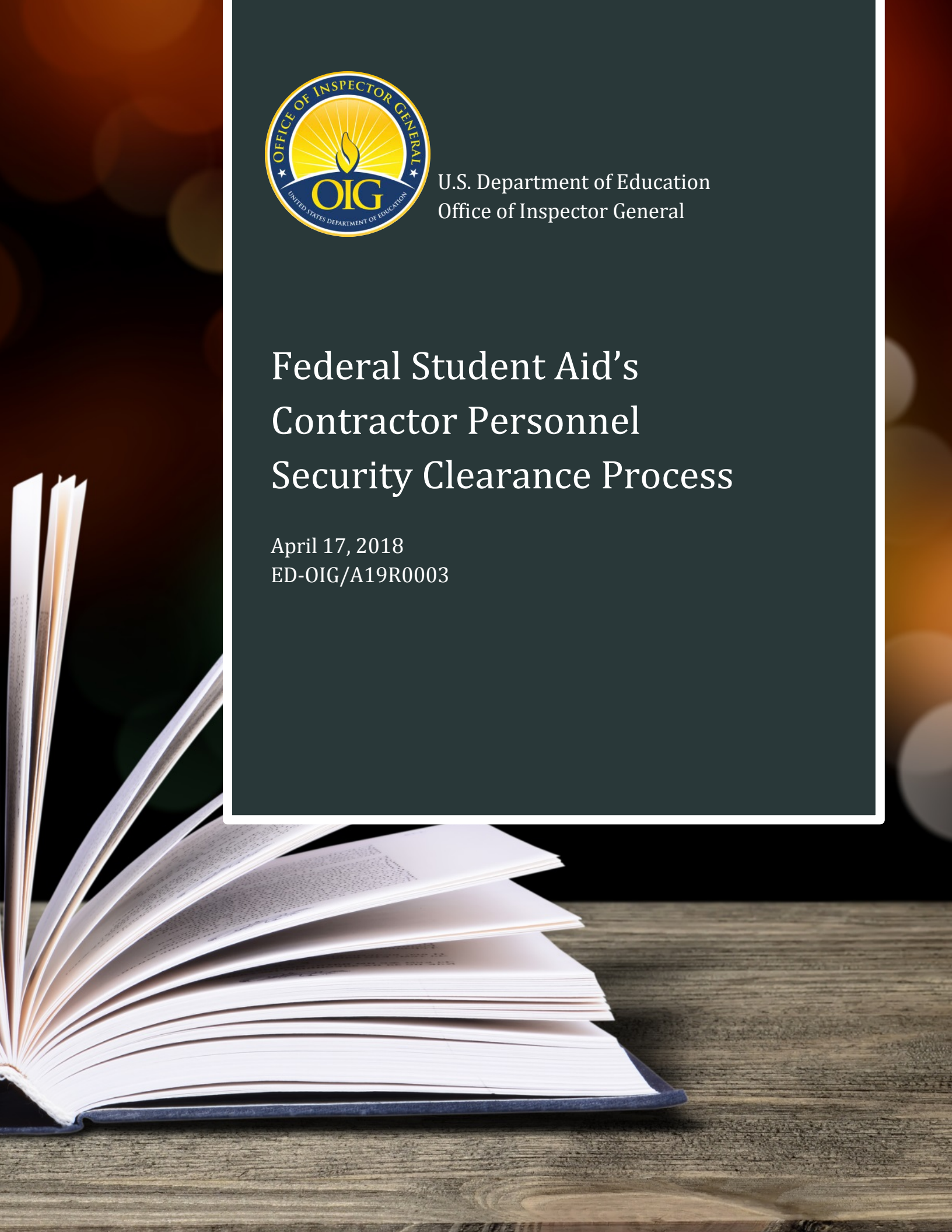

U.S. Department of Education
Office of Inspector General

Federal Student Aid's Contractor Personnel Security Clearance Process

April 17, 2018
ED-OIG/A19R0003

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 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.

April 17, 2018

TO: James F. Manning
Acting Chief Operating Officer
Federal Student Aid

FROM: Patrick J. Howard /s/
Assistant Inspector General for Audit

SUBJECT: Final Audit Report, "Federal Student Aid's Contractor Personnel Security Clearance Process," Control Number ED-OIG/A19R0003

Attached is the subject final audit report that consolidates the results of our review of Federal Student Aid's contractor personnel security clearance process. We have provided an electronic copy to your audit liaison officer. We received your comments concurring with the recommendations 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

What We Did

The objective of the 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 contractor personnel security clearance process in Federal Student Aid (FSA). This audit was part of a review of the Department's contractor personnel security process being performed in several principal offices (PO). A summary report will be provided to the Office of Management (OM), the office responsible for Department-wide oversight of the contractor security screening process, upon completion of the audits in individual POs.

What We Found

We found that FSA did not effectively implement Department requirements for the contractor personnel security screening process. We specifically noted weaknesses in FSA's development of internal policies and procedures; designation of contract positions and risk levels; maintenance of contract position, risk, and employee information, notification and maintenance of security screening decisions, and contractor employee departure procedures. We found that FSA staff and officials involved in the process were generally unaware of Department requirements and their related responsibilities for processing contractor employees' security screenings. FSA appears to heavily rely on its contractors for determining contract positions and appropriate risk levels as well as maintaining contractor employee listings without any further review of the adequacy of these determinations or the accuracy of the listings. As a result, there is increased risk that contractor employees are working on Department contracts without appropriate security screenings.

We also determined that FSA has not ensured that all contractor employees have appropriate security screenings and that security screenings are initiated or verified in a timely manner. Additionally, we determined that FSA is not always denying High Risk access[1] to Department Information Technology (IT) systems or Department sensitive or Privacy Act-protected information prior to preliminary security screenings being completed favorably, as required, and inappropriately provided High Risk IT access to non-U.S. Citizens.

[1] High Risk level access encompasses both IT access and non-IT access, which includes access to Privacy Act-protected, personally identifiable (PII), proprietary or other sensitive information and data.

Because FSA did not ensure that the contractor employees assigned to its contracts received appropriate security screenings, the Department lacks assurance that contractor employees with access to Department-controlled facilities and systems and/or unclassified sensitive information 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.

Effective May 10, 2017, FSA noted it convened a task force consisting of cross functional staff whose mission is to analyze the current process and develop an improved process going forward.

What We Recommend

We made several recommendations to improve internal controls over FSA's contractor personnel security screening process. We recommend that the Chief Operating Officer for FSA ensure that staff involved in the contractor personnel security screening process are aware of and comply with Department requirements and fulfill their responsibilities for processing security screenings. This includes developing written policies and procedures to comply with OM Directive: 5-101, Contractor Employee Personnel Security Screenings (Directive), dated July 16, 2010,[2] with explanations of the key duties to be performed by specific FSA staff, requirements of the contract positions and risk designation process including the use of Position Designation Records, and other internal requirements for the FSA contractor personnel security screening process, such as contractor employee departure procedures.

We also recommend that FSA begin tracking all active contractor employees assigned to FSA contracts, along with their risk level and any IT access, to ensure that all contractor employees have undergone security screenings at appropriate risk levels as required by Department policy. For those who have not, take immediate action to complete the security screenings and/or deny further access to Department facilities, systems, and information until appropriate security screenings are completed or required screening information is submitted.

[2] In November 2017, OM's Director of Personnel Security and Emergency Preparedness noted that OM was working on updating the Directive and issuing interim guidance as necessary to ensure Department requirements are aligned with new government-wide policies. This area will be further reviewed and discussed in the summary report that will be issued to OM upon completion of the audits in the individual POs.

We provided a draft of this report to FSA for comment. FSA concurred with the recommendations and provided a list of immediate actions it has taken and longer term solutions it is working on that FSA believes will strengthen the contractor personnel security clearance process. FSA noted that it is committed to continued collaboration with other Department offices, including OM, to discuss lessons learned and to develop standardized procedures in compliance with the Directive. FSA noted that it will also work with other Department offices to create a detailed plan that will identify tasks and timing to address the findings in the report. This plan is expected to be completed by August 2018.

FSA's comments are summarized at the end of each finding. FSA 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 findings or the related recommendations as a result of FSA's comments. The full text of FSA's response is included as Appendix G to this report.

Introduction

Background

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 IT system access, require access to unclassified sensitive information, or perform duties in a school or location where children are present. The Department's requirements for the contractor personnel security screening process are primarily found in the Directive.

The Department's processing of contractor employee security screenings involves two information systems: the Office of Personnel Management's (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) system and the Department's Security Manager system. E-QIP is a web-based 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 the Department's internal system for processing and tracking contractor employee security screenings. OM uses Security Manager to conduct all aspects of the security screening process including documentation review and maintenance, initiation of OPM background investigations, correspondence with OPM and POs, and adjudication of OPM background investigation information.

Within FSA, primary responsibility for contractor personnel security screenings belongs to FSA security screening intake staff,[3] Information System Security Officers (ISSOs), and the Personnel Security Team (Security Team) within FSA's Facilities, Security, and Emergency Management Services (FSEMS) division. Intake staff and ISSOs explained that their responsibilities include facilitating information exchange between contractor companies and the Security Team, tracking and monitoring contractor employee

[3] FSA's Business Operations office has an intake team responsible for receiving security screening information from contractor employees working on contracts under that office's purview. Four of the contracts we reviewed in our sample fell under that office's purview. We also reviewed a contract under the purview of the FSA Technology Office as part of our sample. The intake team for that contract was made up of the ISSO and backup ISSO for the contract.

security screenings, and maintaining security screening information.[4] The Security Team explained that it is also responsible for maintaining certain security screening information, such as the dates when screening packages were submitted to OM or OPM, reciprocity actions taken by the team, and the dates and reasons why certain screening packages were rejected. Additionally, the Security Team is responsible for reviewing security screening package information provided by intake staff for completeness and initiating contractor employee security screenings with OM for contractor employees in High Risk positions and with OPM directly for contractor employees in Moderate Risk and Low Risk positions.[5] [6]

Processing an FSA contractor employee's security screening involves coordination between the contractor company and employee, FSA's intake staff for the contract, the Security Team, OPM, and OM (for contractor employees in positions designated as High Risk). The process is to begin with the contractor company submitting a contractor employee's security screening information to the appropriate FSA intake staff for the contract, through e-QIP, email, and overnight or second-day mail, to inform FSA of the contractor employee's assignment to the contract and to initiate the security screening. The intake staff are expected to review the information for accuracy and completeness and provide the initial information to Security Team staff who should again review the information for accuracy and completeness. If any errors are detected, the Security Team staff are to coordinate with intake staff to assist the contractor company and employee with submitting the required information. After it is determined that a contractor employee's security package has been completed appropriately, the Security Team should release the contractor employee's e-QIP security screening information to OM through Security Manager, or directly to OPM. The Security Team should also

[4] According to the Directive, each Contracting Officer's Representative (COR) is expected to play a key role in tracking the personnel security adjudication determinations of contractor employees as a supplemental responsibility in monitoring the contract, along with other more specific responsibilities involving the security screening process; however, the CORs of each of the contracts we reviewed stated they had little to no responsibility involving security screening process requirements or in tracking any related contractor employee information.

[5] Due to the high volume of contractor employees working under FSA contracts requiring a security screening, FSA releases screening information for contractor employees working in Moderate Risk and Low Risk positions directly to OPM rather than providing it to OM. The OM Director of Personnel Security and Emergency Preparedness noted that FSA is the only program office in the Department with the ability to initiate investigations directly with OPM.

[6] See page 23 for definitions of position risk levels.

provide OM with the required hardcopy security screening information, compiled by the contractor company and employee, that includes a Request for Security Officer Action form, fingerprint documents, and required signature pages.

Contractor employees whose positions are not designated as High Risk can start working under an FSA contract as soon as their complete security screening package is submitted to FSA through e-QIP. Contractor employees whose positions are designated as High Risk can start working under an FSA contract at the Moderate Risk level as soon as their complete security screening package is submitted to FSA through e-QIP, but must wait until OM notifies FSA that a preliminary screening was completed favorably before beginning work at the High Risk level under the contract. Once OM staff receive a security package from FSA through Security Manager 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 High Risk level investigation. Once the preliminary High Risk level investigation is completed by OPM and adjudicated by OM, OPM then proceeds with the full High Risk level background investigation.

After OPM completes the requested background investigation, OPM sends OM a report of the results electronically through e-QIP into 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.

We selected FSA for review because it represented a significant number and dollar value of the active contracts within the Department at the outset of our review, and because FSA contracts involve IT systems that access a considerable amount of sensitive PII and have a considerable number of contractor employees requiring screenings at the High Risk level. We judgmentally selected the five FSA contracts with the highest dollar value[7] using the Department's most current active contract listing at the time,[8] including a

[7] Because four of the top five highest-funded FSA contracts were Title IV Additional Servicing (TIVAS) contracts, we judgmentally selected for review the two highest-funded TIVAS contracts and the next three highest-funded non-TIVAS contracts to diversify our sample. Those three contracts included a Private Collection Agency (PCA) and the contracts for the Debt Management Collection System (DMCS) and FSA's Virtual Data Center (VDC), which served as a hosting facility for FSA systems that process student financial aid applications, provide schools and lenders with eligibility determinations, and support payments from and repayment to lenders.

[8] The Department's April 15, 2016 active contract listing was the most recent listing available during the time of our contract sample selection.

sample of 110 contractor employees assigned to those contracts.[9] A listing of the contracts selected for review, to include key Department IT systems accessed under these contracts, is included as Appendix B.

[9] For this sample and other samples of contractor employees selected for review, probability of selection varied by contract and percentages reported reflect unweighted results and are not projectable.

Finding 1. FSA Did Not Effectively Implement Department Requirements for the Contractor Personnel Security Screening Process

We found that FSA did not effectively implement Department requirements for the contractor personnel security screening process. We specifically noted weaknesses in the following areas:

- development of internal policies and procedures;
- designation of contract positions and risk levels;
- maintenance of contract position, risk, and employee information;
- notification and maintenance of security screening decisions; and
- contractor employee departure procedures.

We found that FSA staff and officials involved in the process were generally unaware of the Directive requirements and their responsibilities for processing contractor employees' security screenings. As a result, there is increased risk that contractor employees are working on Department contracts without appropriate security screenings (discussed further in Finding 2).

FSA Policies and Procedures

We found that FSA has not established internal written policies and procedures that comply with the Directive. While FSA has a finalized procedural manual for its contractor employee security screening process entitled, "Investigation Request Manual," (FSA Manual), developed by the Security Team, we found that this document does not fulfill all Directive requirements. Specifically, we noted that the FSA Manual does not identify all responsible officials involved in the contractor personnel security screening process that will perform key duties, to include ISSOs, CORs, and Contracting Officers (CO), along with the FSA Executive Officer. In addition, the FSA Manual does not explain requirements for certain areas of the screening process such as the contract position risk designation process, how FSA staff should handle contractor employee reinvestigations and departures, or how FSA should maintain security screening information including lists of contract positions and risk levels and contractor employee security screening records. The FSA Manual primarily discusses the administrative steps involved in assisting contractor companies and employees through the e-QIP application process and lists the required forms that constitute a security screening package.

Section VI, Procedures and Responsibilities, Part A.1 of the Directive states that each PO must establish and maintain on file with the Chief of Personnel Security, a management official within OM Security Services, its own procedural document for complying with the Directive, and that all modifications to the document must be forwarded to the Chief of Personnel Security for review. The document will identify the responsible officials such as CORs, Computer Security Officers (CSO), or System Security Officers within the PO who will be performing key duties. The Directive also states that 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.

The FSA Manual was created by the Security Team in order to help Security Team staff with consistency during the processing of contractor employees' security screenings. The Security Team's main responsibility involves managing the contractor security screening process through e-QIP and submitting contractor employee security screening packages to OM and OPM. The FSA Manual is therefore limited in scope to the elements of the contractor security screening process that are the main focus of the Security Team. A member of the Security Team explained that no updates have been made to the FSA Manual since it was issued in 2012, although certain aspects of the screening process have changed. The staff member noted the lack of an update was due to a lack of time and resources and added that the basic process is still the same in e-QIP which makes updates to the FSA Manual not absolutely necessary. The former Deputy Chief Administration Officer noted that the FSA Manual is on file with OM but there is nothing OM would need to vet or approve about these policies and procedures and stated his belief that they are not required to be on file with OM.

We found a draft security screening procedures document located on the FSA Acquisitions (Acquisitions) Group Policy and Guidance internal SharePoint site. We determined that with appropriate updates in key areas, and with official approval, the document could be used by FSA to comply with the Directive. We were told by the Director of FSA's Strategic Initiatives & Knowledge Management Division within FSA Acquisitions that the draft document should not have been on the site, and that it has been removed. This official explained that although the document was found on the Acquisitions site, any related policy is the responsibility of the Security Team. The Director of FSEMS explained that FSA has initiated a task force to address the issues surrounding the contractor security screening process and to provide FSA management with a proposed plan and timeline for updating the documentation to align with the Directive. The official noted that FSA will update its guidance as part of the task force action items.

Without a comprehensive internal FSA procedural document for the contractor personnel security screening process, FSA cannot ensure that all FSA staff are aware of their roles and responsibilities within the process and that contractor screening requirements are being appropriately implemented.

Designation of Contract Positions and Risk Levels

We determined that FSA's process for designating contract positions and assigning position risk levels does not adequately fulfill Directive requirements. We found that FSA is not developing complete position lists for each contract, assigning risk levels for each position, or involving all required staff and officials in the process. FSA appears to heavily rely on its contractors for determining contract positions and appropriate risk levels without any further review of the adequacy of these determinations.

The CSO is required to be involved in the position risk level assignment process, to include concurring in writing with each contract position risk designation. However, FSA's Chief Information Security Officer (CISO), whose position was noted by FSA staff to equate to the CSO, explained that he has a role in ensuring that access requirements are being met, but did not indicate any responsibility regarding contract position and risk level assignment. When asked if their role involved contract position and risk level assignment, the ISSO for each contract we reviewed explained that their only responsibility involving contract position risk levels is to verify that appropriate screening steps have occurred prior to granting a contractor employee access to Department and FSA information systems. Each ISSO explained that it is not an ISSO's responsibility to assign position risk levels, but rather the contractor company's, based on what the contractor employee will be working on for the contract.

In addition, Security Team staff, intake staff, COs, CORs, and Acquisitions officials all explained that they do not have responsibility for designating risk levels for a contract's positions. During discussions with these individuals, each one informed us that these responsibilities belonged to another person or group within FSA even after they were identified by someone else as the person or belonging to a group responsible for that task. For example:

- The Directive requires that CORs sign off on position designation information; however, the COR for each contract we reviewed explained they have a very limited role during the security screening process, and do not have any responsibility involving the assignment of position risk levels.
- The Directive requires that the CO, among others, ensure that each contractor employee position is assigned an appropriate risk level and that this information is included in the solicitation (in the case of non-performance based contracts)

or communicated to the contractor at the earliest possible time during the acquisition (in the case of performance based contracts). COs for the contracts in our sample explained that they do not have any role related to position risk level designation. The Director of FSA's Strategic Initiatives & Knowledge Management Division added that this responsibility falls under the purview of a contract's COR and ISSO and explained that COs are fulfilling their Directive responsibilities by simply including required security screening provisions and clauses in FSA contract solicitation and award documentation.

- Intake staff explained their team does not have any role in vetting the risk level for the position of a contractor employee and noted that the Acquisitions Group is responsible for performing this action.
- Security Team staff explained that this responsibility falls under the purview of the CO and ISSO for the contract.
- The Executive Officer is required to be involved in the position risk level designation process by concurring in writing with each contract position risk designation; however, the FSA Executive Officer stated that she does not have a role in this process.

Additionally, FSA staff did not identify any role for the Chief of Personnel Security in the position risk level designation process and there is no role identified in the FSA Manual.

We also found that FSA did not use or maintain Position Designation Records for any contract positions included under the five contracts in our sample as required. A Position Designation Record provides written justification for classification of a contract position as High, Moderate, Low, or No Risk and provides for sign-offs of key officials noting concurrence with the assigned risk level. [A copy of the Position Designation Record is included as Appendix C to this report.] We noted that the ISSOs for two of the contracts we reviewed were able to provide a position and risk level designation matrix for their contract using OPM's position risk designation tool as a template, but neither matrix was complete as a significant number of contract positions were not included on each. For example, the position risk level designation documentation for one contract included only 2 positions while the active contractor employee listing included over 50 positions. One of the ISSOs noted that limited positions were included on the position risk level designation matrix for their contract because that was the information provided by the CO, and that it is the CO's and the COR's responsibility to ensure that the contractor employee's risk level suggestion is appropriate for the contractor employee position responsibilities at the time of the request for screening.

Another ISSO provided the applicable contract system security plan as position designation documentation that he said FSA reviews and approves, but we determined that this also was not close to being complete. This ISSO explained there are too many different contractor employee positions for each to be included in position risk level designation documentation. The ISSO of the one contract we reviewed that did have complete position risk level designation information available explained that the information was provided to FSA by the contractor and he was not sure if FSA had approved the position risk level information. He noted that the position risk level designation information is not used by FSA anyway, as that information was not shared with Acquisitions or the Security Team and is not compared to a contractor employee's screening documentation when it is submitted to see if the risk levels match.

Additionally, the ISSOs of three of these contracts noted that documentation showing any position risk level assignment was not developed or collected until after contract award. An Acquisitions official, along with the CO and ISSO for one of the contracts, erroneously believed position risk level designation records were not required to be developed at the time the contract was awarded back in 2006 due to the fact that the contract was awarded prior to establishment of the current Directive. However, we noted that the same requirement was noted in a version of the Directive as far back as 2002.

We noted that FSA had listings of contract positions and risk levels documented for two of the contracts as part of an internal report that was prepared for each contract to determine the cost related to security screenings, and the analyses appear to have been performed prior to contract award. However, neither of these reports included all current contract positions or noted any concurrence by key officials with the assigned risk levels.

Section VI, Parts A.3-A.4 of the Directive states that each PO must determine the risk levels for each contractor position, in coordination with the CSO and the Chief of Personnel Security, prior to contract award.[10] The PO must maintain a current position risk level designation record for each contractor position to which the Directive applies. This information will be recorded on the Position Designation Record included as an appendix to the Directive and should be maintained on file with either the COR or CO for the contract. The Position Designation Record must be signed by the COR for the contract as well as the PO's CSO and Executive Officer. Part A.9 states that the PO COR must also ensure that a contractor employee is not placed in a more sensitive position

[10] New positions and labor categories can subsequently be added to a contract if approved by each PO.

than that for which he or she was previously approved, without the approval of the Chief of Personnel Security and the PO's CSO.

As noted above, the FSA Manual does not provide information on the roles of each contract's ISSO, COR, and CO, along with the FSA Executive Officer, and does not explain the requirements for the contract position risk designation process such as the use of Position Designation Records. As a result, FSA officials and staff do not appear to be familiar with their expected roles in the security screening process or aware of specific requirements from the Directive.

Without coordinating on position risk level designations and ensuring that the actual positions and risk levels are approved, FSA has little assurance that the risk levels assigned by the contractor are appropriate for a contractor employee's position responsibilities, or correspond to risk levels assigned to similar positions. As a result, FSA cannot ensure that contract employees are receiving the appropriate security clearances. Furthermore, without Position Designation Records or complete position risk level designation matrices showing FSA approval, FSA has no written justification for the decisions regarding the assignment of position risk levels.

Maintenance of Contract Position, Risk, and Employee Information

We found that FSA did not maintain up-to-date lists of all contract positions, risk level designations, or contractor employees as required for any of the five contracts we reviewed. At the start of our audit fieldwork, FSA officials explained that up-to-date listings of contractor employees working under each contract were not being maintained by FSA and that FSA would need to request that information from contractor companies. During our audit fieldwork, Acquisitions provided us with the listings of current contractor employees compiled by the contractor companies of each contract we reviewed as part of our sample. However, these listings did not include the date that the contractor employee screening information was submitted or the date of the final personnel security screening determination for each contractor employee listed. We also noted that four of the five contract listings included employees with the same position title working under the same contract but with different risk levels assigned.

The Security Team provided us with listings of contractor employees it had received for screening initiation under each contract for fiscal years (FY) 2014 through the date of our request for this information (December 15, 2016), which included the name of the contractor firm, the risk level designation for each contractor employee included on the listing, and the date the contractor employee's investigative forms or previous screening information was submitted, but Security Team staff noted that these lists would not necessarily include all current contractor employees working on the contract. We also

noted that the Security Team listings did not include positions or the date of the final personnel security screening determination for each contractor employee included.

Section VI, Part A.9 of the Directive states that each PO must maintain an up-to-date list of all contract positions and risk level designations. The list must include the name of the employing firm, the risk level designation of each position, the name of each contractor employee currently in that position, the date the contractor employee investigative forms or previous screening information were submitted, and the date of the final personnel security screening determination.

FSA staff involved in the screening process, to include Acquisitions officials, intake staff, Security Team staff, CORs, and COs, did not appear to be aware of the applicable Directive requirements. With regard to the incomplete Security Team lists, Security Team staff explained that some contractor employees end up working on the contract without their security screening information being sent to the Security Team. Security Team staff also noted that others either do not make it through their screening or leave the contract shortly after assignment, which means they would be included on the Security Team listing for the contract but would no longer be included on the active employee listing maintained by the contractor.

If FSA does not maintain the information required by the Directive, it will be unable to track contractor employees' assignment to and departure from contracts, ensure that contractor employees are placed in approved positions with correctly assigned risk levels, and monitor contractor employees' screening statuses. Failure to appropriately track and maintain this information may result in FSA's inability to ensure that only contractor employees with appropriate security screenings are working on Department contracts.

Notification and Maintenance of Security Screening Decisions

We found that for each of the five contracts in our sample, no one in FSA maintained records of final OM personnel security adjudication determinations for individual contractor employees or informed relevant parties including the CO, ISSO, or contractor companies of these final determinations as required. In general, we noted that intake staff were unaware of a contractor employee's screening status after submitting the security package information to the Security Team and for Moderate Risk level contractor employees the Security Team was unaware of the screening status after submitting the information to OPM. For contractor employees in positions designated as High Risk, we found that the Security Team documented preliminary High Risk level clearances granted by OM but was unaware of the screening status after that.

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 CO, CSO, and/or the System Security Officer. Part A.7 states that each COR must ensure that the CO, and if necessary the CSO, is kept informed during the contractor employee screening process, including notification of the screening determination. In addition, Part A.8 notes that each COR must notify the contractor company of the personnel security adjudication determination and maintain a copy of the determination. Part A. 9 notes that each PO must maintain the date of the final personnel security screening determination for each contractor employee.

FSA staff stated that while FSA does receive preliminary High Risk clearance information from OM for some contractor employees in positions designated as High Risk, FSA does not receive notification of final adjudication decisions from OM for contractor employees working at any risk level. The Director of FSEMS and the former Deputy Chief Administration Officer confirmed that FSA does not receive such notifications from OM. In order to determine the status of a contractor employee's security screening, Security Team staff and/or ISSOs must review information in Security Manager or contact OM to request the status of a screening. Multiple FSA staff noted that the lack of notification from OM is a weakness in the security screening process. The Director of FSEMS and the former Deputy Chief Administration Officer explained an easy fix in the short term would be to have OM report out on all adjudications. A Security Team staff member noted that FSA has requested that OM provide monthly adjudication reports, but that no such updates have been provided. The staff member noted that the last request was made in early 2017, and as of June 2017, FSA has not received any reports.

OM officials verified that OM does not provide POs any notification of favorable adjudication decisions. OM officials stated that OM has an agreement with POs that if PO staff do not hear back 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 CO for the contract by sending an email with an official letter attached. In January 2018, OM's Director of Personnel Security and Emergency Preparedness noted that OM is working on developing in Security Manager the capability to generate a report that lists batches of contractor employees, potentially by contract or PO, that have had cases adjudicated within a certain timeframe.

The Security Team staff can view OM adjudication determinations for FSA contractor employees but stated they do not have the resources to track all contractor employee security screening results due to the volume of FSA contractor employees requiring

security screening. Security Manager does not provide a batch search function. As a result, each contractor employee needs to be individually reviewed to determine the screening status.

In cases when FSA is not aware of final OM adjudication decisions, contractor employees may be allowed to work on Department contracts and have access to Department IT systems without complete and appropriate screenings.

Contractor Employee Departure Procedures

We determined that FSA did not always ensure that procedures involving contractor employee departure from a contract were performed as required. Specifically, we found that FSA did not always report contractor employee departures to OM within the required timeframe or did not report them at all.[11] We found that FSA did not inform OM of contractor employee departures for 20 of the 41 (49 percent) contractor employees reviewed, and 6 of the 21 (29 percent) departures that FSA reported to OM were not reported within the required 3 business days.

We also determined that FSA is not always collecting Personal Identity Verification (PIV) cards as required after employee departure. We noted that 2 of the 41 departed contractor employees we reviewed were provided PIV cards. We found that neither PIV card was returned to the contract's COR for collection. In one case the PIV card was returned to the FSA Badging Office, but FSA was not aware of who provided it or when. In the other case, the PIV card was not returned, and upon further FSA investigation, FSA was told that a contractor manager had shredded the card.

Section VI, Part A.11 of the Directive states that each PO COR must notify the Chief of Personnel Security within 3 business days of the departure of a contractor employee, either voluntary or involuntary, and furnish the reason(s) and the date of the departure, unless the departure resulted from action by the Chief of Personnel Security.

Section VI, Part C.7 of the Directive also states that each contractor must report to the COR within 2 business days any removal of a contractor employee from a contract; within 1 business day if removed for cause. The contractor is responsible for returning a Department ID badge to the COR within 7 business days of the contractor employee's departure.

[11] Separate from our analysis involving the security screenings of the sample of 110 contractor employees, we reviewed a random sample of 41 contractor employees who were confirmed to have worked on and departed from the five contracts that we reviewed in our sample.

FSA did not inform OM of any of the contractor employee departures for two of the contracts we reviewed and did not provide an adequate explanation as to the reason why. Under one contract, FSA staff explained that they were not notified by the contractor about two of the employees' departures. We determined that the contractor did not provide timely departure information for 2 of the 6 contractor employees that FSA reported late to OM.

As noted above, the FSA Manual does not provide information on the roles of each contract's key staff, and does not explain the requirements of contractor employee departure procedures. As a result, FSA officials and staff do not appear to be familiar with or aware of specific requirements from the Directive. Regarding the two cases where departure information was not provided by the contractor, FSA staff explained that the departures were discovered by FSA during analysis in response to the Office of Inspector General's (OIG) inquiry.

Regarding PIV card collection, officials within FSA's Technology Office, along with the applicable ISSO and COR, indicated that FSA does have information within its contracts stating that contractors are to provide PIV cards to the COR upon contractor employee departure. With regard to the two cases noted above, it was explained this was an oversight on FSA's part and they are working on a better process to ensure all departing contractor ID badges as well as any other Government-furnished equipment are received upon departure.

Failure to appropriately track and report contractor employee departures may hinder FSA's and the Department's ability to ensure that only active contractor employees with appropriate security screenings have access to Department facilities and IT system access.

Recommendations

We recommend that the Chief Operating Officer for FSA:

1.1 Ensure that staff involved in the contractor personnel security screening process are aware of and comply with the Directive requirements, to include any subsequent updates to the requirements, and fulfill their responsibilities for processing security screenings.

1.2 Develop written policies and procedures to comply with the Directive, to include explanations of the key duties to be performed by specific FSA staff, requirements of the contract positions and risk designation process including the use of Position Designation Records, and other internal requirements for the FSA contractor personnel security screening process, as well as contractor employee departure procedures.

1.3 Have appropriate FSA staff develop and approve complete position category listings and associated risk level designations for all contractor positions on each contract, through FSA justification of position responsibilities and access, and through reconciliation of current contract position risk levels and any available position risk level designation records.

1.4 Ensure that screenings are initiated at the appropriate risk level based on the contractor employee's position risk level that was classified and approved by FSA.

1.5 Coordinate with OM to learn the adjudication results of current contractor employees assigned to FSA contracts to ensure that all contractor employees either have a screening initiated or have been appropriately cleared to work on Department contracts.

1.6 Monitor the screening status of contractor employees until final OM adjudication decisions are made.

1.7 Maintain all information and records required by the Directive, to include up-to-date listings of all contractor employees assigned to FSA contracts and records of OM adjudication decisions for all contractor employees assigned to FSA contracts.

1.8 Ensure that all contractor employee departures are reported to OM as required, and inform contractor companies on a regular basis of their responsibility to notify FSA of contractor employee departures. Also ensure that contractors provide PIV cards to the COR upon contractor employee departure, as required.

FSA Comments

FSA concurred with the recommendations. FSA noted that it will continue to work with other parts of the Department to ensure that FSA's written policies and procedures comply with the Directive, and that all staff responsible for personnel security screening, position category, and risk level designations understand their responsibilities and have the appropriate procedures to ensure accuracy and consistency in processes. FSA also noted that it will continue to work with other parts of the Department to review FSA's internal processes to ensure that the required reviews, communications, and documentation are maintained according to the Directive. FSA stated that its leadership will develop monitoring processes to ensure adherence to applicable processes and procedures.

OIG Response

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

Finding 2. FSA Has Not Ensured That All Contractor Employees Have Appropriate Security Screenings and That Security Screenings Are Initiated or Verified in a Timely Manner

Security Screening Coverage

We reviewed FSA records and information contained in Security Manager for a stratified random sample of 110 contractor employees from the five contracts we reviewed to determine whether FSA ensured that contractor employees received an appropriate security screening. Of the 110 contractor employees included in the sample, 75 were in positions designated as High Risk; 35 were in positions designated as Moderate Risk. As part of our review, we determined whether screenings had been completed for each of these employees, were at the appropriate risk level, and had favorable OM adjudication decisions. We determined that all 110 contractor employees in the sample required a security screening.[12] We found the following:

- 87 (79 percent) contractor employees had an appropriate security screening completed.[13] This includes 16 contractor employees that received screenings under a prior Department contract they worked on or for prior employment at another Federal agency. We found FSA appropriately verified the screenings for 15 of these 16 contractor employees.

[12] All contractor employees required a security screening because they met the Directive-defined criteria for security screenings, such as assignment to a Department contract for more than 30 days or access to Department IT systems.

[13] Not all of the security screenings were initiated in a timely fashion. See the "Security Screening Timeliness" section on page 25 for further discussion.

- 18 (16 percent) contractor employees did not have evidence of an appropriate security screening. 4 of these 18 contractor employees were in positions designated as High Risk.[14]

- 5 (5 percent) contractor employees began work on their contract shortly before we began our review. Each had a background investigation initiated at the appropriate risk level that was still pending with OPM.

In addition, we found that 3 of these contractor employees for which a reinvestigation was required did not have a reinvestigation initiated by FSA.

For the 18 contractor employees that did not have evidence of an appropriate security screening, we found that each had records in Security Manager, indicating that a security screening had at least been initiated at some point, but there was insufficient evidence that a complete security screening had occurred.

- For 15 of the 18 contractor employees, which includes all 4 of the employees in positions designated as High Risk, there was evidence that an OPM background investigation was completed at the appropriate risk level, but there was no evidence of an OM adjudication decision.[15] OM favorably adjudicated a reinvestigation for 1 of these employees which was completed 5 years after the employee's prior investigation was completed by OPM.

- For 2 of the 18 contractor employees, we found no evidence that an OPM background investigation was ever completed. We determined that OPM had discontinued the background investigation for both contractor employees and

[14] We determined that 3 of the 4 contractor employees were working at the High Risk level prior to the required completion of a preliminary security screening. We could not determine whether the other employee received High Risk level access prior to the completion of a preliminary security screening. While we determined this employee did not receive High Risk IT access, neither FSA nor the contractor could provide the date when the contractor employee's non-IT High Risk access began.

[15] This includes nine short-term contractor employees for which a Special Agreement Check (SAC) investigation was completed but there was no evidence of an OM adjudication decision. FSA staff stated that OM adjudications are not necessary on a SAC investigation for short-term employees. However, we have found cases when OM has adjudicated SAC investigations. While there is no written policy covering short-term contractor employees included in the Directive or in any other security screening policy guidance developed by the Department, OM staff explained that contractor companies can be granted waivers of the regular screening process allowing SACs to cover short-term employees working for 90 days or less on a Department contract.

FSA had not resubmitted a complete and appropriate investigation package back to OPM after the discontinuation, even though the contractor employees were allowed to continue work on the contract.

- For 1 of the 18 contractor employees, there was evidence that an OPM background investigation was completed, but at a lower risk level than was necessary for the contract position. This contractor employee was designated as short-term but worked on the contract for a period of time longer than allowed for under this designation.[16] As a result, this contractor employee was required to have a full Moderate Risk level screening.

We found that these contractor employees were permitted to work on their contracts without an appropriate security screening for the following periods:

- 4 (22 percent) were on the contract for more than 2 years (3 were in positions designated as High Risk);
- 4 (22 percent) were on the contract between 6 months and 1 year (1 was in a position designated as High Risk);
- 7 (39 percent) were on the contract between 30 days and 6 months; and
- 3 (17 percent) were on the contract for less than 30 days.

Because of the significant discrepancies found between the active contractor employee listings we received from the 5 contractors included in our sample and the listings of contractor employees we received from the Security Team, we also reviewed an additional 120 contractor employees to determine whether they had appropriate screenings initiated. [17] We selected a stratified random sample of 50 of the 646 contractor employees that were included on the lists provided by the contractors but were not included on FSA's internal screening listing provided by the Security Team, and 70 of the 462 contractor employees that were included on the active employee lists provided by the contractors that had information included on the Security Team listing indicating that screening packages for these individuals had been rejected by either FSA,

[16] FSA staff noted that this employee voluntary terminated before the SAC investigation expired. However, this employee was included on the active contractor employee listing provided by the contractor more than 10 months after the employee began working on the contract.

[17] As previously noted, contractor employees in positions designated as Moderate or Low Risk can start working under an FSA contract as soon as their complete security screening package is submitted to FSA. Contractor employees in positions designated as High Risk can start working at the Moderate Risk level upon submission of their complete security screening package.

OM, or OPM. We found that 22 (18 percent) of the 120 contractor employees we reviewed were permitted to work on their contracts without an appropriate security screening ever being initiated or reinitiated after being rejected.

We determined that these 22 contractor employees, 2 of which were in positions designated as High Risk,[18] were permitted to work on their contracts for the following periods without having an appropriate security screening initiated or reinitiated after being rejected:

- 2 (9 percent) for more than 2 years;
- 5 (23 percent) between 1 year and 2 years (1 was in a position designated as High Risk);
- 1 (5 percent) between 6 months and 1 year;
- 13 (59 percent) between 3 months and 6 months (1 was in a position designated as High Risk);
- 1 (5 percent) for less than 3 months.

Section IV, Applicability, Part A of the Directive states that the Department's policy is to ensure that all contractor and subcontractor employees undergo personnel security screenings if, during the performance of the contract, they will:

1. Require an identification badge granting unescorted access to Department facilities;
2. Require Department IT system access;
3. Require access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary or other sensitive information and data; or
4. Perform duties in a school or location where children are present.

Section VI, Part A.3 of the Directive also defines the three position risk levels and their investigative requirements[19] as the following:

[18] We could not confirm whether the two employees in positions designated as High Risk were working at the High Risk level during the time periods noted as that information was not made available.

[19] See Appendix D for a detailed summary of investigative types and coverage as included in the Directive.

- High Risk: Positions with the potential for exceptionally serious impact on the efficiency of the Department. This includes access to Department IT systems that allows the bypass of security controls or access that, if taken advantage of, could cause serious harm to the IT system or data. A Background Investigation is the type of investigation required.
- Moderate Risk: Positions with the potential for moderate to serious impact on the efficiency of the Department, including all positions that require access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary or other sensitive information and data. A National Agency Check with Written Inquiries (NACI), and a credit check, is the type of investigation required. The investigation will be expanded to a Minimum Background Investigation or a Limited Background Investigation if the NACI plus credit check investigation develops information that the Chief of Personnel Security considers potentially actionable.
- Low Risk: Includes all other positions to which the Department's security screening policy applies. A NACI is the type of investigation required.

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.

With regard to the 15 contractor employees we identified that did not have evidence of a final adjudication determination from OM, OM staff could not provide an adequate explanation for why these cases had not been adjudicated. OM staff stated that 3 of the cases were pending adjudication. We noted that these 3 cases had been pending adjudication anywhere between 15 months to 2 years. For the two contractor employees that had background investigations discontinued by OPM, we determined that FSA had not resubmitted a complete and appropriate investigation package back to OPM due to a lack of clearly defined PO roles and responsibilities covering the security screening process. For the one contractor employee with evidence that an OPM background investigation was completed, but at a lower risk level than was necessary for the contract position, we determined that FSA would not be aware if a short term contractor employee remained on the contract for a longer period of time than a SAC investigation covers because FSA is not maintaining active contractor employee listing information. For the contractor employees with no evidence that a reinvestigation was initiated after the required amount of time for continued clearance for work on the contract, FSA staff explained that reinvestigation requests for these employees were not sent. FSA staff noted that the contractor was informed to wait on reinvestigations due to updates being performed at OPM and OPM was not equipped to receive reinvestigations yet.

Overall, we determined that some contractor employees were allowed to work on a contract without an appropriate security screening due to a lack of any formalized process within FSA to track screenings of contractor employees, to include that no one involved in FSA's security screening process has accepted responsibility for ensuring that security screenings are initiated and completed appropriately.

We found that the intake staff were not forwarding the screening packages received from the contractors to the Security Team, or the Security Team staff were not forwarding the screening packages received from the intake team to OM or OPM for processing. Neither the intake staff nor Security Team staff could explain why some screening packages were not forwarded at all, or why some screening packages were not forwarded until after the contractor employee had been working on the contract for a significant period of time. FSA staff also noted that while some screening packages were assembled and prepared to ship to OM or OPM at the time of hire, review of records could not confirm that FSA actually shipped the packages, and when it was discovered that there was no adjudication, the employee completed a new screening package and it was re-submitted as soon as possible. In addition, we noted that FSA would not be aware of contractor employees being added to a contract that needed screenings initiated since FSA is generally not maintaining up-to-date lists of contractor employees as required.

With regard to contractor employees that were allowed to continue work on a contract after an initial FSA rejection of the contractor employee's security screening package, FSA staff explained that some of these cases were re-initiated later than they should have been because there are no formal processes or procedures to quickly notify contractors when there are issues with contractor employee security screenings. Security Team and intake staff noted that they return these rejected security screening packages to CORs and ISSOs with notations explaining what must be corrected by the contractor. Security Team and intake staff explained that it is a COR and ISSO responsibility to ensure that the rejected packages are corrected by contractor employees and resubmitted.

With regard to contractor employees that were allowed to continue work on a contract after a discontinued or rejected OPM investigation, Security Team staff noted they receive notifications from OPM pertaining to cases deemed unacceptable which are forwarded onto the COR and ISSO that are responsible for the submissions. The COR and ISSO are instructed to resubmit the investigation within 7 business days, if the contractor is still on the contract. OPM also sends an email to the Security Team requesting confirmation of employment when a contractor employee is either uncooperative or unable to be reached during the scheduling of the subject interview. These emails are also forwarded to the COR and ISSO with instructions to reply within

10 days or the case will be automatically discontinued. However, neither of these parties claim responsibility for the roles noted. ISSOs explained that COs and CORs are responsible for ensuring screenings are completed for employees working under FSA contracts and that ISSOs are responsible only for ensuring that appropriate steps have been taken before providing an employee with applicable IT access. CORs explained they do not have much, if any, responsibility in the screening process. COs and the Director of FSA's Strategic Initiatives & Knowledge Management Division explained that COs do not have a role in this process except for including appropriate clauses and provisions in FSA's contracts.

Because FSA did not ensure that the contractor employees assigned to its contracts received appropriate security screenings, the Department lacks assurance that contractor employees with access to Department-controlled facilities and systems and/or unclassified sensitive information are suitable for the level of access granted to them. The Department's information and systems, which include sensitive PII such as social security numbers and birth dates, 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.

Security Screening Timeliness

We reviewed security screening records for the 110 contractor employees in our sample to determine whether FSA initiated or verified the security screenings within established timeframes. For the 94 contractor employees for which there was no prior screening available for verification, we determined that 62 (66 percent) did not have their security screenings initiated within the required 14-day timeframe established by the Directive. For the 16 individuals that had prior screenings, 9 (56 percent) were not verified by FSA in a timely fashion.[20]

For the 62 contractor employees that did not have their security screenings timely initiated (38 of which were in positions designated as High Risk), we found the following:

- 5 (8 percent) were initiated more than 4 years late;
- 2 (3 percent) were initiated between 2 years and 3 years late;
- 1 (2 percent) were initiated between 1 year and 2 years late;

[20] While the Directive does not include verification timeliness requirements, we considered a verification to be timely if it occurred in the same timeframe established by the Directive for screening initiation.

- 32 (52 percent) were initiated between 30 days and 6 months late;
- 22 (35 percent) were initiated less than 30 days late.

Verification of security screenings occurred between 1 day and 3 years late, with a median of 12 days.

Section VI, Part C.3 of the Directive states that each contractor must ensure that its contractor employees submit all required personnel security forms to the COR within 2 business days of an assignment to an ED contract and ensure that the forms are complete. In the event that forms are not complete, the contractor must resubmit the forms to the COR within 7 business days or the contractor employee must be removed from the contract.

Section VI, Part A.5 of the Directive states that for High Risk level positions, each PO must have the COR submit completed contractor employee investigative forms, and a "Request for Security Officer Action" form for each individual, on a pre-appointment basis.[21] With regard to all other positions, Section VI, Part A.6 of the Directive states that each PO must have the COR submit completed contractor employee investigative forms and a "Request for Personnel Security Officer Action" for each individual required to have a security screening, to the Chief of Personnel Security within 14 days of the date the contractor employee is placed in a position. The Directive emphasizes that no contractor employees are permitted unescorted or unsupervised access to Department facilities, unclassified sensitive information, or IT systems until they have submitted applicable investigative forms.

Section VI, Part C.2 states that contractor employees who have undergone appropriate personnel security screening for another Federal agency will be required to submit proof of that personnel security screening for validation, or otherwise be subject to ED personnel security screening requirements as stated in this policy. The PO must maintain the date a contractor employee's previous screening information was submitted and CORs must ensure that a contractor employee is not placed in a more sensitive position than that for which he or she was previously approved without the approval of the Chief of Personnel Security and the PO's CSO.

[21] As discussed in the "Access to IT Systems and Sensitive Information" section on page 27, the PO must deny the contractor employee High Risk level access to IT systems or Department sensitive or Privacy Act-protected information, until the Chief of Personnel Security notifies the COR that the preliminary security screening was completed favorably.

Section VI, Parts B.4 and B.5 of the Directive note that the Contracting Officer is to be involved in ensuring that all contractor employees are screened in a timely manner and that the procedures in the Directive are fully implemented throughout the performance of the contract, to include the requirement that each contractor timely submit completed forms to the PO.

FSA staff do not appear to have a full understanding of their responsibilities related to security screening initiation and verification timeliness. In general, for contractor employees without screening package errors or rejections, intake and Security Team staff could not provide an adequate explanation for FSA's noncompliance with the timeliness requirements included in the Directive. FSA staff stated that in some cases the contractor employee or company has not submitted required information. We note that several of these contractor employees have or had been working on their contracts for months or years without having submitted the required information and that there does not appear to be any indication of follow-up by FSA staff. Under one contract, FSA staff explained that processing delays were due to the contractor being behind on processing, and that the issue is being addressed by increasing administrative staff at the contractor to handle the clearance documents.

Additionally, it appears that FSA's intake and Security Team staff could not completely handle the volume of contractor employees needing security screenings as Security Team staff noted there was a backlog in processing.

If FSA does not ensure that security screenings are initiated or verified in a timely manner, there may be contractor employees working on Department contracts for long periods of time despite not being suitable for the access granted.

Access to IT Systems and Sensitive Information

We determined that FSA is not always denying contractor employees High Risk level access to IT systems or Department sensitive or Privacy Act-protected information prior to preliminary security screenings being completed favorably, as required. We reviewed available FSA records and security screening information in Security Manager along with employee records compiled by contractor companies for the 75 contractor employees from our sample that were in positions designated as High Risk. We found that 30 (40 percent) of these contractor employees were granted High Risk level access prior to the completion of a preliminary security screening and as many as 30 (40 percent) more may have been granted High Risk access prematurely.

- For 3 of the contracts we found that 30 of the 45 contractor employees we reviewed received High Risk level access prior to the completion of a preliminary security screening.

- For one of the contracts we could not determine whether the 15 contractor employees we reviewed received High Risk level access prior to the completion of a preliminary screening, as neither FSA nor the contractor company could provide the date that contractor employees began High Risk level work.
- For the remaining contract, we found that all 10 of the 15 contractor employees we reviewed that had High Risk IT access had a preliminary security screening completed prior to receiving High Risk level access to the related IT system. However, we could not determine whether non-IT High Risk access had been given prematurely because neither FSA nor the contractor could provide the dates when the contractor employees' non-IT High Risk access began. As a result, we could not determine whether the 15 contractor employees we reviewed for this contract worked at the High Risk level prior to completing a preliminary security screening.

Lastly, the Directive allows granting non-U.S. citizens High Risk IT system access in those circumstances where a non-U.S. Citizen possesses a unique or unusual skill or expertise urgently needed by the Department but a suitable U.S. Citizen is not available. In order to do so, several conditions must be met and written approval must be filed with the CO before requesting a preliminary personnel security screening and/or investigation.[22] Our sample of contractor employees included two such individuals for which we found security screenings completed at the appropriate level, however FSA was unable to provide any of the additionally required documentation and approvals needed for the appointment of these individuals.

Further, FSA alerted us to the fact that three foreign national contractor employees[23] were allowed to work with High Risk level access to IT systems under one of the contracts we reviewed for a period of 8 months without an appropriate screening and appropriate documentation and approval. FSA only detected the error when the contractor company requested waivers for these employees. After the error was detected, the contractor company appeared to comply with an FSA request to remove system access for these individuals; however, FSA found that two of the individuals were accessing the system under different contractor employee logins, still without an

[22] In related correspondence, FSA referred to this process of granting non-U.S citizens High Risk IT system access as a waiver process. We therefore referred to this process as such in related discussion in the report.

[23] For the purposes of this report, we are using the terms "foreign national," as referenced in FSA correspondence, and "non-U.S. citizen," as referenced in the Directive, interchangeably.

appropriate security screening initiated or completed. Upon our request for further information regarding the status of these two employees, the Director of the Security Division within FSA Business Operations explained that an incident report was filed with the Department's Computer Incident Response Capability Coordinator and the two individuals were removed from the contract. The official noted he was not aware of any punitive action taken by FSA or the Department regarding the incident.

Section VI, Part A.5 of the Directive states that the PO must deny the contractor employee High Risk level access to IT systems or Department sensitive or Privacy Act-protected information, until the Chief of Personnel Security notifies the COR that the preliminary security screening was completed favorably. Section VI, Part C.1 of the Directive states that each contractor must ensure that all non-U.S. Citizen contractor employees are lawful permanent residents of the United States or have the appropriate work authorization to work in the United States. In those circumstances where a non-U.S. Citizen possesses a unique or unusual skill or expertise urgently needed by ED, but a suitable U.S. Citizen is not available, a non-U.S. Citizen may be assigned to a High Risk IT (6C) level position, provided: he/she is a Lawful Permanent Resident of the United States; has resided continuously in the United States for a minimum of 3 years; the head of the PO, or his/her designee that owns the IT system, information, or network, approves the assignment in writing; and the written approval is filed with the Contracting Officer before requesting a preliminary personnel security screening and/or investigation. Section VI, Part A also states that a PO has the option to deny contractor access to their controlled facilities, unclassified sensitive information, or IT systems, until the Chief of Personnel Security has made personnel security adjudication determinations.

We determined that FSA does not have proper controls in place over the access being granted to IT systems or Department sensitive or Privacy-Act protected information. FSA is required to deny this access until the Chief of Personnel Security notifies the COR that the preliminary security screening was completed favorably. As noted above, we have found that this process lacks formality in the sense that no one involved in the process is taking ownership of their role in the process and there is confusion over who is responsible for what. As previously noted, FSA's ISSOs have stated that their only role in the screening process is to ensure that appropriate steps have been taken before providing an employee with applicable IT access, however they do not appear to be adequately performing this role. FSA appears to rely heavily on its contractors to ensure applicable security screening paperwork is initiated and processed and does not control or properly track contractor employee High Risk or other system access to make sure access is not granted prematurely or inappropriately.

In general, FSA could not provide an adequate explanation for why High Risk access was provided to contractor employees prior to them receiving notice from OM that a preliminary security screening was favorably completed. FSA staff noted that for one of the contracts we reviewed, it is the contractor company that provides contractor employees with access to FSA systems as what they called an "external business partner." FSA staff explained that some contractor companies have the ability to appoint an administrator that acts as that entity's ISSO who enrolls and removes individuals for access to the National Student Loan Data System (NSLDS). Officials within FSA Business Operations noted that security screenings are not performed for the individuals enrolled for NSLDS access under this capability, even though they will have access to sensitive PII, as they are not considered Federal or contractor staff. We reviewed the NSLDS System Security Policy and noted that the security screening requirements of the policy mirror the Directive and do not include any exceptions for external business partners. Therefore, we determined that this access was provided inappropriately. We followed up with FSA to obtain a response regarding our determination; however, no response was provided.

Under another contract, FSA staff explained that the contactor does not consistently complete the required access forms prior to granting FSA system access. When asked to elaborate, FSA staff noted there have been inconsistences in the Contractor Owned Contractor Operated environment related to FSA systems. FSA staff added that the contractor has allowed system access without completing the appropriate process. Staff and officials within FSA's Technology Office noted that FSA is in the process of addressing this issue, which includes the FSA Technology Office updating access documentation and standard operating procedures to reflect requirements for CORs and ISSOs to validate system access forms against the vendor provided access list. The Technology Office is also looking at requirements for automating the process. In other cases under other contracts, FSA could not provide an explanation as to why IT access was provided prematurely.

With regard to the two non-U.S. citizens included in our sample for which FSA could not provide any of the additionally required documentation and approvals, it appears that FSA lacks familiarity with the Directive requirements involving waiver information. Regarding the three foreign nationals FSA alerted us to who were found to be without security screenings but working with High Risk IT access under one of the contracts we reviewed, the Director of the Security Division within FSA Business Operations explained that the responsible ISSO(s) gave inappropriate system access to two of these individuals under the prior FSA contract they worked on, and then their system access rolled over to the successor contract. The FSA official added that it appeared the responsible CO and COR allowed these employees to work on the prior contract without having them complete the required paperwork based on the risk determination of the

position they held. We determined that FSA did not obtain the requested letters of reciprocity from the successor contractor to confirm that appropriate screenings had been completed for these individuals prior to the start of the new contract. The third foreign national with inappropriate High Risk IT access initially had a completed screening but did not have the appropriate reinvestigation initiated for continued High Risk work.

As noted above, the Department's information and systems include sensitive PII such as social security numbers and birth dates. If FSA does not deny a contractor employee High Risk level access to IT systems or Department sensitive or Privacy Act-protected information until the Chief of Personnel Security notifies FSA that a preliminary security screening was completed favorably, there may be contractor employees working with access to sensitive PII despite not being suitable for the access granted. Similarly, failure to appropriately document non-U.S. Citizen waiver information may hinder FSA's and the Department's ability to ensure that only non-U.S. Citizen contractor employees with appropriate security screening steps completed are provided High Risk access to Department information and IT systems. Based on our findings, it appears there may have been instances of unauthorized access to Department information and systems.

During audit fieldwork, FSA thanked OIG for bringing to FSA's attention contractor employees whose records need to be reviewed and assured that it will address those specifically. FSA also noted it agrees with OIG's conclusions that the security process needs to be reviewed, clarified, and documented. Effective May 10, 2017, FSA noted it convened a task force consisting of cross functional staff whose mission is to analyze the current process and develop an improved process.

Recommendations

We recommend that the Chief Operating Officer for FSA:

2.1 Identify and begin tracking all active contractor employees assigned to FSA contracts, along with their risk level and any IT access, to ensure that all contractor employees have undergone security screenings at appropriate risk levels as required by Department policy. For those who have not, take immediate action to complete the security screenings and/or deny further access to Department facilities, systems, and information until appropriate security screenings are completed or required screening information is submitted. Alert the Department CISO of the condition.

2.2 Determine through system security audit logs and other appropriate validation processes, if there were instances of unauthorized access to Department information and systems and report appropriately, at a minimum to the Department's CISO.

2.3 Ensure that security screenings and reinvestigations are initiated within the timeframes established by the Directive.

2.4 Ensure that all contractor employees complete the appropriate screening steps before receiving access to IT systems or Department sensitive or Privacy Act-protected information.

2.5 Ensure that contractor employees review and sign applicable Rules of Behavior for IT systems they are accessing.

2.6 Ensure that ISSOs maintain and exercise access approval rights over any IT systems that contain or can access sensitive Department data, whether owned by the Department or by the contractor, and modify applicable contracts accordingly to reflect the FSA ISSO approval rights.

2.7 Ensure that any contractor employees with discontinued or rejected investigations have all access to sensitive Department information, including any IT access, discontinued until appropriate screening steps have been completed. Alert the Department CISO should this condition exist.

2.8 Ensure that all non-U.S. citizens, current and prospective, are permitted to work on Department contracts only after appropriate steps have been taken with regard to waiver documentation, as required by the Directive.

2.9 Ensure that FSA staff are aware of and have an understanding of their responsibilities and applicable policies and procedures.

FSA Comments

FSA concurred with the recommendations. FSA noted that its Technology Office will work with other parts of the Department to ensure that all system access policies and procedures are documented and consistently followed. FSA noted that it will continue to work with other parts of the Department to review its internal processes to ensure that the required reviews, communications, and documentation are maintained according to the Directive. FSA also noted that its leadership will develop monitoring processes to ensure adherence to applicable processes and procedures.

Further, FSA described costs and risks that must be considered when planning for corrective actions. FSA noted that extended delays in background investigations and the limitations on system access based on such delayed background investigations for contractors can result in fewer contractors being available to achieve expected operational or developmental requirements. FSA noted that in turn, these unexpected delays and resource limitations may result in the need for millions of dollars in additional funding for project implementations, reductions in customer service for

contact center operations, or risks of operational failures due to fewer properly skilled resources available for systems operations and maintenance.

OIG Response

We did not make any changes to the finding or recommendations as a result of FSA's comments. As noted in the report, contractor employees whose positions are not designated as High Risk can start working under an FSA contract as soon as their complete security screening package is submitted to FSA through e-QIP. Contractor employees whose positions are designated as High Risk can start working under an FSA contract at the Moderate Risk level as soon as their complete security screening package is submitted to FSA through e-QIP, but must wait until OM notifies FSA that a preliminary screening was completed favorably before beginning work at the High Risk level under the contract. As such, ensuring that security screenings are initiated or verified within the timelines established in the Directive will assist with availability of contractor employees for contract work.

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 FSA. We reviewed applicable laws and regulations, Department and FSA policies and procedures, and the Government Accountability Office's (GAO) "Standards for Internal Control in the Federal Government." In addition, to identify potential vulnerabilities, we reviewed prior OIG, GAO, and other Federal agencies' audit reports with relevance to our audit objective.

We conducted discussions with FSA management and staff involved in FSA's contractor personnel security screening process. These discussions focused on FSA policies, procedures, and standard practices for conducting contractor personnel security screenings. In addition, we conducted discussions with officials and staff from OM regarding the office's role in oversight of the FSA contractor personnel security clearance process and their coordination with FSA during the process.

We focused our review on contracts that were active as of April 15, 2016. We obtained the listing of active contracts as of that date from the Department's publicly 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 FSA for review as it represented a significant number (125 or 22 percent) and dollar value ($763 million or 24 percent) of the active contracts within the Department at the outset of our review,[24] and because FSA contracts involve IT systems that access a considerable amount of sensitive PII and have a considerable number of contractor employees requiring screenings at the High Risk level. Because four of the top five highest-funded FSA contracts were TIVAS contracts, we judgmentally selected for review the two highest-funded TIVAS contracts and the next three highest-funded non-TIVAS contracts to diversify our sample. The five contracts we selected totaled $613,587,950 or 41 percent of the total $1.5 billion in contract funding for active FSA contracts. A listing of the contracts selected for review is included as Appendix B.

[24] We used a listing of Department contracts obtained from the Department's publicly available website that were active as of December 16, 2015, to determine which POs to include in our review.

Sampling Methodology

To determine whether FSA contractor employees received appropriate security screenings, we reviewed documentation for stratified random samples of contractor employees from each of the five FSA contracts we selected.

We received two separate listings of contractor employees for each of the five FSA contracts we selected for review. Each of the five contractor companies provided a listing of the active employees working on their contract as of the date they received the request for this information. Additionally, the Security Team provided a listing for each contract that included contractor employees with security screenings initiated or reinitiated by the Security Team from FY 2014 through the date of our request for this information (December 15, 2016). The Security Team listings also included information regarding any rejection by FSA, OM, or OPM of the contractor employees' security screening packages. We found discrepancies between the listings we received for each contract. As a result, our sampling methodology involved varying sampling approaches, as detailed below.

We divided the contractor employees for each of the contracts into the following groups: (1) contractor employees included on both the contractor company's listing and the corresponding Security Team listing without any discrepancies between the listings; (2) contractor employees included on both the contractor company's listing and the corresponding Security Team listing with indications on the Security Team listing that the security screening packages for these employees were rejected by either FSA, OM, or OPM; (3) contractor employees included on the contractor company's listing but not the corresponding Security Team listing;[25] and (4) contractor employees included on the Security Team listing but not the corresponding contractor company's listing.

For group 1, we reviewed a stratified random sample of 110 out of 4,116 contractor employees. To select the group 1 sample, we categorized contractor employees by risk level designation and randomly selected 15 contractor employees in positions designated as High Risk and 5 contractor employees in positions designated as Moderate Risk from each contract. One contract also included contractor employees with the TEMP 5C (short term) risk level designation; therefore, we separated TEMP 5C contractor employees from Moderate Risk contractor employees for this contract and

[25] We did not include contractor employees whose security screenings were initiated or reinitiated prior to FY 2014 and were included on the contractor companies' listings but not the corresponding Security Team listing because the Security Team listings began with security screenings initiated or reinitiated in FY 2014.

randomly selected an additional 10 contractor employees with the TEMP 5C risk designation for review. For each selected contractor employee, we reviewed records provided by contractor companies, intake staff, ISSOs, the Security Team, and OM, as well as security screening information from Security Manager, and evaluated attributes such as whether security screening investigations were completed, screenings were at the appropriate risk level, adjudication decisions were noted, and whether screening information was submitted in accordance with required timeframes. We also reviewed applicable contract position risk level documentation to determine designated contractor employee positions and risk levels. To determine whether FSA was providing High Risk access to contractor employees only after completion of a preliminary security screening, we reviewed available High Risk access data provided by FSA and contractor companies for the 75 contractor employees in positions designated as High Risk included in these samples, along with preliminary security screening completion dates found in Security Manager. To determine whether FSA was maintaining waiver information regarding non-U.S. Citizens, as required, we reviewed Security Manager information and requested documentation from FSA for the two applicable contractor employees from these samples.

As a result of significant discrepancies noted during our comparison of the listings of contractor employees we received from the contractors and the listings received from the Security Team, we reviewed documentation for an additional stratified random sample of 120 out of 1,108 contractor employees to determine whether they had appropriate security screenings initiated or whether they had appropriate screenings reinitiated after their security screening package was rejected by either FSA, OM, or OPM. We randomly selected 15 contractor employees out of group 2 from each contract (except for the contract with only 10 employees in group 2), and 10 out of group 3 from each contract. For each selected contractor employee from groups 2 and 3, we reviewed records provided by contractor companies, intake staff, ISSOs, and the Security Team, as well as security screening information from Security Manager, and evaluated whether these active contractor employees had appropriate security screenings initiated or reinitiated.

To determine whether contractor employee departure notifications occurred as required, we reviewed a stratified random sample of 50 out of 3,707 contractor employees. We randomly selected 10 contractor employees from group 4 for each contract. We then confirmed whether or not the selected contractor employees did in fact work on and then depart from the contracts. We confirmed that 41 of the 50 selected contractor employees departed from the contracts. For each of these contractor employees, we reviewed departure notification information provided by FSA staff and contractor companies, and evaluated whether contractor companies had notified FSA of departures as required and whether FSA had notified OM of departures

as required. We also evaluated whether PIV card collection procedures occurred as required.

Appendix E includes a breakdown of our selection of contractor employees by contract.

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 FSA and contractor companies, to include preliminary security screening completion dates. We noted issues with the data provided by FSA and contractor companies that limited our ability to reconcile the data, to include discrepancies between the listings of contractor employees provided. Additionally, the information provided by FSA 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 FSA implemented the requirements for the contractor employee security screening process.

We conducted fieldwork at Department offices in Washington, DC, during the period November 2016 through December 2017. We provided our audit results to Department officials during an exit conference conducted on December 5, 2017.

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. FSA Contracts Selected for Review

No.	Contractor Company	Contract Description	Contract Number	Contract Value (as of 4/15/2016)	Award Date	Key Department IT Systems Accessed[26]
1	Great Lakes Educational Loan Services, Inc.[27]	TIVAS	ED-FSA-09-D-0012	$204,962,248	6/17/2009	NSLDS; FMS;[28] COD[29]
2	Navient, LLC	TIVAS	ED-FSA-09-D-0015	$200,511,082	6/17/2009	NSLDS; FMS; COD
3	Maximus Federal Services, Inc.	DMCS	ED-FSA-13-C-0021	$126,715,465	9/30/2013	NSLDS; FMS
4	Dell Services Federal Government, Inc.[30]	VDC	ED-06-CO-0107/0021	$43,140,155	9/1/2014	NSLDS; CPS;[31] FMS[32]
5	Continental Services Group, Inc.	PCA	GS-23F-0084P/ED-FSA-15-O-0029	$38,259,000	4/22/2015	NSLDS

[26] This table includes key Department IT systems that may be accessed by contractor employees working under the contract listed; there are other Department IT systems that may be accessed by contractor employees working under the contract that are not listed.

[27] In February 2018, Great Lakes Educational Loan Services, Inc. was acquired by Nelnet.

[28] Financial Management System

[29] Common Origination and Disbursement System

[30] This contract expired in August 2016. The contract was recompeted as the Next Generation Data Center and awarded to Hewlett-Packard Enterprise Services.

[31] Central Processing System

[32] The VDC serves as the hosting facility for these systems.

Appendix C. 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 & Date	Printed Name & Date	Printed Name & Date
_____	_____	_____
Telephone	Telephone	Telephone

Appendix D. Summary of Investigative Types and Coverage

Background Investigation (BI)	Conducted for High Risk (6 or 6C) positions	PRSI (Personal Interview) Employment Education Residence Local Law Enforcement Court Records Credit National Agency Checks	Personal Interview 5 years 5 years and highest degree verified 3 years 5 years 5 years 7 years
Limited Background Investigation (LBI)	Agency option for Moderate Risk (5 or 5C) Positions.	PRSI (Personal Interview) Employment Education Residence References Local Law Enforcement Court Records Credit National Agency Checks	Personal Interview 3 years 3 years and highest degree verified 1 year 1 year 5 year 3 years 7 years
Minimum Background Investigation (MBI)	Agency option for Moderate Risk (5 or 5C) Positions. (Coverage is by inquiry only except for PRSI)	PRSI (Personal Interview) Employment Education Residence References Local Law Enforcement Credit National Agency Checks	Personal Interview 5 years (written inquiry) 5 years and highest degree verified (written inquiry) 3 years (written inquiry) Those Listed on Investigative Forms (written inquiry) 5 years 5 years 7 years
National Agency Check with Written Inquiries (NACI)	Conducted for Low Risk (1 or 1C) Positions.	Employment Education Residence References Law Enforcement NACs (National Agency Checks)	5 years 5 years and highest degree verified 3 years 5 years
National Agency Check with Written Inquiries and Credit (NACI-C)	Conducted for Moderate Risk (5 or 5C) Positions. Used at ED as the standard Moderate Risk investigation unless need to upgrade to MBI or LBI	Employment Education Residence References Law Enforcement NACs (National Agency Checks) Credit Check	5 years 5 years and highest degree verified 3 years 5 years 7 years
Periodic Reinvestigation – Residence (PRIR)	Conducted as a 5-year update for High Risk Computer/ADP positions	PRSI (Personal Interview) References Local Law Enforcement Residence NACs (National Agency Checks) – includes credit check	Personal Subject Interview 5 years 5 years 3 years

Appendix E. Contractor Employee Sample

Contract Number	Contractor Company	Total Contractor Employees Identified in Sampling Universes	Category	Category Universe Size	Sample Size	Selection Method
ED-FSA-09-D-0012	Great Lakes Educational Loan Services, Inc.	1794	(1) No discrepancy; High Risk	145	15	Random
			(1) No discrepancy; Moderate Risk	611	5	Random
			(2) Active with rejection indicated	95	15	Random
			(3) Active; not on Security Team listing	219	10	Random
			(4) Included only on Security Team listing	724	10	Random
ED-FSA-09-D-0015	Navient, LLC	4509	(1) No discrepancy; High Risk	419	15	Random
			(1) No discrepancy; Moderate Risk	1674	5	Random
			(2) Active with rejection indicated	154	15	Random
			(3) Active; not included on Security Team listing	246	10	Random
			(4) Included only on Security Team listing	2016	10	Random
ED-FSA-13-C-0021	Maximus Federal Services, Inc.	1376	(1) No discrepancy; High Risk	146	15	Random
			(1) No discrepancy; Moderate Risk	306	5	Random
			(1) No discrepancy; TEMP 5C	87	10	Random
			(2) Active with rejection indicated	79	15	Random
			(3) Active; not included on Security Team listing	94	10	Random
			(4) Included only on Security Team listing	664	10	Random
ED-06-CO-0107/0021	Dell Services Federal Government, Inc.	484	(1) No discrepancy; High Risk	286	15	Random
			(1) No discrepancy; Moderate Risk	8	5	Random
			(2) Active with rejection indicated	10	10	All Selected
			(3) Active; not included on Security Team listing	21	10	Random
			(4) Included only on Security Team listing	159	10	Random
GS-23F-0084P/ED-FSA-15-O-0029	Continental Service Group, Inc.	768	(1) No discrepancy; High Risk	26	15	Random
			(1) No discrepancy; Moderate Risk	408	5	Random
			(2) Active with rejection indicated	124	15	Random
			(3) Active; not included on Security Team listing	66	10	Random
			(4) Included only on Security Team listing	144	10	Random
Total		**8,931**		**8,931**	**280**	

Appendix F. Acronyms and Abbreviations

Acquisitions	FSA Acquisitions Group
CISO	Chief Information Security Officer
CO	Contracting Officer
COD	Common Origination and Disbursement System
COR	Contracting Officer's Representative
CPS	Central Processing System
CSO	Computer Security Officer
Department	U.S. Department of Education
Directive	OM Directive OM:5-101, Contractor Employee Personnel Security Screenings
DMCS	Debt Management Collection System
e-QIP	Electronic Questionnaires for Investigations Processing
FMS	Financial Management System
FSA	Federal Student Aid
FSA Manual	FSA Investigation Request Manual
FSEMS	Facilities, Security, and Emergency Management Services
FY	fiscal year
GAO	Government Accountability Office
ISSO	Information System Security Officer
IT	information technology

NACI	National Agency Check with Written Inquiries
NSLDS	National Student Loan Data System
OIG	Office of Inspector General
OM	Office of Management
OPM	Office of Personnel Management
PCA	Private Collection Agency
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PO	Principal Office
SAC	Special Agreement Check
Security Team	FSA Personnel Security Team
TIVAS	Title IV Additional Servicing
VDC	Virtual Data Center

Appendix G. FSA Response to the Draft Report

April 3, 2018

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

FROM: James F. Manning
Acting Chief Operating Officer
Federal Student Aid

SUBJECT: Response to Draft Audit Report:
Federal Student Aid's Contractor Personnel Security Clearance Process
Control No. ED-OIG/A19R0003

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft audit report on "Federal Student Aid's Contractor Personnel Security Clearance Process" dated February 16, 2018. The purpose of the audit was to assess the Federal Student Aid (FSA) contractor personnel security clearance process. We appreciate the work done by OIG and have taken a number of steps to strengthen the contractor personnel security clearance process not only within Federal Student Aid (FSA), but also within the Department as a whole.

FSA's leadership is committed to continued collaboration with the Office of Management (OM), Office of the Chief Information Officer (OCIO), Office of the Chief Financial Officer (OCFO), and the Institute for Education Sciences (IES) to discuss lessons learned, and develop standardized processes and procedures that will be followed across the Department. These procedures will also be in compliance with OM:5-101 guidance.

As the OIG recognized in the draft report, FSA, in conjunction with other Department units, has been proactive in resolving a number of the challenges identified by the OIG and in planning for the future. These actions include:

Immediate Actions

1. In May 2017, FSA convened a task force of staff from OM and FSA to develop improved personnel security processes that address identified deficiencies.

2. FSA has modified contracts to include clauses 39-5 - Monthly Vendor Reports and 39-6 - Security Protocol for Reporting Contract Employee Departure from a Contract.

3. The Secretary has approved the hiring of additional Personnel Security staff for OM and FSA. These additional positions increase overall current staffing levels by 225%. This level

of increase will substantially help in resolving issues identified. Both FSA and OM are working to fill the open positions.

4. FSA completed an analysis of an OIG identified list of 1,626 users by validating the OIG list against the contractor provided lists and system access audit logs. Of the 1,626 users, FSA found:
    - 13% had access removed;
    - 4% of users had actual system access;
    - Of those that had access, 78% had a 6C clearance but not the proper access records;
    - 16% of users had a 5C in lieu of a 6C clearance; and
    - 4% of users had a 6C clearance in process, but adjudications were not final.

5. The OCIO has scheduled regular monthly PIV (Personal Identity Verification) meetings to ensure all staff remain up to date on current policy, any potential issues, and upcoming changes.

6. In July 2017, the Department implemented the USAccess credentialing process to a pilot group of contractors. This process ensures that all contractors requiring a PIV not located near the DC metropolitan area or the regional offices are able to obtain the necessary credentials in a timely manner.

7. The Department has implemented policy changes by requiring personnel security approvals prior to gaining an EDUCATE (ed.gov) account.

8. The Department has implemented a new process for obtaining Privileged User Accounts on the EDUCATE network, to include verification from personnel security of their current background investigation. This new process is also now required to be repeated annually.

9. OM has developed training to ensure background package reviews are conducted properly, packages are coded correctly for the Office of Personnel Management's (OPM) National Background Investigations Bureau, and on the use of Security Manager. OM has provided this training to IES and will be pushing the training out to the rest of the Department, including FSA.

10. In 2016, the FSA e-Qip case return rate from the Office of Personnel Management (OPM) was at 87%. Because of quality control procedures and processes that have been instituted since that time, the return rate from OPM is less than 1%. This has helped ensure that we have no contractors who are working without an active investigation.

11. The OCIO and the FSA Chief Information Security Officer (CISO) have upgraded the incident response procedures.

Longer Term Solutions

1. Various offices across the Department are working together to establish the requirements and responsibilities that will be part of the process of expanding FSA's current Personnel Security Unit to perform background investigations from initiation to completed adjudication. In alignment with OM:5-101 and Department policy and procedures, this new unit is allowing FSA to be proactive in the process for the initiation of all background investigations with the exception of National Security; track and monitor investigation statuses in a timely manner; and have a clear line of authority and accountability of this process.

2. OM and FSA are working with the vendor of Security Manager to make changes that allow FSA to receive automatic notifications regarding the status of investigations.

3. FSA is working with OCIO, OCFO, and OM to further clarify roles and responsibilities of the staff responsible for background investigations and system access processes, while simultaneously initiating quality control processes to ensure processes and procedures are followed.

4. Under the leadership of the Deputy Chief Acquisition Officer and Senior Procurement Executive, the Department of Education Acquisition Regulation (EDAR) Program Working Group (EPWG), which consists of OCFO, OCIO, OM, and the Office of the General Counsel (OGC), have partnered to develop standardized language for consistently addressing cybersecurity and privacy requirements to be included in contracts awarded by the Department. Outcomes of the group are expected to result in standardized language to be added to Section C of the contract(s) that address Federal and ED cybersecurity and privacy requirements to include vendor responsibility and accountability efforts required during the performance of the contract(s). The Department will publish internal acquisition policies, guidance, and instructions to support standardized processes for access by the ED Acquisitions Workforce.

5. OM has worked with the project team of the Access Request Management System (ARMS) solution to establish requirements and potential interfaces to automate processes utilizing Security Manager.

6. The OCIO and the CISO have upgraded the incident response procedures and are working to create training to educate our vendors on violations, validations, and reporting requirements.

FSA, along with OCIO, OCFO, and OM, will collaborate to create a detailed plan that will identify tasks and timing to address the findings in the report and will ensure completion of that plan. This plan is expected to be completed by August 2018.

While the Department takes these findings very seriously, we need to also acknowledge that the extended delays in background investigations and the limitations on system access based on such delayed background investigations for contractors can result in fewer contractors being available to achieve expected operational or developmental requirements. In turn, these unexpected delays and resource limitations may result in the need for millions of dollars in additional funding for project implementations, reductions in customer service for contact center operations, or risks of operational failures due to fewer properly skilled resources available for systems operations and maintenance. These additional costs and risks are also impacts of the deficiencies noted by the OIG and must be considered when planning for corrective actions.

FSA recognizes and appreciates the OIG's concern that sensitive personally identifiable information (PII) "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." We have analyzed and balanced short-term and long-term risks, while being able to maintain performance levels and protect against inappropriate disclosure, and abuse by contractor employees. And, as a result, the Department is pleased to inform the OIG that we found no evidence of such disclosures and abuse, and we are moving forward to ensure this concern is fully remedied.

For the convenience of OIG, FSA has grouped the responses to the recommendations into like categories.

FINDING 1: FSA Did Not Effectively Implement Department Requirements for the Contractor Personnel Security Screening Process

FINDING 2: FSA Has Not Ensured That All Contractor Employees Have Appropriate Security Screenings and That Security Screenings Are Initiated or Verified in a Timely Manner

Staffing

Recommendation 1.1: Ensure staff involved in the contractor personnel security screening process are aware of and comply with the Directive requirements, to include any subsequent updates to the requirements, and fulfill their responsibilities for processing security screenings.

Recommendation 1.3: Have appropriate FSA staff develop and approve complete position category listings and associated risk level designations for all contractor positions on each contract, through FSA justification of position responsibilities and access, and through reconciliation of current contract position risk levels and any available position risk level designation records.

Recommendation 2.9: Ensure that FSA staff are aware of and have an understanding of their responsibilities and application policies and procedures.

FSA concurs with these recommendations. FSA leadership will continue to work with other parts of the Department to ensure that all staff responsible for personnel security screening, position category, and risk level designations understand their responsibilities, and have the appropriate procedures to ensure accuracy and consistency in processes. FSA leadership will develop monitoring processes to ensure adherence to applicable processes and procedures.

Policies/Procedures

Recommendation 1.2: Develop written policies and procedures to comply with the Directive, to include explanations of the key duties to be performed by specific FSA staff, requirements of the contract positions and risk designation process including the use of Position Designation Records (PDR), and other internal requirements for the FSA contractor personnel security screening process, as well as contractor employee departure procedures.

FSA concurs with these recommendations. FSA will continue to work with other parts of the Department to ensure that our written policies and procedures comply with OM:5-101.

Processes

Recommendation 1.4: Ensure that screenings are initiated at the appropriate risk level based on the contractor employee's position risk level that was classified and approved by FSA.

Recommendation 1.5: Coordinate with OM to learn the adjudication results of current contractor employees assigned to FSA contracts to ensure that all contractor employees either have a screening initiated or have been appropriately cleared to work on Department contracts.

Recommendation 1.6: Monitor the screening status of contractor employees until final OM adjudication decisions are made.

Recommendation 1.7: Maintain all information and records required by the Directive, to include up-to-date listings of all contractor employees assigned to FSA contracts and records of OM adjudication decisions for all contractor employees assigned to FSA contracts.

Recommendation 1.8: Ensure that all contractor employee departures are reported to OM as required, and inform contractor companies on a regular basis of their responsibility to notify FSA of contractor employee departures. Also ensure that contractors provide PIV cards to the COR upon contractor employee departure, as required.

Recommendation 2.3: Ensure that security screenings and reinvestigations are initiated within the timeframes established by the Directive.

Recommendation 2.8: Ensure that all non-U.S. citizens, current, and prospective, are permitted to work on Department contracts only after appropriate steps have been taken with regard to waiver documentation, as required by the Directive.

FSA concurs with these recommendations. FSA will continue to work with other parts of the Department to review our internal processes to ensure that the required reviews, communications, and documentation are maintained according to OM:5-101. FSA Leadership will develop monitoring processes to ensure adherence to applicable processes and procedures.

System Access

Recommendation 2.1: Identify and begin tracking all active contractor employees assigned to FSA contracts, along with their risk level and any IT access, to ensure that all contractor employees have undergone security screenings at appropriate risk levels as required by Department policy. For those who have not, take immediate action to complete the security screening and/or deny further access to Department facilities, systems, and information until appropriate security screenings are completed or required screening information is submitted. Alert the Department CISO of the condition.

Recommendation 2.2: Determine through system security audit logs and other appropriate validation processes, if there were instances of unauthorized access to Department information and system and report appropriately, at a minimum to the Department's CISO.

Recommendation 2.4: Ensure that all contractor employees complete the appropriate screening steps before receiving access to IT systems or Department sensitive or Privacy Act-protected information.

Recommendation 2.5: Ensure that contractor employees review and sign applicable Rules of Behavior for IT systems they are accessing.

Recommendation 2.6: Ensure that ISSOs maintain and exercise access approval rights over any IT systems that contain or can access sensitive Department data, whether owned by the Department or by the contractor, and modify applicable contracts accordingly to reflect the FSA ISSO approval rights.

Recommendation 2.7: Ensure that any contractor employees with discontinued or rejected investigations have all access to sensitive Department information, including any IT access, discontinued until appropriate screens steps have been completed. Alert the Department CISO should this condition exit.

FSA concurs with these recommendations. FSA's Technology Office will work with other parts of the Department to ensure that all system access policies and procedures are documented and consistently followed. FSA leadership will develop monitoring processes to ensure adherence to processes and procedures.

We appreciate the effort you have made on this audit work, and we appreciate this opportunity to comment and provide technical comments as well. We hope you find this response helpful. Please let me know if you have questions or need further information.

Enclosure: Technical Comments