High Risk can start working under a Department contract at the Moderate Risk level as soon as their complete security screening package is submitted through e-QIP to the applicable PO, but must wait until OM notifies the PO that a preliminary personnel security screening was completed favorably before beginning work at the High Risk level under the contract.[5] Once OM staff receive a security screening package from PO staff for a contractor employee in a High Risk position, OM staff provide the necessary information to OPM electronically through e-QIP to initiate the preliminary personnel security screening. Upon completion of the screening, OPM proceeds with the full High Risk level background investigation while OM reviews the preliminary screening results for suitability.

After OPM completes the requested background investigation, OPM sends OM a report of the results electronically through Security Manager. OM reviews the background investigation report in Security Manager and makes a final personnel security adjudication determination on whether the contractor employee is suitable for employment on the contract at the risk level requested.

In April 2004, the Office of Inspector General (OIG) issued a memorandum entitled, "Inspection of the U.S. Department of Education's Contractor Employee Security Clearance Procedures," (ED-OIG/I13D0009). OIG reported that the Directive (dated October 21, 2002) provided general procedures to be followed in requesting security clearances for contractors, but that OM did not have its own internal procedures for processing clearances, which resulted in inconsistencies in file organization and hampered the clearance process. OIG also determined that OM did not track the status of clearance requests and that investigations were not routinely initiated for all contractors within 14 days as required by Federal regulations and OM policy. In addition, OIG found that OM did not routinely conduct monitoring reviews of pending files to determine whether background investigations were progressing appropriately. Finally, OIG determined that the Department did not routinely monitor to determine if only cleared contractor employees were performing contract functions.

[5] Exceptions may be granted by OM for contractor employees needing immediate High Risk access, but these individuals must be escorted and supervised by an authorized Department employee or authorized cleared contractor employee at all times.

Finding. The Department Did Not Effectively Implement Requirements for the Contractor Personnel Security Screening Process

We found that the Department did not effectively implement requirements for the contractor personnel security screening process. Specifically, we found that OM did not provide adequate guidance or oversight of the process to ensure that key requirements of the Directive were implemented and that contractors had appropriate screenings. OM did not:

- ensure the Directive reflected current Federal and Department requirements;
- comply with Directive requirements specific to OM;
- ensure the timeliness of security screening activities;
- ensure contractor employee screening information maintained was accurate and reliable; or
- provide adequate training to POs with regard to process requirements and PO responsibilities.

Department-Wide Policies and Procedures

OM did not ensure that the Directive reflected current Federal and Department requirements. The purpose of the Directive is to establish Department policy regarding the personnel security screening requirements for all contractor and subcontractor employees assigned to positions that require such screenings. However, we identified areas of the contractor personnel security screening process that were not addressed by the Directive or by other interim guidance issued by OM. These areas include Federal requirements and Department practices established subsequent to the issuance of the Directive in 2010.

For example, in 2011, OPM began requiring that, similar to the requirement for High Risk public trust positions, reinvestigations for Moderate Risk public trust positions be conducted every 5 years. In addition, in 2012, OPM established a tiered system for background investigations.[6] Investigation classifications were changed, to include certain background investigation types being discontinued or consolidated with other types of background investigations. None of these changes are reflected in the Directive or in any interim guidance issued by OM.

[6] See Appendix C for updated OPM investigation and reinvestigation requirements.

We also found that the Directive was not updated to reflect changes in Department requirements and practices for the security screening process that were implemented after the Directive was issued in July 2010. For example, in August 2010, OPM recommended that agencies requesting OPM investigations use the Position Designation Tool. The former Director of the Office of Security, Facilities, and Logistics Services stated that in 2014, OM began requiring Department staff to use the Position Designation Tool to designate contract positions and risks.[7] He did not provide any evidence of dissemination of this requirement to Department staff. The current Director of Personnel Security was unsure of the effective date of the Position Designation Tool requirement. We noted that OM's requirement for use of the Position Designation Tool is not reflected in the Directive or in any issued interim guidance, and it conflicts with the Directive requirement to use the Position Designation Record that is included as an appendix to the Directive.[8] We also found that the Department established an abbreviated security screening process for contractor employees who will work on a contract for more than 30 days but fewer than 90 days. OM allows these contractor employees, referred to as "short-term" contractor employees, to forego the normal security screening process and to instead receive a special agreement check, which is an abbreviated security screening. OPM permits agencies to forego the normal security screening process in some cases, as long as the agency conducts appropriate checks (such as the short-term screening process the Department uses) to ensure contractor employee suitability.[9] The Department's special agreement check process is allowable, but not addressed in the Directive or any other written interim guidance.

The Director of Personnel Security, along with the former Director of Personnel Security and former Director of the Office of Security, Facilities, and Logistics Services, confirmed that OM considers most of the Directive to be outdated and not reflective of current government requirements. Other Department officials involved in the process agreed, adding that the Directive does not reflect the actual responsibilities of some PO staff. For example, the Directive includes requirements for Office of the Chief Financial Officer

[7] Position designation assesses duties and responsibilities of a position to determine the potential damage resulting from the misconduct of an individual occupying the position. Designating positions using the Position Designation Tool determines the level of investigative vetting required for a position.

[8] See Appendix D for the Position Designation Record included in the Directive.

[9] Code of Federal Regulations Title 5, Section 731.104(c) states that positions that are not to exceed an aggregate of 180 days per year in either a single continuous appointment or series of appointments, do not require a background investigation; however, an agency must conduct such checks as it deems appropriate to ensure the suitability of the person.

(OCFO) officials and staff, such as ensuring security screening requirements are included in solicitations and contracts, ensuring that contractor employees are screened in a timely manner, and notifying contractor companies if a contractor employee is deemed not acceptable for employment on a contract. OCFO's former Enterprise Procurement Initiatives Director stated OCFO recommended that the Directive be updated to reflect actual business practices and the division of responsibility between OM and contracting officials. The former Senior Procurement Executive stated that the Directive is long overdue for an update to language specific to OCFO responsibilities. He explained that the language in the Directive is not clear with regard to current security screening process requirements and is not detailed enough to describe the appropriate roles for OCFO staff involved in the process to ensure appropriate contract monitoring takes place. He noted that aligning current contract review procedures with the Directive would ensure consistency and decrease any confusion in the screening process for responsible staff.

The Director of Personnel Security noted that for some areas, such as new requirements for granting access to Department IT systems, OM is currently working with the Office of the Chief Information Officer to develop interim guidance to supplement the Directive. Similarly, OM is working with OCFO to clarify COR responsibilities and contract requirements. We noted that in April 2018, OM submitted a draft of an updated version of the Directive to the Department's administrative control system document review process.

Principle 12.02 of the Government Accountability Office's Standards for Internal Control in the Federal Government, dated September 2014, states that management should document in policies the internal control responsibilities of the organization. In addition, Principle 12.03 states that management should document in policies for each unit its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness. Principle 12.05 adds that management should periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately.

The OM Personnel Security Functional Statement states that Personnel Security develops policies, procedures, and guidelines for the personnel security functions in accordance with applicable Federal laws, regulations, and Executive Orders and ensures each individual's employment will promote the efficiency of the service and is consistent with the public trust and national security interest. In addition, Section VI, Part D.1 of

the Directive states that the Chief of Personnel Security provides oversight and guidance for all matters relative to the Directive's policies and procedures.

OM appears not to have prioritized updating written policies as long as OPM processing requirements were being met. For example, the former Director of Personnel Security noted that because OPM will not accept investigation requests without required information, the Department has to provide the necessary information to OPM even though written policies were not updated to match those requirements. He also noted that OM has had trouble keeping up with OPM's changing investigation policy requirements and that the Directive would need to be updated every 6 months in order to keep up with OPM's requirements.

The Director of Personnel Security stated that in some cases OM communicates information directly to PO staff in certain offices because they have the greatest number of contractor employees to process. She noted that she generally does not need to share related information with other POs because they are not processing that many contractor employees.

The lack of updated written policies and guidance may hinder the Department's ability to effectively implement all of the requirements for the contractor personnel security screening process, to include ensuring key staff involved in the security screening process are aware of their expected responsibilities, ensuring consistency in PO processes, and ensuring compliance with government-wide policies. For example, during our reviews of the two POs included in this audit, we found that the Position Designation Tool was either not being used because staff were unaware of it, or if it was used, it was not being used correctly as not all contract positions were included.

Compliance with Policies and Procedures

We found that OM did not comply with Directive requirements in several areas, to include ensuring POs submitted to OM PO-specific procedures for complying with the Directive; providing notice to POs of final adjudication determinations; and coordinating with POs with regard to contract position and risk designation.

PO-Specific Procedures

We found that OM did not ensure that POs submitted to OM PO-specific procedures for complying with the Directive. The Directive states that each PO must establish and maintain on file with OM its own procedural document for complying with the Directive. The former Director of the Office of Security, Facilities, and Logistics Services said that OM had some PO procedures on file but not all of them. When asked to provide the PO procedures it had on file, OM provided documents for only two POs. However, neither

of the documents were PO-specific procedures. Both of the documents provided were actually memoranda from OM to the POs outlining general screening requirements. The current Director of Personnel Security stated that OM does not maintain or review PO-created procedures. During the course of our audit, we noted that one PO did provide OM with its own procedural document for review; however, over 1 year later, OM still had not reviewed the document or provided feedback to the PO.

Section VI, Part A.1 of the Directive states that each PO must establish and maintain on file with the Chief of Personnel Security, its own procedural document for complying with the Directive. The document will identify the responsible officials such as CORs, Computer Security Officers, or System Security Officers within the PO who will be performing key duties. Each PO must include in its procedures the requirements for screening contractor employees serving 30 calendar days or more on a Department contract or project provided they meet certain conditions such as requiring access to Department IT systems or unclassified sensitive information. All modifications to the PO procedures document must be forwarded to the Chief of Personnel Security for review.

OM officials provided different explanations for why OM did not maintain PO procedures. The Director of Personnel Security stated that OM did not require POs to submit internal policies and procedures to comply with the Directive because OM did not have the resources to enforce the requirement. She also noted that she would like the updated Directive to be more comprehensive and to eliminate the need for POs to establish their own policies and procedures. Contrary to what the Directive states, the previous Director of Personnel Security stated that there is no requirement for POs to file internal procedures with OM and that OM does not need to approve the PO procedures. Finally, the former Director of the Office of Security, Facilities, and Logistics Services stated that not all POs employed enough contractors that they were required to provide OM internal procedures. However, the Directive does not specify a threshold for when POs must provide the procedural document.

OM's failure to ensure POs submit internal procedures for the screening process and failure to review changes to such procedures can result in POs having no or inadequate detailed procedures for this process. Staff may not be aware of or adequately understand their roles and responsibilities within the process and contractor screening requirements may not be appropriately implemented.

The two POs included in this audit provided us with procedures they had prepared related to the screening process. Our review of the procedures noted that neither document fulfilled all Directive requirements. Specifically, the documents did not identify all key officials involved in the contractor personnel security screening process and did not explain requirements for the screening process such as the contract position and risk designation process and the contractor employee screening information that

should be maintained. We found that PO officials and staff did not appear to be familiar with their expected roles in the security screening process or be aware of specific requirements from the Directive, and there was resulting confusion over who was responsible for different parts of the process. For example, one COR said that she did not know who was responsible for determining and approving position risk levels for her contract in her PO or why specific risk designations had been made.

We determined that one PO did not develop adequate procedures with regard to contractor access to IT systems or Department-sensitive or Privacy-Act protected information, which led to contractor employees being inappropriately granted access.

Notification of Adjudication Determinations

We found that OM does not notify POs of all contractor employees' final adjudication determinations as required by the Directive. OM officials confirmed that OM does not notify POs of favorable adjudication determinations and stated that OM has an agreement with POs that if PO staff do not receive adjudication results from OM during the security screening process for a particular contractor employee, then the PO should assume that everything is acceptable with the security screening. OM officials noted that if there is an unfavorable adjudication determination, OM will notify the COR and Contracting Officer for the contract by sending an email with an official letter attached.

Section VI, Part D.8 of the Directive states that the Chief of Personnel Security will forward notification or verification of a personnel security adjudication determination for contractor employees to the COR for distribution to the Contracting Officer, Computer Security Officer, and/or the System Security Officer.

In addition, Section VI, Part A.8 of the Directive notes that each COR must notify the contractor company of the personnel security adjudication determination and maintain a copy of the determination. Section VI, Part A.9 notes that each PO must maintain the date of the final personnel security screening determination for each contractor employee.

The Director of Personnel Security stated that OM used to send hard copy certificates of investigation to communicate the results of completed and favorably adjudicated investigations for individual contractor employees. However, OM stopped sending these notifications since PO staff said they did not find them useful and did not know what to do with them. The Director of Personnel Security is unaware of the timeline in which the certificates were no longer sent to PO staff because it was before she joined the Department. Similarly, the Security Manager System Manager stated that OM previously used a feature of Security Manager that allowed the system to send out emails communicating a final adjudication determination to PO staff. Again, OM discontinued

use of this feature because of the volume of emails being produced. The Director of Personnel Security stated that the current configuration of Security Manager does not permit direct emails to PO staff.

In addition to not sending determinations for individual contractor employees, the Director of Personnel Security confirmed that Security Manager is not currently configured to generate reports that list batches of contractor employees, such as by contract or PO, that have had cases adjudicated within a certain timeframe. She noted that OM intends to work with the Security Manager contractor to develop this feature.

We found that POs were generally unaware of adjudication determinations and did not maintain documentation or inform applicable individuals as required. Multiple staff in the POs we reviewed noted that the lack of adjudication notification from OM is a weakness in the security screening process. We reviewed 123 contractor employees that had security screenings initiated from the two POs included in this audit and found that 30 (24 percent) either did not have a completed investigation, had an investigation completed at a lower risk level than required, or had an investigation that had not been adjudicated by OM.[10] Without notification of all adjudication determinations, POs may incorrectly assume contractors have been favorably adjudicated and allow them to work indefinitely without a completed or appropriate screening.

Designation of Contract Positions and Position Risk Levels

We found that OM did not participate in the contract position and risk designation process as required by the Directive. The Director of Personnel Security confirmed that OM is not involved in this process. Furthermore, neither of the two POs included in our review identified a role for the Director of Personnel Security in the risk designation process when explaining their processes and there was no role identified in their internal procedures.

Section VI, Parts A.3 - A.4 of the Directive state that a PO must assign a position risk level to each applicable contractor employee position, before the solicitation is released, in coordination with the Computer Security Officer and the Chief of Personnel Security.

[10] The contractor employees did not have final adjudication determinations from OM because cases were inadvertently left incomplete by OM or OM may not have intended to adjudicate the case, such as for special agreement checks. In other cases, OM could not provide an adequate explanation for why there was no final adjudication determination.

The Director of Personnel Security stated that OM does not participate in the contract position and risk designation process because OM staff do not know the responsibilities of a given contract position and that CORs are responsible for contract position and risk designation. She also stated that OM is only involved with the position and risk designation process for employees and not for contractors unless the COR asks for OM's assistance, which is uncommon. She further explained that sometimes OM notices a position that should have been designated as a High Risk level position and will notify the COR.

OM's failure to participate in or oversee the contract position and risk designation process may have contributed to PO processes that did not adequately fulfill Directive requirements. We identified significant issues with the contract position and risk designation processes in the two POs we reviewed. Specifically, we found that the POs did not:

- involve all required staff and officials in the process;
- develop complete position lists for each contract;
- assign risk levels for each position;
- document position and risk determinations using Position Designation Records or the Position Designation Tool; or
- ensure that the actual positions and risk levels assigned to individual contractor employees corresponded to the positions and risk levels designated in contract solicitations and final approved contracts.

Both POs appeared to heavily rely on their contractors for determining contract positions and appropriate risk levels without any further review of the adequacy of these determinations. Without appropriate oversight of the position risk level designation process, to include appropriate documented approvals of the actual positions and risk levels assigned, the Department has little assurance that the risk levels assigned to the positions are appropriate for the position responsibilities or correspond to risk levels assigned to similar positions and the Department may not be able to ensure that contract employees are receiving the appropriate security screenings.

Timeliness of Security Screening Activities

We found that OM did not ensure that all stages of the security screening process were completed within required timeframes. Specifically, the following elements of the security screening process exceeded established timeframes:

- Security screening initiations
- Adjudications
- Reinvestigations

Security Screening Initiations

OM is primarily responsible for initiating security screenings with OPM for all non-FSA contractor employees and High Risk FSA contractor employees. OPM recommends security screenings to be initiated with OPM within 14 days of the date that the contractor employee certifies the e-QIP forms. In addition, OPM recommends agencies maintain a less than 5 percent rejection rate for security screening initiations.[11]

We reviewed aggregate information from OPM Quality and Timeliness Reports for the time period from October 2016 to April 2018 to determine the timeliness of the Department's security screening initiations with OPM as well as the associated rejection rates. The OPM Quality and Timeliness reports, which cover both Department employees and contractor employees, indicate that the average time between an employee's or contractor employee's certification in e-QIP to the date of receipt of a complete and accurate investigative request at OPM ranged from a high of 91 days in February 2017 to a low of 36 days in April 2018. While we noted that the Department has kept rejection rates at or below 5 percent since November 2017, the Department is not averaging submission timelines at or below 14 days.[12] However, the Department has steadily decreased the average submission time for initiation of security screenings with OPM over the past several months. Table 1 shows the average e-QIP submission timeliness and the percentage of e-QIP submissions returned as unacceptable for the time period from October 2016 to April 2018.

[11] OPM returns a case as unacceptable when requested information is not returned to OPM within the required time. The case is then marked as unacceptable by OPM and a new e-QIP package submission is required.

[12] The OPM Quality and Timeliness Reports do not contain any specific information regarding the percentage of e-QIP submissions that were submitted within 14 days.

Table 1. E-QIP Submission Average Timeliness[13] and Rejection Rates

Month Received by OPM	Average Submission Timeliness (Days)	Percentage of e-QIP Submissions Returned as Unacceptable
10/2016	55	9%
11/2016	62	8%
12/2016	75	8%
01/2017	78	12%
02/2017	91	14%
03/2017	86	16%
04/2017	90	6%
05/2017	74	7%
06/2017	78	6%
07/2017	82	6%
08/2017	73	4%
09/2017	56	5%
10/2017	65	6%
11/2017	55	5%
12/2017	52	4%
01/2018	41	3%
02/2018	41	4%
03/2018	38	5%
04/2018	36	5%

[13] The submission timeliness calculations exclude special agreement checks, cases that had to be reopened, and cases rejected as unacceptable by OPM.

Section VI, Part D.2 of the Directive states that the Chief of Personnel Security will receive, process, and forward contractor employees' forms to the investigating agency as necessary. The investigating agency may be a Federal agency or individual contractor.

The OPM Human Capital Management Hiring Reform Security and Suitability metrics state that there are a few metrics managers and Human Resources Offices can use to measure the success of the Security and Suitability process, to include submission timeliness reduced to 14 days or less with less than a 5 percent rejection rate.

The Directive requires POs to submit a contractor employee's security screening package to OM within 14 days of the date the contractor employee is placed in a non-High Risk position. We note, however, that OPM's 14-day metric asks for agencies to initiate a security screening with OPM within 14 days of the e-QIP form's certification. OPM's 14-day metric for security screening initiation is not included in the Directive. Additionally, OM's 14-day initiation requirement that is referenced in the Directive is not aligned with the OPM metric. As required by the Directive, PO staff should attempt to initiate a security screening with OM within 14 days of a contractor employee's assignment to a contract and not necessarily with OPM within 14 days of a contractor employee's e-QIP certification. PO staff may be unaware of the OPM initiation metric and the differences between the Directive and OPM metric may result in delays in initiating security screenings with OPM.

In addition, the Director of Personnel Security stated that backlogs in adjudications and reinvestigations negatively impact OM's ability to ensure that the 14-day initiation timeline is met.

Adjudications

OPM requires OM to report the results of a contractor employee's adjudication within 90 days of receiving the results of the background investigation from OPM and suggests that agencies strive to adjudicate 90 percent of cases within 20 days. We determined that within our sample of 205 contractor employees, there were 131 contractor employees who had background investigation results returned by OPM.[14] We reviewed Security Manager records for these 131 contractor employees to evaluate adjudication timeframes. We found that OM did not consistently maintain the date adjudication results were sent to OPM for individual contractor employees. Therefore, we could not determine whether OM reported adjudication results to OPM within 90 days as

[14] We excluded contractor employees with special agreement checks from this review because these cases are generally not adjudicated.

required. However, to evaluate timeliness, we compared the date OPM returned the investigation results to OM to the date OM made the adjudication determination for the 131 contractor employees to determine whether OM adjudicated cases within 20 days and within 90 days. We found that 74 of the 131 cases (56 percent) were adjudicated in 20 days or less and 97 of the 131 cases (74 percent) were adjudicated within 90 days. Overall, we found the following adjudication timeframes for the 131 cases:

- 74 cases (56 percent) took 20 days or less;
- 23 cases (18 percent) took between 20 days and 90 days;
- 11 cases (8 percent) took between 90 days and 6 months;
- 7 cases (5 percent) took between 6 and 9 months;
- 2 cases (2 percent) took between 9 and 12 months; and
- 9 cases (7 percent) took over 12 months.

For five cases (4 percent), OPM returned background investigation results but OM had not made any adjudication decisions at the time of our review. Four of these five cases had been open between 7 and 8 years according to data in Security Manager.

In addition, we reviewed aggregate Security Manager data to determine the number of cases that took longer than 90 days to adjudicate.[15] We found that OM exceeded this timeframe for 791 (51 percent) of 1,537 cases. Adjudication dates ranged from 91 days to 600 days after OPM returned investigation results with a median of 181 days.

We also reviewed aggregate Security Manager data to the determine length of time that adjudications have been pending for contractor employees that OM considers to be active. We identified 5,423 active contractor employee positions in Security Manager with at least one adjudication pending. As of June 12, 2018, these adjudications had been pending from 18 days to 3,840 days (over 10 years) with a median of 402 days.

The OPM Human Capital Management Hiring Reform Security and Suitability metrics state that there are a few metrics managers and Human Resources Offices can use to measure the success of the Security and Suitability process. One metric includes aligning the adjudication process to allow for the timeliness of 90 percent of cases within 20 days.

[15] We reviewed cases where OPM returned background investigation results to OM between October 1, 2016, and December 31, 2017.

Code of Federal Regulations Title 5, Section 732.302 (b) states that in accordance with section 14(c) of Executive Order 10450, agencies shall report to OPM the action taken with respect to individuals investigated pursuant to Executive Order 10450 as soon as possible and in no event later than 90 days after receipt of the final report of investigation.

OM's Supervisory Personnel Security Specialist said that OM's ideal internal timeline for final adjudication would be within 30 days after receiving the closed case from OPM, but with the extensive backlog and shortage of personnel, OM is unable to meet that timeline. In general, there is a lot of variability in the length of time that it takes OM to adjudicate an individual case. For example, if there are no issues, a case can be adjudicated within an hour. If there are major issues in a case, the adjudicator has to do more work on the case such as reaching out to the COR who has to contact the contractor employee informing him or her to contact OM in order to provide additional information. Contractor employees are given 10 days to contact OM, but depending on how long it takes the contractor employee to obtain the information requested by OM, the process could take weeks. She noted that there are some cases that have been pending adjudication since June 2016 due to ongoing attempts to work with individuals to obtain required information. Additionally, the number of cases OM must adjudicate within any given month can range from 20 cases to over 100 cases per adjudicator depending on how many cases OPM returns in the timeframe.[16]

The former Director of Personnel Security stated that workload continues to increase for the same amount of workers, and backlogs will happen if more people are not hired to handle processing needs. OM officials stated that as of February 2018, there was a backlog of approximately 5,400 security screening cases to be adjudicated for both employees and contractor employees.

OM has six staff qualified as adjudicators; however, four of the six staff are assisting with a backlog of reinvestigations and other day-to-day office requirements such as customer service, personal identity verification card requests, and e-QIP initiations. Therefore, OM has only two staff devoted full time to adjudications. OM officials have noted that one way to address the backlog of adjudications would be to hire additional staff, and added that OM is in the process of hiring nine more employees for Personnel Security.

[16] Adjudicators process cases for both employees and contractor employees.

Reinvestigations

OPM requires reinvestigations every 5 years for contractor employees in Moderate and High Risk public trust positions and the Directive requires OM to coordinate with POs when a reinvestigation is due. We identified 28 contractor employees in Moderate and High Risk positions who were required to have a reinvestigation in our sample of 205 PO contractor employees.[17] We found that 17 of these contractor employees (61 percent) had a reinvestigation initiated on or before their reinvestigation due date.[18] One contractor employee (4 percent) had a reinvestigation initiated approximately 6 months after the due date. The remaining 10 contractor employees (36 percent) did not have a reinvestigation initiated and were listed as active in Security Manager at the time of our review. The reinvestigations have been pending from less than 6 months to more than 4 years, with a median of 2 years.

Code of Federal Regulations Title 5, Section 731.106(b) states that positions at the High or Moderate risk levels would normally be designated as public trust positions. Section 731.106(d) states that agencies must ensure that reinvestigations are conducted and a determination made regarding continued employment of persons occupying public trust positions at least once every 5 years.

Section VI, Part A.5 of the Directive states that contractor employees occupying High Risk level IT positions must undergo reinvestigation every 5 years for the duration of their contract at the Department, or if there is a break-in-service to a Department contract of 365 days or more. In addition, Section VI, Part D.9 of the Directive states that the Chief of Personnel Security will coordinate with the Principal Office COR when contractor employees require periodic screenings at five-year intervals.

The Director of Personnel Security stated that as of February 2018, the Department had a backlog of approximately 13,000 contractor employees who required reinvestigations. She noted that many of the backlogged cases are most likely for contractor employees who are no longer employed with the Department. Security Manager includes an unknown number of contractor employees who are no longer employed with the Department. To address this issue, OM sent POs lists of contractor employees from

[17] There were 6 contractor employees in Moderate Risk positions and 22 contractor employees in High Risk positions from our sample who were listed in Security Manager as due for a reinvestigation.

[18] The reinvestigation due date is 5 years from the date the initial background investigation was closed by OPM.

Security Manager to determine which contractor employees are still employed at the Department.

Overall, if OM does not ensure that all stages of the security screening process are completed within required timeframes, contractor employees may be permitted to work on Department contracts for extended periods of time with no assurance that they are suitable for the access granted. Specifically, we found that security screenings and reinvestigations were not always initiated and adjudicated timely. For example, we determined that 191 of 205 contractor employees in our sample were required to have a security screening. We found that 131 of these contractor employees (69 percent) were permitted to work on their contracts without an appropriate security screening for the following periods:[19]

- 75 (57 percent) for less than 1 year;
- 13 (10 percent) between 1 year and 2 years;
- 9 (7 percent) between 2 and 3 years; and
- 27 (21 percent) for more than 3 years.

Maintenance of Security Screening Information

We found that OM did not ensure that the contractor employee data maintained in Security Manager was accurate and reliable. Specifically, we found discrepancies between the information in Security Manager and the information maintained by POs, missing information in key data fields, and inaccurate information. OM uses Security Manager for processing and tracking contractor personnel security screenings and according to OM officials, Security Manager contains all related data and information. OM uses Security Manager to conduct all aspects of the security screening process including documentation review and maintenance, adjudication of OPM background investigation information, and tracking reinvestigations. According to the former Director of the Office of Security, Facilities, and Logistics Services, all information related to personnel security has been stored in Security Manager since December 2012.

We noted discrepancies between PO records and Security Manager data for information including contractor employee names, contractor companies, assigned contracts, and position risk levels. For example, we identified contractor employees listed in PO

[19] We were unable to determine the time spent on the contract without an appropriate security screening for 7 of the 131 (5 percent) contractor employees.

records with one name and listed in Security Manager under a different name such as a maiden name or alias.

We also found that certain key data elements in Security Manager were generally missing for individual contractor employees such as the contractor company, the assigned contract number, and the date the contractor employee departed the contract (when applicable). These data elements would be particularly useful for tracking groups of contractor employees assigned to specific contracts and determining whether contractor employees are still working on Department contracts. We reviewed Security Manager records to determine the frequency with which the contractor employee records were missing assigned contractor companies and contract numbers. We found that of the 48,286 total contractor employee records in Security Manager at the time of our review, 14,436 records (30 percent) did not have a contractor company assigned and 48,269 (99.9 percent) did not have a contract number assigned.[20]

We also found that certain data fields in Security Manager are generally unreliable, particularly the data related to employment status. We noted that POs do not always update OM when contractor employees depart from their contracts. Therefore, there are numerous contractor employees in Security Manager classified as actively employed by the Department that have already separated from the Department or ended their contract work under a particular contract. This issue has significant repercussions on the quality of the data in Security Manager.

Section VI, Part D.1 of the Directive states that the Chief of Personnel Security provides oversight and guidance for all matters relative to these policies and procedures.

Principle 11.09 of the Government Accountability Office's Standards for Internal Control in the Federal Government states that management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Principle 13.01 states that management should use quality information to achieve the entity's objectives. Principle 13.05 notes that quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

[20]The numbers reflect the number of records in Security Manager at the time of our review and not the total number of contractor employees at that time. A contractor employee could have multiple records in Security Manager with different assigned contractor company names and contract numbers.

Discrepancies between the information maintained by POs and the information maintained in Security Manager may be due to the fact that PO information is provided by contractor companies and maintained by CORs while information in Security Manager is generally taken from e-QIP and input by OM staff or by PO staff other than CORs. If differences exist between information provided on the e-QIP form and information provided by the contractor company, it may go unnoticed. We found that CORs generally do not have access to Security Manager to review information for individual contractor employees. In fact, access to Security Manager is limited to only a few staff within a PO and for some POs, no employees have been given access to the system. The Director of Personnel Security stated that PO access to Security Manager is restricted due to the sensitivity of Security Manager data and the limited number of licenses available for use of the system. The former Director of the Office of Security, Facilities, and Logistics Services noted that some reconciliation issues between PO records and Security Manager records may be due to formatting issues and data entry errors such as extra digits in social security numbers.

Missing data in key fields can generally be attributed to the fact that OM does not require certain data fields to be filled in when completing a contractor employee's profile in Security Manager. While data such as first and last names and social security numbers are required, data fields such as contractor company and contract number are not. The former Director of the Office of Security, Facilities, and Logistics Services confirmed that information in Security Manager such as a contractor employee's assigned contract number is unreliable. He noted that OM has not always collected contract information such as contractor companies and contract numbers from POs. He said that this information was previously inconsistently collected and that at times, PO staff would provide incorrect contract numbers.

We asked OM whether Security Manager could be configured to require certain information such as contract number to complete a profile for a contractor employee. The Director of Personnel Security stated that the system could be configured to require this information; however, OM users currently do not have access to this type of information and it is unavailable through e-QIP. OM would have to first require that PO staff provide the contract number to OM staff in cases where OM directly inputs information for contractor employees.

Other inaccurate and unreliable information in Security Manager such as employment status is due to a failure of POs to provide up-to-date information to OM or to independently update Security Manager. Most information on contractor employees, such as departures from the contract, is sent by contractor companies to PO staff and then POs provide the information to OM. When contractor companies and POs do not provide OM this information, OM has no way of knowing the status of an individual

contractor employee's employment to update Security Manager. The Director of Personnel Security stated that in order to address this issue, in February and April 2018, OM provided POs with lists of all contractor employees assigned to their contracts according to Security Manager data and requested that the POs indicate whether the contractor employees are still employed on the POs' contracts or whether they have departed the contracts.

We reviewed the responses provided by 12 of the POs.[21] We compared the number of contractor employees assigned to each PO in Security Manager (as determined by OM) to the number of contractor employees classified as actively employed on a PO contract as determined by each PO. We found that of the 30,692 contractor employees assigned to the 12 POs in Security Manager, the POs determined that only 4,457 (15 percent) of these contractor employees are actively assigned to their contracts. For the remaining 26,235 contractor employees (85 percent), the POs classified them as inactive or departed, could not locate them in internal records, could not determine the contractor employees' employment status, or determined that the contractor employees may be assigned to a different PO's contracts.

Overall, the lack of quality data in Security Manager may impact OM's ability to effectively oversee the contractor personnel security screening process and may affect a PO's ability to complete various activities for the security screening process. Limited PO access to Security Manager may prevent POs from ensuring the accuracy of contractor employee information maintained in the system. Discrepancies between PO records and Security Manager data may cause problems for PO staff attempting to track a contractor employee's security screening status. PO staff noted that they do not always have access to personally identifiable information, such as social security numbers, for contractor employees. Therefore, if PO staff want to verify the security screening status of a contractor employee in Security Manager, they may be unable to locate the contractor employee records if the contractor employee names in the PO records and Security Manager are not an exact match. In addition, missing data in key data fields may inhibit OM's ability to assist POs with tracking security screenings such as providing PO staff with adjudication reports based on contract number. The Director of Personnel Security noted that when contractor employees are incorrectly listed in Security Manager as actively employed on a Department contract when they are not, OM may waste money by continuing OPM investigations that could be discontinued. Additionally, OM may waste time attempting to contact departed contractor employees

[21] At the time of our review, OM had not received complete lists of active contractor employees from 8 additional POs, including the PO with the largest number of contractor employees.

for screening initiations or adjudications. Without accurate information, OM is unable to determine the number of contractor employees actively employed on Department contracts or determine where contractor employees are working.

Training Provided to Staff

We found that OM does not provide PO staff with adequate training on the contractor personnel security screening process and related requirements, to include use of Security Manager. The former Director of the Office of Security, Facilities, and Logistics Services noted that there is no specific Department training related to the contractor security screening process and that even for OM staff, training is on-the-job. The Director of Personnel Security acknowledged that Department staff do not currently adhere to all of the requirements of the Directive. We found that although OM was aware that POs were not in compliance with a number of key requirements in the Directive, it has taken limited action to ensure POs understand and implement those requirements.

The Director of Personnel Security worked with OCFO's Contracts and Acquisitions Management division to provide a training course for CORs in May 2017 on aspects of the security screening process, but CORs were not required to attend. She also stated that OM recently provided an in-person training to staff in one PO on elements of the screening process such as use of Security Manager. However, as with the May 2017 training, the PO training was not required for CORs or other staff involved in the contractor personnel security screening process.

Section VI, Part D.1 of the Directive states that the Chief of Personnel Security provides oversight and guidance for all matters relative to these policies and procedures.

The Director of Personnel Security stated that she did not want to develop training until the updated Directive is finalized so that staff can learn the new procedures. She noted that OM intends to develop a PowerPoint training to supplement the in-person training once the updated Directive has been finalized. She also stated that OM is working with Contracts and Acquisitions Management to amend the COR Delegation and Appointment Memorandum to ensure CORs better understand their role in the contractor security training process. She noted that OM has not provided any specific training on use of the Position Designation Tool to PO staff because OPM offers a free training course on the tool and OM is not an authorized trainer.

In both POs included as part of this audit, we found that staff and officials involved in the process were generally unaware of Department requirements and their related responsibilities for processing contractor employees' security screenings. Of the 191 contractor employees reviewed in these POs that were required to have a screening, we

identified 66 (35 percent) that did not have evidence of an appropriate screening. We found that the POs did not maintain required information for any of the 10 contracts we reviewed and instead relied on contractor companies to maintain contractor employee information. We also noted that one PO was not always denying contractor employees High Risk level access to IT systems or the Department's sensitive or Privacy Act-protected information prior to preliminary personnel security screenings being completed favorably, as required by the Directive.

If OM does not provide training to PO staff on the contractor personnel security screening process, OM lessens assurance that POs are aware of and understand the requirements of the Directive and the importance of compliance with these requirements. This may lead to a lack of consistency in the process amongst POs, and ultimately a lack of effectiveness of the screening process Department-wide.

Recommendations

We recommend that the Assistant Secretary for Management:

1.1 Develop and distribute written policies and procedures that include (1) new Federal and Department requirements for the contractor personnel security screening process established since the issuance of the Directive in 2010, and (2) existing Department practices for the screening process that have been informally approved by OM but are not addressed in current written policies and procedures.

1.2 Periodically review the security screening process and assess the need to update policy accordingly. Develop and distribute interim guidance as necessary.

1.3 Require POs to develop internal procedures for the contractor personnel security screening process, review the PO-developed procedures for compliance with the Directive, review any modifications to PO procedures, and maintain the procedural documents provided by POs.

1.4 Develop a process to ensure POs receive and maintain notification of all final adjudication determinations, both favorable and unfavorable, for each individual contractor employee who has received a security screening.

1.5 Establish an appropriate role for OM in the contract position and risk designation process, in coordination with PO and OCFO staff, and ensure requirements for position risk designation tools and documentation requirements are adequately communicated.

1.6 Ensure that all elements of the security screening process, including initiation, adjudications, and reinvestigations are conducted within required timeframes. Align Directive requirements with applicable OPM metrics.

1.7 Review the staff structure and resources of Personnel Security and make changes, as appropriate, to ensure timely processing of security screenings and that proper oversight and guidance of the Department's contractor personnel security screening process is provided.

1.8 Coordinate with POs to reconcile current Security Manager data with PO records on individual contractor employees for information such as contractor employee name, contractor company, assigned contract number, employment status, and departure date as applicable. Periodically reconcile Security Manager data with PO records.

1.9 Require information necessary for tracking the status of contractor employees' security screenings and employment on Department contracts to be entered into Security Manager, to include contractor company and contract number.

1.10 Review the current access of PO staff to Security Manager to determine if granting further access to key staff could help ensure the reliability of Security Manager data, and then grant access accordingly.

1.11 Develop comprehensive training for the contractor personnel security screening process that covers process requirements and the responsibilities of key PO officials and staff, to include use of Security Manager and the Position Designation Tool. Require all applicable staff to attend.

OM Comments

OM did not disagree with the finding or recommendations and noted that many of the audit recommendations have been implemented or are in the process of being implemented. In particular, OM stated that guidance, entitled *Interim Personnel Security Requirements and Guidance to Support Access to Department Information, Information Systems, and Facilities,* was signed for release on August 22, 2018, and that an updated Directive is currently in the agency clearance process. In addition, OM stated that it has developed a notification process to alert POs of favorable and unfavorable adjudication determinations for each contractor employee, has hired additional staff to help reduce lead times associated with the screening process, and is working with all internal and external stakeholders to update the information included in Security Manager.

OIG Response

OM's comments were responsive to the recommendations. We did not make any substantive changes to the finding or recommendations as a result of OM's comments.

Appendix A. Scope and Methodology

To answer our objective, we gained an understanding of internal controls applicable to the Department's contractor personnel security screening process at OM. We reviewed applicable laws and regulations, OM and PO policies and procedures, and the Government Accountability Office's "Standards for Internal Control in the Federal Government." In addition, to identify potential vulnerabilities, we reviewed prior OIG, Government Accountability Office, and other Federal agencies' audit reports with relevance to our audit objective. We also reviewed applicable OPM management reports regarding Department security screening timeliness.

We conducted discussions with OM management and staff involved in the contractor personnel security screening process. These discussions focused on OM policies, procedures, standard practices, tools, and systems for conducting contractor personnel security screenings and for providing oversight of the Department' security screening process. In addition, we conducted discussions with applicable officials and staff from OCFO, IES, and FSA regarding their coordination with OM during the contractor personnel security screening process.

The scope of our audit included reviews of the contractor security screening process within two POs. POs were selected based on a listing of Department contracts that were active as of December 16, 2015, obtained from the Department's publically available website. As this information was used primarily for informational purposes and did not materially affect the findings and resulting conclusions noted in this report, we did not assess its reliability. We selected IES for review as it represented the PO with the highest number of active contracts (204 or 36 percent) and highest overall contract dollar value ($1.6 billion or 49 percent). We selected FSA for review as it represented a significant number (125 or 22 percent) and dollar value ($763 million or 24 percent) of active contracts and because FSA contracts involve IT systems that access a considerable amount of sensitive personally identifiable information and have a considerable number of contractor employees requiring screenings at the High Risk level. A listing of the contracts selected for review and the applicable contract dollar value is included as Appendix B.

Sampling Methodology

To determine whether contractor employees received appropriate security screenings, we judgmentally selected 5 contracts from each PO as noted above and reviewed applicable documentation for random samples of contractor employees from each of the contracts. In total, we reviewed 205 contractor employees out of a total of 10,357 from the 10 contracts selected.

For each selected contractor employee, we evaluated PO records and Security Manager data to determine whether security screenings were completed at the appropriate risk level, adjudication determinations were documented, and security screenings were processed in a timely manner. We also reviewed applicable contract position risk level documentation to determine designated contractor employee positions and risk levels.

Because we did not weight the sample results by their probabilities of selection, the percentages reported in this audit are not statistical estimates and should not be projected over the unsampled contractor employees.

Use of Computer-Processed Data

We relied on computer-processed data obtained from Security Manager to determine whether appropriate security screenings had been initiated and adjudicated by OM for the contractor employees in our sample. We reconciled data in Security Manager with information provided by POs, to include dates of security screening activities, contractor employee employment statuses, background investigation levels, and adjudication information. We noted issues with the data provided by POs and contractor companies that limited our ability to reconcile the data, to include discrepancies between the listings of contractor employees provided. In addition, the information provided by POs and contractor companies did not always include all required data. Because source data for some of this information is located at the individual contractor sites, our ability to perform an assessment of the information was limited, and as such, we could not fully determine the reliability of the data. However, despite these limitations, we believe the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objective. Specifically, the limitations noted did not impact our ability to assess whether the Department implemented the requirements for the contractor employee security screening process.

We conducted fieldwork at Department offices in Washington, DC, during the period December 2015 through June 2018. We provided our audit results to Department officials during an exit conference conducted on June 28, 2018.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B: Contracts Reviewed in this Audit

Table 2 identifies the IES and FSA contracts reviewed in this audit and the dollar value of each contract at the time it was selected for review.

Table 2. Contracts Reviewed in this Audit

No.	PO	Contractor Company	Contract Number	Contract Value[22]	Award Date
1	IES	American Institutes for Research in the Behavioral Sciences	ED-IES-12-D-0002	$200,000,000	12/15/2011
2	IES	Westat, Inc.	ED-IES-13-C-0019	$114,491,562	3/7/2013
3	IES	Educational Testing Service	ED-IES-13-C-0017	$54,104,015	3/7/2013
4	IES	NCS Pearson, Inc.	ED-IES-13-C-0021	$47,212,984	3/7/2013
5	IES	Research Triangle Institute	ED-05-CO-0033	$46,852,191	9/30/2005
6	FSA	Great Lakes Educational Loan Services, Inc.	ED-FSA-09-D-0012	$204,962,248	6/17/2009
7	FSA	Navient, LLC	ED-FSA-09-D-0015	$200,511,082	6/17/2009
8	FSA	Maximus Federal Services, Inc.	ED-FSA-13-C-0021	$126,715,465	9/30/2013
9	FSA	Dell Services Federal Government, Inc.	ED-06-CO-0107/0021	$43,140,155	9/1/2014
10	FSA	Continental Service Group, Inc.	GS-23F-0084P/ED-FSA-15-O-0029	$38,259,000	4/22/2015
-	-	**Total**	-	**$1,076,248,702**	-

[22] The contract values for IES and FSA contracts are as of December 16, 2015, and April 15, 2016, respectively.

Appendix C. Updated OPM Background Investigation and Reinvestigation Requirements

Table 3 shows the background investigation types in the Directive compared to the current OPM background investigation types and reinvestigation timeframes.

Table 3. Updated OPM Background Investigation and Reinvestigation Requirements[23]

Prior Investigation Type (as listed in the Directive)	Current OPM Investigation and Reinvestigation Type	Position Designation Type	Risk Designation Level	Current OPM Reinvestigation Timeframe for the Position Designation Type
National Agency Check with Written Inquiries	Tier 1	Low Risk	1/1C	None Required
Minimum Background Investigation	Tier 2/Tier 2 Reinvestigation	Moderate Risk Public Trust	5/5C	Every 5 years
National Agency Check with Written Inquiries and Credit	Tier 2/Tier 2 Reinvestigation	Moderate Risk Public Trust	5/5C	Every 5 years
Limited Background Investigation	Tier 2/Tier 2 Reinvestigation	Moderate Risk Public Trust	5/5C	Every 5 years
Background Investigation	Tier 4	High Risk Public Trust	6/6C	Every 5 years
Periodic Reinvestigation-Residence	Tier 4 Reinvestigation	High Risk Public Trust	6/6C	Every 5 years

[23] OPM also implemented Tier 3 and Tier 5 investigations and reinvestigations. Tier 3 investigations and reinvestigations are required for positions designated as non-critical sensitive and/or requiring eligibility for access to Confidential or Secret information. Tier 5 investigations and reinvestigations are required for positions designated as critical sensitive, special sensitive, and/or requiring eligibility for access to Top Secret or Sensitive Compartmented Information. Tier 3 and Tier 5 investigations and reinvestigations were not associated with any prior investigation type referenced in the Directive.

Appendix D: Position Designation Record Template

Appendix II: Position Designation Record for all Applicable Contractor Positions

PRINCIPAL OFFICE: _____ ORG. CODE: _____
CONTRACTOR (Company Name): _____
CONTRACTOR POSITION TITLE: _____

I. INFORMATION TECHNOLOGY (IT) RISK LEVEL: _____

JUSTIFICATION: _____
_____
_____
_____

Reminder: Be sure you have considered all pertinent access controls of the relevant IT system when determining the position risk level, such as separation of duties, least privilege and individual accountability.

If the position is Moderate or High Risk from an IT standpoint, you do not need to perform the next step. If the position is Low Risk from an IT standpoint, Step II below may adjust the final position risk level to a Moderate Risk level position.

II. This is a Moderate Risk level position because the contractor employee will require access to: (Please check if applicable)

_____ Unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary, or other unclassified sensitive information or data.
_____

III. This is a Low Risk level position because individual(s) will require:

____ An ID badge granting unescorted access to ED facilities; and/or
____ Perform duties in a school or location where children are present.

IV. FINAL POSITION RISK LEVEL PLACEMENT: _____ (Where the duties of the position involve more than one risk level, the higher of the two risk levels will be assigned to the position.)

V. ____ No risk level required for this position(s)

_____	_____	_____
(Signature) Contracting Officer's Representative	(Signature) Computer Security Officer	(Signature) Executive Officer
_____	_____	_____
Printed Name and Date	Printed Name and Date	Printed Name and Date
_____	_____	_____
Telephone	Telephone	Telephone

Appendix E. Acronyms and Abbreviations

COR	Contracting Officer's Representative
Department	U.S. Department of Education
Directive	OM Directive: 5-101, Contractor Employee Personnel Security Screenings
e-QIP	Electronic Questionnaires for Investigations Processing System
FSA	Federal Student Aid
IES	Institute of Education Sciences
IT	Information Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OM	Office of Management
OPM	Office of Personnel Management
Personnel Security	Personnel Security and Emergency Preparedness Division
PO	Principal Office

Appendix F. OM Response to the Draft Report

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

September 4, 2018

TO: Michele Weaver-Dugan
Director, Operations Internal Audit Team
Office of Inspector General

FROM: Denise L. Carter
Acting Assistant Secretary
Office of Management

SUBJECT: Response to Draft Audit Report:
The Department's Implementation of the Contractor Personnel Security Clearance Process
Control No. ED-OIG/A19P0008

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft audit report on "The Department's Implementation of the Contractor Personnel Security Clearance Process" dated August 2, 2018.

Prior to this audit, the Office of Management (OM) was aware of security clearance issues related to contractor personnel and was taking proactive steps to resolve the issues. OM will continue to improve the agency's personnel security program. As a result of these ongoing improvement efforts, many of the recommendations detailed in this audit have been implemented or are the in the process of being implemented. Specific responses to the recommendations are provided below:

- **Department Wide Policies and Procedures:**

  1.1 Develop and distribute written policies and procedures that include (1) new Federal and Department requirements for the contractor personnel security screening process established since the issuance of the Directive in 2010, and (2) existing Department practices for the screening process that have been informally approved by OM but are not addressed in current written policies and procedures.

  RESPONSE (1.1): *Interim Personnel Security Requirements and Guidance to Support Access to Department Information, Information Systems, and Facilities* was signed for release on August 22, 2018 and the formal policy OM Directive OM: 5-101, Contractor Employee Personnel Security Screenings (the Directive) has been updated and is currently in the agency clearance process.

400 MARYLAND AVE., S.W., WASHINGTON, DC 20202
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

Page 2

- **Compliance with Policies and Procedures:**

  1.2 Periodically review the security screening process and assess the need to update policy accordingly. Develop and distribute interim guidance as necessary.

  1.3 Require POs to develop internal procedures for the contractor personnel security screening process, review the PO-developed procedures for compliance with the Directive, review any modifications to PO procedures, and maintain the procedural documents provided by POs.

  RESPONSE (1.2): - OM reviewed the security screening process and developed the following guidance: *Interim Personnel Security Requirements and Guidance to Support Access to Department Information, Information Systems, and Facilities*. The new guidance will be posted on connectED and provided to all Executive Officers.

  RESPONSE (1.3): The updated Directive requires offices to develop standard operating procedures to ensure compliance with the Directive. OM will review the procedures and provide feedback, as appropriate. OM will maintain the procedural documents provided by the offices.

- **Notification of Adjudication Determinations:**

  1.4 Develop a process to ensure POs receive and maintain notification of all final adjudication determinations, both favorable and unfavorable, for each individual contractor employee who has received a security screening.

  RESPONSE (1.4): OM has developed a notification process to alert offices of favorable and unfavorable adjudication determinations for each contractor employee. OM is exploring options for automating the new notification process.

- **Designation of Contract Positions and Position Risk Levels:**

  1.5 Establish an appropriate role for OM in the contract position and risk designation process, in coordination with PO and OCFO staff, and ensure requirements for position risk designation tools and documentation requirements are adequately communicated.

  RESPONSE (1.5): OM will work with offices to assist them with obtaining the required training for contract position and risk designation, including key internal and document controls they need to implement to effectively manage their individual contract position and risk designation decision processes and clarify the appropriate role for OM in the process.

Page 3

- **Timeliness of Security Screening Activities:**

  1.6 Ensure that all elements of the security screening process, including initiation, adjudications, and reinvestigations are conducted within required timeframes. Align Directive requirements with applicable OPM metrics.

  RESPONSE (1.6): OM hired additional staff to help reduce the lead times associated with the agency portion of the personnel security screening process, including initiation, adjudications, and reinvestigations and will align Directive requirements with applicable OPM metrics.

- **Maintenance of Security Screening Information:**

  1.7 Review the staff structure and resources of Personnel Security and make changes, as appropriate, to ensure timely processing of security screenings and that proper oversight and guidance of the Department's contractor personnel security screening process is provided.

  RESPONSE (1.7): OM reviewed the staffing structure and hired additional employees to help address processing and further strengthen oversight and guidance.

  1.8 Coordinate with POs to reconcile current Security Manager data with PO records on individual contractor employees for information such as contractor employee name, contractor company, assigned contract number, employment status, and departure date as applicable. Periodically reconcile Security Manager data with PO records.

  RESPONSE (1.8): OM started the data reconciliation process in May 2018 and is working with all internal and external stakeholders to update the information accordingly.

  1.9 Require information necessary for tracking the status of contractor employees' security screenings and employment on Department contracts to be entered into Security Manager, to include contractor company and contract number.

  RESPONSE (1.9): OM will implement this recommendation.

  1.10 Review the current access of PO staff to Security Manager to determine if granting further access to key staff could help ensure the reliability of Security Manager data, and then grant access accordingly.

  RESPONSE (1.10): OM will review all current roles in the Security Manager system and determine if granting additional access will help ensure the reliability of the Security Manager data.

- **Training Provided to Staff:**

  1.11 Develop comprehensive training for the contractor personnel security screening process that covers process requirements and the responsibilities of key PO officials and staff, to include use of Security Manager and the Position

Page 4

Designation Tool. Require all applicable staff to attend.

RESPONSE (1.11): OM will consider the best ways to provide the necessary training.

If you have any questions or need additional information, please contact Richard Smith, Acting Director of Security, Facilities, and Logistics Services at (202) 260-8987 or richard.smith@ed.gov