UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES

March 8, 2017

**Control Number**
**ED-OIG/A19R0002**

Thomas Brock
Commissioner for Education Research
Delegated Duties of the Director
Institute of Education Sciences
U.S. Department of Education
400 Maryland Avenue, S.W.
Washington, DC 20202-4300

Dear Mr. Brock:

This **final audit report**, titled *The Institute of Education Sciences' Contractor Personnel Security Clearance Process*, presents the results of our audit. This audit was part of a review of the Department of Education's (Department) contractor personnel security screening process being performed in several principal offices (PO). The objective of the audit was to determine whether the Department has effectively implemented the requirements for contractor personnel security screenings. 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.

## 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 information technology (IT) system access, require access to unclassified sensitive information, or perform duties in a school or location where children are present. The Department's requirements for the contractor personnel security screening process are primarily found in OM Directive: 5-101, *Contractor Employee Personnel Security Screenings* (Directive), dated July 16, 2010.

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 the Institute of Education Sciences (IES), primary responsibility for contractor personnel security screenings belongs to IES Contracting Officer's Representatives (CORs) for individual contracts and the Statistical Standards and Data Confidentiality (referred to in this report as SSDC) staff within IES's National Center for Education Statistics (NCES). CORs are responsible for facilitating information exchange between contractor companies and SSDC, tracking and monitoring contractor employee security screenings, and maintaining security screening information. SSDC is responsible for creating contractor employee accounts in e-QIP, reviewing security screening information, and initiating contractor employee security screenings with OM.

Processing an IES contractor employee's security screening involves coordination between the contractor company and employee, the COR for the contract, SSDC, OM, and OPM. The process begins with the contractor company submitting a contractor employee's name and information to the COR to inform the Department of the contractor employee's assignment to the contract and to initiate the security screening. The COR provides the initial information to SSDC staff who create an account for the contractor employee in e-QIP, assist the contractor employee with submitting required information, and review the information for completeness. SSDC then releases the contractor employee's information in e-QIP to OM and provides OM with a hardcopy security package that includes a Request for Security Officer Action form, fingerprint documents, and required signature pages. Contractor employees who are not designated as high risk can start working under a Department contract as soon as their complete security package is submitted to OM for processing. Once OM staff receive a security package, they input the contractor employee's information into Security Manager and electronically provide the necessary information to OPM to initiate a background investigation. After OPM conducts the requested background investigation, it provides the results in a report to OM. OM reviews the background investigation report and makes a final personnel security adjudication determination on whether the contractor employee is suitable for employment on the Department contract.

We selected IES for review because it represented a significant number and dollar value of the active contracts within the Department as of December 16, 2015. We selected for further review the five IES contracts with the highest dollar value as of that date, including a random sample of 95 contractor employees assigned to these contracts.[1] A listing of the contracts selected for review is included as Attachment 2 to this report.

[1] Probability of selection varied by contract and percentages reported reflect unweighted results and are not projectable. See "Sampling Methodology" in Objective, Scope and Methodology for details.

# AUDIT RESULTS

Overall, we found that IES did not effectively implement Department requirements for the contractor personnel security screening process. We specifically noted weaknesses in IES's development of internal policies and procedures, designation of contract positions and position risk levels, notification and maintenance of security screening decisions and other related information, and inclusion of required contract provisions in contract solicitations. We found that IES staff and officials involved in the process were generally unaware of Department requirements and their related responsibilities for processing contractor employees' security screenings.

We also determined that IES has not ensured that all contractor employees have appropriate security screenings and that security screenings are initiated in a timely manner. We determined that 81 of the 95 contractor employees in our sample required a security screening. We found that there was no evidence of an appropriate security screening for 48 (59 percent) of the 81 contractor employees.[2] We found that an additional 15 (19 percent) of the 81 contractor employees received security screenings under a prior Department contract they worked on or for prior employment at another Federal agency, but IES did not verify the screenings for any of these employees as required.[3] We also found that IES did not always initiate the screenings within the 14-day timeframe established by the Directive.

Because IES 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, unclassified sensitive information, and/or school children are suitable for the level of access granted to them. Additionally, the Department's information and systems might be vulnerable to 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.

In its response to the draft audit report, IES acknowledged that its contractor personnel security screening process could be improved and committed to implementing the recommendations, but stated that it will need support and assistance from OM and Contracts and Acquisitions Management (CAM) staff in the Office of the Chief Financial Officer (OCFO) to do so. IES noted that it is pleased that the draft report acknowledged the action IES has already taken since the audit was initiated to develop detailed policies and procedures to ensure that IES employees are aware of their responsibilities under the Directive. Based on the recommendations in the draft report, IES stated that it has further revised its procedural documentation for complying with the Directive, assigned additional staff to serve as IES Contractor Personnel Security Representatives, and provided detailed guidance to all IES CORs to clarify their responsibilities as well as the roles of the IES Contractor Personnel Security Representatives, Computer Security

[2] Of the 48 contractor employees we determined did not have evidence of an appropriate security screening, 30 were in moderate risk positions and 18 were in low risk positions.

[3] Of the 15 contractor employees with a prior screening that IES did not verify, 12 were in moderate risk positions and 3 were in low risk positions.

Official, and Executive Officer in the screening process. IES also provided proposed action steps addressing each recommendation.

IES's comments are summarized at the end of each finding. We did not make any changes to the audit findings or the related recommendations as a result of IES's comments. The full text of IES's response is included as Attachment 6 to this report.

## FINDING NO. 1 – IES Did Not Effectively Implement Department Requirements for the Contractor Personnel Security Screening Process

We found that IES 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 position risk levels;
- notification and maintenance of security screening decisions;
- maintenance of contract position, risk, and employee information; and
- inclusion of required contract provisions in contract solicitations.

During the course of the audit we found that IES 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).

### *IES Policies and Procedures*

We found that IES has not established internal written policies and procedures that comply with the Directive. While IES has a procedural guide for its contractor employee security screening process entitled, "NCES Contractor Security Clearance Process Guide," developed by SSDC staff, we found that this document does not fulfill all Directive requirements. Specifically, we noted that the IES procedural guide does not identify all responsible officials involved in the contractor personnel security screening process that will perform key duties, to include the IES Computer Security Officer (CSO) and IES Executive Officer, and does not provide complete information on COR responsibilities. In addition, the guide does not explain requirements for certain areas of the screening process such as the contract position risk designation process, how IES staff should handle contractor employee reinvestigations, or how IES should maintain security screening information, including lists of contract positions and risk levels, and contractor employee security screening records. The guide 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.

We also noted the IES procedural guide was not finalized, and it does not appear the guide was ever submitted to OM for review and to maintain on file as required by the Directive. Subsequent to our fieldwork, we were informed that IES has submitted a revised guide to OM that is pending review. We found that the revised guide provides information not included in the original guide such as specific responsibilities for IES CORs and the CSO during the contractor employee security screening process and reinvestigation initiation requirements; however, the revised guide does not specify a role for the IES Executive Officer in the contractor security screening process and does not specify a requirement for the use of Position Designation Records. An IES official noted at the exit conference that the updated procedural guide is now in use within IES and an OM official stated that the revised guide is pending OM review. 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, its own procedural document for complying with the Directive. The document will identify the responsible officials such as CORs, CSOs, 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.

We found that the original IES procedural guide was created by SSDC in order to help SSDC staff with consistency during the processing of contractor employees' security screenings. SSDC's role is limited to managing the contractor security screening process through e-QIP and submitting contractor employee security screening packages to OM. The IES guide is therefore limited in scope to the elements of the contractor security screening process that are directly under the purview of SSDC. SSDC staff stated that the IES guide is constantly under revision due to continuing changes in requirements from OM and OPM. SSDC staff stated that some changes to the security screening process are not yet in writing.

Without a comprehensive internal IES procedural document for the contractor personnel security screening process, IES cannot ensure that all IES 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 Position Risk Levels*

We found that IES's process for determining contractor positions and risk levels does not involve all staff and officials required by the Directive. While 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, the IES CSO stated that he does not have any input in the determination of position risk levels during the preparation phase of the contract solicitation. He stated that his role is to verify that the correct clearance level is requested for a contractor employee when submitting security screening packages to OM, and to verify the existence of clearances prior to granting contractor employees access to Department and IES information systems. As described by the CSO, this involvement occurs after position risk levels have already been designated and after specific contract positions have been assigned to individual contractor employees. The Executive Officer is also required to concur in writing with each contract position risk designation; however the IES Executive Officer stated that she does not have a role in this process. Additionally, IES staff did not identify any role for the Chief of Personnel Security in the process and there is no role identified in the IES procedural guide.

We also found that IES did not use or maintain Position Designation Records for any contract positions included in the five contracts we reviewed. A PO is required to use a Position Designation Record to provide a written justification for classification of a contract position as high, moderate, low, or no risk and for key officials to concur in writing with the assigned risk level. IES did not provide any documentation to support position risk designations or written approval from required officials for the contracts we reviewed. A copy of the Position Designation Record is included as Attachment 3 to this report.

Lastly, we found that IES does not ensure that the actual positions and risk levels assigned to individual contractor employees correspond to the positions and risk levels designated in contract solicitations and final approved contracts. For example, for one contract we reviewed, 12 positions/labor categories were identified in the solicitation, but 59 contractor employees occupied positions that we could not directly match to the 12 positions/labor categories from the solicitation. We found similar circumstances for three other contracts we reviewed. For another contract, the contractor assigned some employees to a labor category that was not included in the solicitation or final contract and left the risk level as undefined. Although the risk level was undefined for the labor category, the contractor company determined on its own that some contractor employees within the labor category should receive security screenings and others should not. New positions and labor categories can be added to a contract if approved by IES; however, for the additional positions we identified, there was no documentation to support that these had received IES approval prior to assignment.

Section VI, Parts A.3 - A.4 of the Directive state that a PO must assign a position risk level to each applicable contractor employee position, before the solicitation is released, in coordination with the CSO and the Chief of Personnel Security. The CSO must concur in writing with the designated risk level. 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. Section VI, Part A.3 states that the PO must maintain a current position risk level designation record for each contractor position to which the Directive applies.

As noted above, the original IES procedural guide does not provide any information on the roles of the IES CSO and Executive Officer, does not provide complete information on COR responsibilities, and does not explain the requirements for the contract position risk designation process such as the use of Position Designation Records. As a result, IES officials and staff do not appear to be familiar with their expected roles in the security screening process or be aware of specific requirements from the Directive. For example, one COR said that she does not know who was responsible for determining and approving position risk levels for her contract or why specific risk designations had been made. We also noted that CORs seemed generally unaware that the Directive required use of Position Designation Records for assigning position risk levels. In addition, CORs were not always aware of contractors adding positions to the contract and whether the positions and risk levels assigned to contractor employees received preapproval from IES officials.

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

During our exit conference, IES officials stated that the CSO is involved in the contractor position and risk designation process by reviewing and approving contract Statements of Work (SOW). We note that while SOWs include general requirements for contractor employee security screenings, they do not include specific position and risk level information for individual contract positions. IES officials also noted that there is an emphasis on CSO involvement in this process and IT-related risks, but wanted to point out their concern that the Directive deems contractor employees that will have access to school children as low risk. The officials suggested that this designation should be reconsidered by OM.

*Notification and Maintenance of Security Screening Decisions*

We found that for each of the five contracts we reviewed, IES did not maintain records of final OM personnel security adjudication determinations for individual contractor employees and did not inform relevant parties including the CO, CSO, or contractor companies of these final determinations as required by the Directive. In general, we noted that CORs were unaware of a contractor employee's screening status after submitting the security package information to SSDC, and SSDC was unaware of the screening status after submitting the information to OM. We also identified cases where IES staff incorrectly provided us the date of OPM's background investigation closure as support for the final security adjudication determinations. OPM background investigations provide information for the Department to use as the basis for suitability determinations. Only OM can make the final determination on suitability after reviewing the information provided.

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.

IES staff stated that IES does not receive notification of final adjudication decisions from OM and an IES official noted that the lack of notification from OM is a weakness in the security screening process. OM officials verified that OM does not notify POs of final adjudication decisions. OM officials stated that OM has an agreement with POs that if PO staff do not receive adjudication results from OM during the security screening process for a particular contractor employee, then the PO should assume that everything is acceptable with the security screening. OM officials noted that if there is an unfavorable adjudication determination, OM will notify the COR and CO for the contract by sending an email with an official letter attached.

Without notification of an adjudication determination from OM, IES must review information in Security Manager or contact OM staff directly in order to determine the status of a contractor employee's security screening. However, access to Security Manager was only recently provided to IES in 2015, and access was only provided to the employees that work in the SSDC group. IES also noted that Security Manager does not provide a batch search function. Each contractor employee needs to be individually reviewed to determine the screening status. In addition, IES officials noted that IES's contractors employ thousands of employees that need clearances, including periodic reinvestigations, and that all of these things can hinder IES's ability to effectively implement the contractor security clearance process.

In cases when IES is not aware of final OM adjudication decisions or when IES staff incorrectly assume that an employee is cleared after the OPM investigation is completed, contractor employees may be allowed to work on Department contracts without complete and appropriate screenings.

*Maintenance of Contract Position, Risk, and Employee Information*

We found that IES 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. We requested this information from the applicable CORs and SSDC staff for each of the five contracts we reviewed. We received lists from the CORs for all five contracts and lists from SSDC for three of the five contracts.[4]

We found that both the COR and SSDC lists omitted contractor employees who should have been included on the lists and that the SSDC lists mistakenly included employees on the lists who were not assigned to the contracts. For the three contracts where we were able to obtain lists from both the COR and SSDC staff, we noted that the names on the lists did not match. Additionally, many of the individual positions and risk levels noted in these lists did not correspond to the positions and risk levels noted in the contract solicitations and contract documents. CORs were not aware that these positions and risk levels had been assigned to contractor employees and were not always able to match these new positions to the positions from the solicitation or contract documents. SSDC does not generally maintain contract position information for individual contractor employees. We also noted risk levels were not listed or were listed as "undefined." CORs stated that they were not able to provide this information because it was unavailable from the contractor companies or that the risk levels for the positions had never been defined.

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.

CORs informed us that they do not independently maintain information on individual contractor employees. To respond to our requests for information, CORs asked contractor companies to provide the information. CORs stated that generally during the course of contract performance, they rely on monthly budget reports from contractor companies to provide up-to-date information on the contractor employees currently assigned to their contracts. We found that CORs were able to provide required information such as current contractor employees, position risk levels, and significant dates only to the extent this information was maintained by the

[4] SSDC stated that their lists contained only contractor employees that had been processed by SSDC staff. According to the COR, there were no contractor employees screened for one contract we reviewed. Therefore, SSDC did not provide a list of contractor employees for this contract. For the other contract where SSDC did not provide a list, SSDC explained that employee names are recorded under the contract number for which they first received a security screening. Subsequent contract numbers may not be associated with the contractor employee. For a given contract number, SSDC will not be able to identify contractor employees assigned to that number if they are in SSDC records under a different contract number. SSDC said that there may have been no contractor employees assigned to the contract number we requested in SSDC records.

contractor companies. One COR noted that it is difficult to maintain contractor records because contractor employee turnover on contracts is very high.

SSDC stated that it maintains records only for contractor employees that are processed by the team and does not track contract positions. Therefore, SSDC records alone do not fulfill the requirements of the Directive.

If IES 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 assigned risk levels, and monitor contractor employees' screening statuses. Failure to appropriately track and maintain this information may result in IES's inability to ensure that only contractor employees with appropriate security screenings are working on Department contracts.

### *Required Contract Provision*

We found that the solicitations for three of the five contracts we reviewed did not contain a required contractor security screening provision: "Notice to offerors of Department security requirements." The three contracts were awarded under the same solicitation and the solicitation omitted this provision.

Section VI, Part B.3 of the Directive states that all active solicitations and contracts meeting the requirements of the Directive will include personnel security screening requirements for Department contractor employees. The regulations at 48 C.F.R. § 3439.702, "Department security requirements," state that a contract must include the solicitation provision in 48 C.F.R. § 3452.239–71, "Notice to offerors of Department security requirements," when contractor employees will have access to Department-controlled facilities or space, or when the work (wherever located) involves the design, operation, repair, or maintenance of information systems and access to sensitive but unclassified information. The provision includes a notice to the offeror of the requirement to indicate the offeror's proposed positions for the employees it anticipates using to perform the contract and their proposed risk levels based on the guidance in the Directive.

According to OCFO CAM staff, the required provision was inadvertently omitted from the solicitation for the three reviewed contracts. If required provisions and clauses are not included in solicitations and contracts, contractor companies may not be fully aware of their obligations regarding personnel security screenings.

### **Recommendations:**

We recommend that the Director of IES:

1.1 Ensure that staff involved in the contractor personnel security screening process are aware of and comply with the Directive 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 IES staff, requirements of the contract positions and risk designation process including the use of Position Designation

Records, and other internal requirements for the IES contractor personnel security screening process.

1.3 Actively coordinate with OM to learn the adjudication results of current contractor employees assigned to IES contracts to ensure that all contractor employees have been appropriately cleared to work on Department contracts.

1.4 Reconcile contractor positions with approved position categories and risk level designations and ensure that any changes to positions or risk levels receive appropriate approval.

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

1.6 Maintain all information and records required by the Directive, to include records of OM adjudication decisions for all contractor employees assigned to IES contracts.

1.7 Coordinate with CAM to ensure that all required provisions and clauses are included in contract solicitations and final contract documents.

**IES Comments**

IES acknowledged the issues identified and stated it is committed to implementing the recommendations as efficiently as possible. IES stated that in addition to the steps it has already taken to enhance its existing contractor employee security protocols, it is in the process of developing a database that will enable IES CORs and Contractor Personnel Security Representatives to track personnel assigned to its contracts, their assessed risk levels, and their screening status. IES also noted that it is in the process of training all IES CORs on their responsibilities related to contractor personnel security screening and will require that all future IES CORs complete this training.

IES stated that without notification from OM regarding security screening determinations, it cannot ensure that its contractors are in compliance with these requirements. IES noted that it is concerned that the variability in the length of time required for the investigations and adjudications makes it impossible for IES CORs to know when they can safely assume that a clearance has been granted. IES also noted that the requirement that offices initiate security screenings within 14 days is not always feasible, particularly when IES is seeking clearance for several hundred contractor personnel at the same time. IES stated it hopes that the Department will consider revising the Directive to address these concerns.

**OIG Response**

We did not make any changes to the audit finding or the related recommendations as a result of IES's comments. Upon completion of the audits of the contractor personnel security screening process in individual POs, we will be providing a summary report to OM that will include observations from the individual PO audits and include any findings and recommendations identified that require attention by OM.

## FINDING NO. 2 – IES Has Not Ensured That All Contractor Employees Have Appropriate Security Screenings and That Security Screenings Are Initiated in a Timely Manner

### *Security Screening Coverage*

We reviewed IES records and information contained in Security Manager for a sample of 95 contractor employees from the five contracts we reviewed to determine whether IES ensured that contractor employees received an appropriate security screening. An appropriate security screening includes an OPM background investigation conducted at the appropriate risk level and a favorable adjudication decision from OM. We determined that 81 of the 95 contractor employees in the sample required a security screening.[5] We found that there was no evidence of an appropriate security screening for 48 (59 percent) of the 81 contractor employees.

Specifically, for 32 of the 48 contractor employees, there were no records in Security Manager, no record of any previous or ongoing OPM background investigation, and no record of any adjudication determination from OM. We found that the remaining 16 contractor employees did have some records in Security Manager, indicating that a screening was initiated with OM, but there was insufficient evidence that a complete security screening ever occurred. For 9 of the 16 contractor employees, there was evidence that an OPM background investigation was conducted and it was at the appropriate risk level, but there was no evidence of any OM adjudication decision. For 5 of the 16 contractor employees, there was no evidence that the required OPM background investigation was ever completed. For the remaining two 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.

We found that these 48 contractor employees were permitted to work on their contracts for significant periods of time without ever completing an appropriate security screening, as follows:

- 14 (29 percent) were on the contract for less than 1 year;
- 12 (25 percent) were on the contract between 1 year and 2 years;
- 4 (8 percent) were on the contract between 2 and 3 years;
- 18 (38 percent) were on the contract more than 3 years.

We determined that an additional 15 (19 percent) of the 81 contractor employees received security screenings under a prior Department contract they worked on or for prior employment at another Federal agency. We found that IES did not verify the screenings for any of these 15 employees.[6]

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:

[5] The remaining 14 employees did not require a security screening because they did not meet 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.

[6] As part of our review, we verified through Security Manager that screenings had been completed for each of these employees, were at the appropriate risk level, and had favorable OM adjudication decisions.

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[7] as the following:

- 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.

For the 32 employees with no records in Security Manager, the primary reasons we noted were that the contractor company did not provide any security package information to IES, IES did not submit information to OM, or IES stated that it submitted information to OM, but could not provide documentation to verify the submission.

Specifically, for 17 of the 32 contractor employees, the contractor company did not provide any security package information to IES. These contractor employees were all assigned to one contract. For this contract, the COR informed us that none of the contractor employees assigned to the contract had undergone a security screening because IES determined at the start of the contract that none of the employees needed a security screening because the employees would not be handling personally identifiable information. Therefore, IES never initiated security screenings for any of the contractor employees and did not request that the contractor company submit information. We determined, however, that seven of the contractor employees occupied positions that were specifically designated as low risk on the COR list provided by IES. The remaining 10 employees were designated as no risk level on the COR list. Based on our review of position titles and risk levels contained in the contract solicitation, we determined that all 17 of these employees occupied positions similar or identical to positions that had been designated as low or moderate risk and therefore required security screenings.

[7] See Attachment 4 for a detailed summary of investigative types and coverage as included in the Directive.

For 14 of the 32 contractor employees, IES received information from the contractor company but did not submit security packages to OM. For these contractor employees, IES explained that in some cases it did not receive complete information from the contractor companies and that SSDC recently experienced problems with the e-QIP site that prevented submission of information to OM. In some cases, IES could not explain why the contractor employees' information was not submitted to OM. We note that many of these contractor employees were working on their respective contracts for months or years without IES submitting information to OM. Recent problems with the e-QIP site should not have impacted IES's ability to submit information to OM for these contractor employees assigned to the contracts in prior years.

For the remaining contractor employee without a record in Security Manager, IES stated that it provided a security package to OM; however, OM officials stated that OM does not have any record of receiving a security package from IES for this contractor employee.

Of the 16 contractor employees with some records in Security Manager, there were 9 contractor employees where there was evidence that the appropriate OPM background investigation was completed, but there was no evidence of a final adjudication determination from OM. When asked why these nine cases were not adjudicated, OM stated that for two cases the adjudications were inadvertently left incomplete, for four cases the contractor employees separated from the contract prior to a determination being made, and for the remaining three cases there was no information available on why there was no adjudication determination.

IES staff gave varying reasons why they did not verify prior Department or other Federal agency screenings. One COR explained that she did not verify prior screenings because the contractor company did not inform her that the contractor employees had prior security screenings. This COR did not explain why she did not initiate screenings for these employees absent that knowledge. Another COR indicated that he could not provide an explanation of verifications because SSDC is the only staff with access to the related records. Two of the CORs and SSDC did not offer any explanation for the lack of verification for individual contractor employees.

It does not appear that IES staff have a full understanding of their responsibilities related to prior screening verifications. When a contractor employee is assigned to a contract in a position requiring a security screening, IES should either initiate a new security screening or verify that a prior security screening provides coverage. It is the responsibility of IES to request this information from the contractor company and verify the prior screening with OM.

We noted that the five contracts included in our review required contractor employees to have access to sensitive information such as personally identifiable information or other Privacy Act protected information because the contractors are conducting surveys and assessments of students, with at least one of the contracts appearing to allow for direct access to minor children to collect this information. We also noted that at least one of the contracts required access to Department IT systems. Because IES 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, unclassified sensitive information, and/or school children are suitable for the level of access granted to them. The Department's information and systems might be vulnerable to inappropriate disclosure and abuse by contractor employees who may not meet security standards.

*Security Screening Timeliness*

We reviewed documentation for the 81 contractor employees in our sample that were required to have a security screening to determine whether IES initiated the screenings within established timeframes. We identified 22 contractor employees for which IES submitted the required paperwork to OM for a contract we reviewed. We determined that only 9 (41 percent) had their forms submitted within the required 14 day timeframe established by the Directive. We were unable to determine whether forms were submitted within the required timeframe for five employees.[8]

Section VI, Part C.3 of the Directive states that each contractor company must ensure that its contractor employees submit all required personnel security forms to the COR within 2 business days of assignment to a Department contract. If the required forms are not complete, the contractor company 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.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, *except* for contractor employees in High Risk IT (6C) Level positions who require preliminary personnel security screenings. 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. Part A 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.

Part A.9 of the Directive also states that the PO must maintain the date a contractor employee's previous screening information was submitted and that 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.

The IES procedural guide states, "All contractor employees must have submitted all required personnel security forms for the security clearance process or have an existing security clearance validated before assignment to an ED [Department] contract."

IES staff offered different explanations for why security screenings were not initiated in a timely manner. They stated that in many cases the security screenings are still pending because the contractor employee or company has not submitted required information. We note that several of these contractor employees have been working on their contracts for months or years without having submitted the required information.

For some contractor employees, IES staff stated that they were unaware that security screenings had not been initiated with OM or stated that they inadvertently failed to initiate or ensure completion of a security screening. As discussed in Finding 1, CORs do not generally track security screenings once they have provided information to SSDC.

[8] IES was unable to provide us either the day the contract employee was assigned to the contract or the date that information was provided to OM.

If IES does not ensure that security screenings are initiated 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.

At the exit conference, IES officials added that there is no official “stop-work” date when contractor employees continue to provide incomplete or incorrect information to the IES CORs and SSDC staff. They also noted that in certain cases, a contractor employee’s work is complete before the employee’s information is processed, which makes continuation of the processing pointless. They added that the 14 day timeframe is unrealistic due to the volume of contractor employees that CORs and SSDC must process and because IES must rely on contractor companies with regard to submission of information. One IES official also noted that OM does not enforce the 14 day timeframe. IES suggested that the security screening process may need to be broken into sub-timeframes to ensure more efficient processing.

At the conclusion of our exit conference, IES officials provided some additional information regarding current efforts in this area as well as ongoing concerns. Specifically, the IES officials noted that IES has already begun implementing changes to its screening process to fix some of the issues discussed. Officials noted SSDC now has three employees instead of only two and the staff are assigned to work with specific CORs and supervisors to better ensure accountability. Officials also noted that these teams have meetings to discuss COR involvement in key steps and to make sure CORs understand the work flow and processing requirements of the Directive, while receiving other more specific guidance for IES contracts. They stated that a team has been assigned to address security screening issues and training.

**Recommendations:**

We recommend that the Director of IES:

2.1 Ensure that all currently active contractor employees assigned to IES contracts have undergone security screenings at appropriate risk levels as required by Department policy. For those who have not, take immediate action to initiate and complete the security screenings. For contractor employees that do not timely submit the required information, coordinate with the Office of the General Counsel and CAM to determine the appropriate course of action, including removal of these employees from their respective contracts.

2.2 Ensure that all future contractor employees obtain appropriate security screenings.

2.3 Ensure that contractor security screenings are initiated within 14 days as required by the Directive.

2.4 Ensure IES staff are aware of and have an understanding of their responsibilities and applicable policies and procedures.

**IES Comments**

IES did not disagree with the finding and stated that it is committed to implementing the related recommendations, but acknowledged that it will take time to reconcile security screening records for contractor personnel on existing contracts. IES stated that for this reason, it is proposing corrective actions in collaboration with the Chief of Personnel Security, the Office of the General Counsel, and CAM that would enable IES to give priority to addressing the most pressing security needs and establish consequences for contractors if their employees do not meet the security screening requirements. IES noted that based on its proposed corrective actions, its intent is to have initiated all required security screenings for contractor personnel on existing contracts by the end of July 2017. IES stated that it will work closely with OM and its contractors to monitor the completion of these screenings.

**OIG Response**

We did not make any changes to the audit finding or the related recommendations as a result of IES's comments.

## OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit was to determine whether the Department has effectively implemented the requirements for contractor personnel security screenings.

To answer our objective, we gained an understanding of internal controls applicable to the Department's contractor personnel security screening process at IES. We reviewed applicable laws and regulations, Department and IES 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 IES management and staff involved in IES's contractor personnel security screening process. These discussions focused on IES policies, procedures, and standard practices for conducting contractor personnel security screenings. In addition, we conducted discussions with officials and staff from OCFO and OM regarding these offices' roles in oversight of the IES contractor personnel security clearance process and their coordination with IES during the process.

We focused our review on contracts that were active as of December 16, 2015. We obtained the listing of active contracts as of that date for all principal offices 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 IES for review as it represented the PO with the highest number of active contracts (204 or 36 percent) and highest overall contract dollar value ($1.6 billion or 49 percent). We selected for further review the five IES contracts with the highest dollar value. These contracts totaled $462,660,752 or 29 percent of the total $1.6 billion in contract funding for active IES contracts. See Attachment 2 for a list of the contracts selected for review, and the applicable contract dollar value.

Sampling Methodology

To determine whether IES contractor employees received the appropriate security screenings, we reviewed documentation for random samples of contractor employees from each of the 5 IES contracts we selected. In total, we reviewed 95 contractor employees out of the total 6,391 from all 5 contracts. For each selected contractor employee, we reviewed records provided by CORs, SSDC, and OM, as well as security screening data from Security Manager, and evaluated attributes such as whether security screenings 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 solicitations and final contracts to determine designated contractor employee positions and risk levels.

We selected the samples of contractor employees from separate lists as provided by the CORs for each contract. Each contract's list contained different information regarding contractor employee positions and risk levels. [See Finding 1 for additional information.] Since we intended to categorize contract employees by risk level for selecting the sample, the inconsistencies among the lists resulted in varying sampling approaches, as detailed below. A summary listing of the contractor employee samples selected is included as Attachment 5 to this report.

(1) ED-05-CO-0033- Research Triangle Institute

We identified a universe of 341 contractor employees. We categorized the contractor employees by risk level designation. We randomly selected 10 from the 202 contractor employees designated as moderate risk. We also randomly selected 10 from the 139 contractor employees designated as any risk level other than moderate, including low risk, non-critical sensitive, and risk levels that were left blank. We selected a total of 20 contractor employees to be reviewed from the contract.

(2) ED-IES-12-D-0002- American Institutes for Research in the Behavioral Sciences

We identified a universe of 134 contractor employees. All contractor employees under this contract were designated as moderate risk. We selected a random sample of 10 contractor employees to be reviewed from the contract.

(3) ED-IES-13-C-0021- NCS Pearson, Inc.

We identified a universe of 37 contractor employees. We categorized the contractor employees by risk level designation. We randomly selected 10 of the 29 contractor employees designated as moderate risk. The remaining 8 contractor employees were designated as no risk and we reviewed all 8 employees resulting in our selecting 18 contract employees in total to be reviewed from this contract.

(4) ED-IES-13-C-0019- Westat, Inc.

We identified a universe of 5,650 contractor employees. We further identified three categories within our universe. The first group included 80 contractor employees designated as moderate risk; the second group included 391 contractor employees designated as risk level "undefined" and in the contract positions of Field Managers or Supervisors; and the third group included 5,179 contractor employees designated as risk level "undefined" and in the contract positions of Assessment Coordinators or Assessment Administrators.[9] We selected a random sample of 10 employees from each category for a total of 30 employees to be reviewed from the contract.

(5) ED-IES-13-C-0017- Educational Testing Service [10]

We identified a universe of 229 contractor employees. We further identified two categories within the universe. The first category included seven contractor employees that were either designated as low risk or were designated as no risk but had the same position title as another contractor employee on the COR listing that was designated as low risk. The second category included 72 contractor employees that were designated as no risk, with position titles that appeared to require either moderate or low risk security screenings based on position titles in the contract solicitation and final contract.[11] We selected all 7 contractor employees from the first group for review and selected a random sample of 10 contractor employees from the second group for a total of 17 contractor employees to be reviewed from the 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.

Reliability 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 the data in Security Manager with information provided by IES, to include the contractor employee listings provided by the CORs. We noted issues with the Security Manager data that limited our ability to reconcile the data, to include missing information such as contract numbers, misspellings of names, and duplicate entries. Additionally, the information provided by IES did not always include all required data and also contained similar discrepancies. Because source data for some of this information is located at the individual contactor 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 IES implemented the requirements for the contractor employee security screening process.

[9] We separated Westat contractor employees designated as risk level "undefined" into two categories because data in the list of contractor employees provided by the COR indicated that IES may have initiated security screenings for contractor employees in the positions of Field Managers and Supervisors, but had not initiated security screenings for contractor employees in the positions of Assessment Coordinators or Assessment Administrators.

[10] Although the IES COR indicated all contractor employees under this contract were no risk and therefore security screenings were not required, we found information in the contract documents and on the list of contractor employees provided by the COR that suggested there were contractor employees in positions that did require security screenings.

[11] The remaining 150 employees were designated as no risk but did not meet the criteria of either of the two subgroups.

We conducted fieldwork at Department offices in Washington, DC, during the period March 2016 through October 2016. We provided our audit results to Department officials during an exit conference conducted on November 1, 2016.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

## ADMINISTRATIVE MATTERS

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. The Department's policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 calendar days of the issuance of this report. The CAP 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.

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

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the OIG are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you have any questions, please call Michele Weaver-Dugan at (202) 245-6941.

Sincerely,

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

**Attachment 1**

## Acronyms/Abbreviations Used in this Report

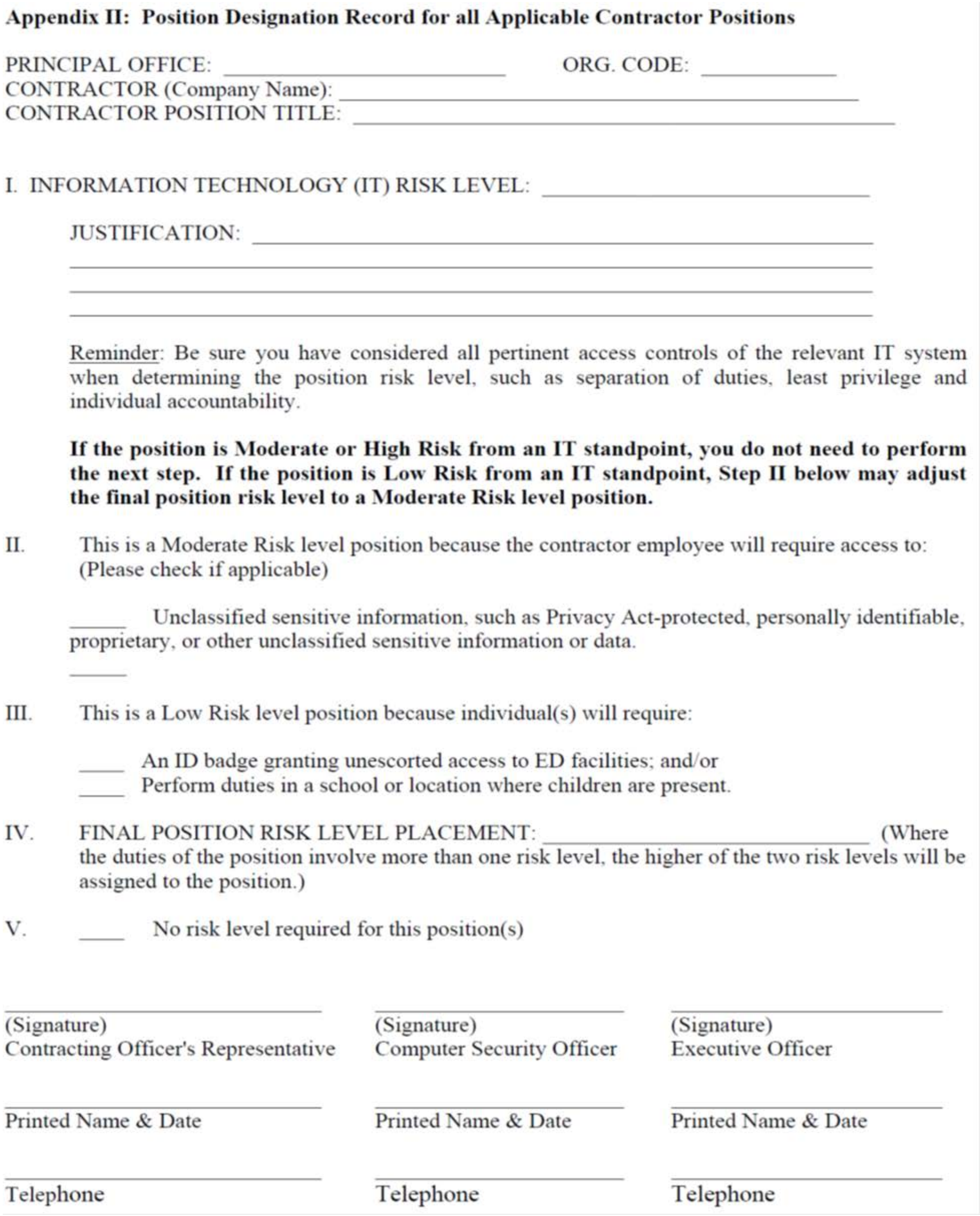
| | |
|---|---|
| CAM | Contracts and Acquisitions Management |
| CAP | Corrective Action Plan |
| CSO | Computer Security Officer |
| COR | Contracting Officer’s Representative |
| Department | U.S. Department of Education |
| Directive | Office of Management Directive: 5-101, *Contractor Employee Personnel Security Screenings* |
| E-QIP | Electronic Questionnaires for Investigations Processing System |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| IES | Institute of Education Sciences |
| IT | Information Technology |
| NACI | National Agency Check with Written Inquiries |
| NCES | National Center for Education Statistics |
| OCFO | Office of the Chief Financial Officer |
| OIG | Office of Inspector General |
| OM | Office of Management |
| OPM | Office of Personnel Management |
| PO | Principal Office |
| SOW | Statement of Work |
| SSDC | Statistical Standards and Data Confidentiality |

**Attachment 2**

## Contracts Selected for Review

| No. | Contractor | Contract Number | Contract Value (as of 12/16/2015) | Contract Award Date |
|---|---|---|---|---|
| 1 | American Institutes for Research in the Behavioral Sciences | ED-IES-12-D-0002 | $200,000,000 | 12/15/2011 |
| 2 | Westat, Inc. | ED-IES-13-C-0019 | $114,491,562 | 3/7/2013 |
| 3 | Educational Testing Service | ED-IES-13-C-0017 | $54,104,015 | 3/7/2013 |
| 4 | NCS Pearson, Inc. | ED-IES-13-C-0021 | $47,212,984 | 3/7/2013 |
| 5 | Research Triangle Institute | ED-05-CO-0033 | $46,852,191 | 9/30/2005 |
|  | **Total** |  | **$462,660,752** |  |

**Attachment 3**



**Appendix II: Position Designation Record for all Applicable Contractor Positions**

PRINCIPAL OFFICE: ______________________ ORG. CODE: __________<br>
CONTRACTOR (Company Name): ________________________________________<br>
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<br>
____ 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)

| | | |
|---|---|---|
| ______________________<br>(Signature)<br>Contracting Officer's Representative | ______________________<br>(Signature)<br>Computer Security Officer | ______________________<br>(Signature)<br>Executive Officer |
| ______________________<br>Printed Name & Date | ______________________<br>Printed Name & Date | ______________________<br>Printed Name & Date |
| ______________________<br>Telephone | ______________________<br>Telephone | ______________________<br>Telephone |

**Attachment 4**

## Summary of Investigative Types and Coverage

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

**Attachment 5**

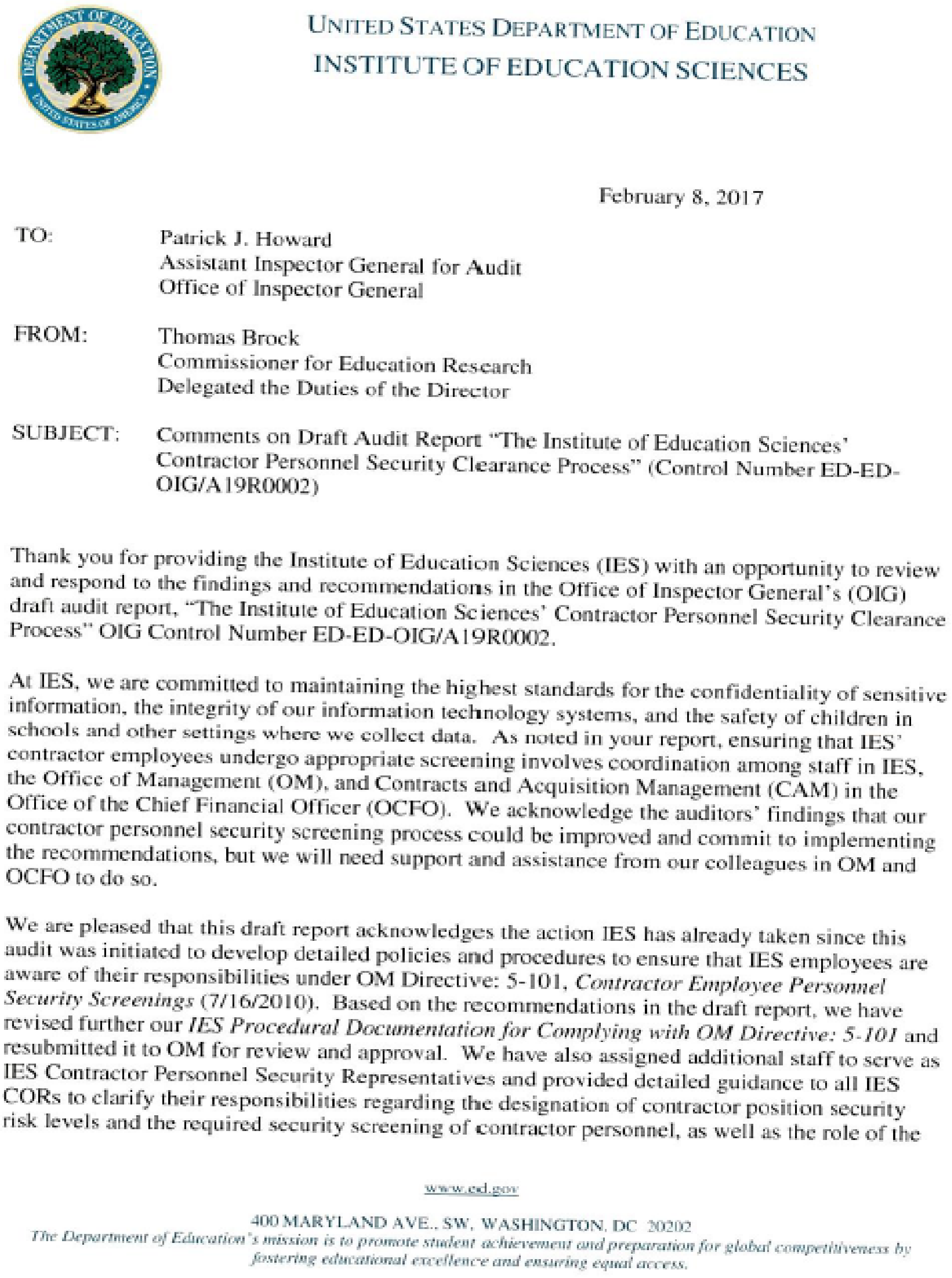
### Contractor Employee Sample Selection

| Contract Number | Contractor | Total Contractor Employees Assigned to Contract* | Category | Universe Size | Sample Size | Selection Method |
|---|---|---|---|---|---|---|
| ED-05-CO-0033 | Research Triangle Institute | 341 | Moderate Risk | 202 | 10 | Random |
| | | | Low risk, Non-Critical Sensitive, or Blank | 139 | 10 | Random |
| ED-IES-12-D-0002 | American Institutes for Research in the Behavioral Sciences | 134 | Moderate Risk | 134 | 10 | Random |
| ED-IES-13-C-0021 | NCS Pearson, Inc. | 37 | Moderate Risk | 29 | 10 | Random |
| | | | No Risk | 8 | 8 | All selected |
| ED-IES-13-C-0019 | Westat, Inc. | 5,650 | Moderate Risk | 80 | 10 | Random |
| | | | Undefined risk level; Field Manager or Supervisor positions | 391 | 10 | Random |
| | | | Undefined risk level; Assessment Administrator or Coordinator positions | 5179 | 10 | Random |
| ED-IES-13-C-0017 | Educational Testing Service | 229 | Low risk | 7 | 7 | All Selected |
| | | | Low or moderate risk | 72 | 10 | Random |
| **Total** | | **6,391** | | **6,241** | **95** | |

*The total contractor employees assigned to the contract represents the total number of contractor employees as of the date the COR provided the list of contractor employees to the audit team.

**Attachment 6**

## IES Response to the Draft Report



UNITED STATES DEPARTMENT OF EDUCATION
INSTITUTE OF EDUCATION SCIENCES

February 8, 2017

TO: Patrick J. Howard
Assistant Inspector General for Audit
Office of Inspector General

FROM: Thomas Brock
Commissioner for Education Research
Delegated the Duties of the Director

SUBJECT: Comments on Draft Audit Report "The Institute of Education Sciences' Contractor Personnel Security Clearance Process" (Control Number ED-ED-OIG/A19R0002)

Thank you for providing the Institute of Education Sciences (IES) with an opportunity to review and respond to the findings and recommendations in the Office of Inspector General's (OIG) draft audit report, "The Institute of Education Sciences' Contractor Personnel Security Clearance Process" OIG Control Number ED-ED-OIG/A19R0002.

At IES, we are committed to maintaining the highest standards for the confidentiality of sensitive information, the integrity of our information technology systems, and the safety of children in schools and other settings where we collect data. As noted in your report, ensuring that IES' contractor employees undergo appropriate screening involves coordination among staff in IES, the Office of Management (OM), and Contracts and Acquisition Management (CAM) in the Office of the Chief Financial Officer (OCFO). We acknowledge the auditors' findings that our contractor personnel security screening process could be improved and commit to implementing the recommendations, but we will need support and assistance from our colleagues in OM and OCFO to do so.

We are pleased that this draft report acknowledges the action IES has already taken since this audit was initiated to develop detailed policies and procedures to ensure that IES employees are aware of their responsibilities under OM Directive: 5-101, *Contractor Employee Personnel Security Screenings* (7/16/2010). Based on the recommendations in the draft report, we have revised further our *IES Procedural Documentation for Complying with OM Directive: 5-101* and resubmitted it to OM for review and approval. We have also assigned additional staff to serve as IES Contractor Personnel Security Representatives and provided detailed guidance to all IES CORs to clarify their responsibilities regarding the designation of contractor position security risk levels and the required security screening of contractor personnel, as well as the role of the

IES Contractor Personnel Security Representatives, Computer Security Official, and Executive Officer in the security screening process.

Our responses to the draft findings are set forth below.

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

**Response:** As noted above, we acknowledge the issues identified by the auditors and are committed to implementing the recommendations as efficiently as possible. In addition to the steps we have already taken to enhance our existing contractor employee security protocols, IES is in the process of developing a database that will enable IES CORs and Contractor Personnel Security Representatives to track personnel assigned to our contracts, their assessed risk levels, and their screening status.

Without notification from OM regarding security screening determinations, IES cannot ensure that our contractors are in compliance with these requirements. Currently, IES staff lack sufficient access to the OM Security Manager database to track security screening determinations on our own, and OM only notifies IES of unfavorable determinations. We note that your draft report indicates that "OM has an agreement with POs that if PO staff do not receive adjudication results from OM during the security screening process for a particular contractor employee, then the PO should assume that everything is acceptable with the security screening." We are concerned that the variability in the length of time required for the investigations and adjudications make it impossible for IES CORs to know when they can safely assume that a clearance has been granted. We are also concerned that the requirement that offices initiate security screening within 14 days is not always feasible, particularly when IES is seeking clearance for several hundred contractor personnel at the same time. We hope that the Department will consider revising the directive to address these concerns.

We are in the process of training all IES CORs on their responsibilities related to contractor personnel security screening and will require that all future IES CORs complete this training. If CORs identify contractor personnel who lack security screening based on their assigned risk level or have not been assessed for risk, they will work with their assigned Contractor Personnel Security Representatives as well as the Computer Security Officer, the Executive Officer, and their Contracting Officers in CAM to ensure that appropriate security screening is initiated and completed and that accurate records on contractor personnel are maintained.

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

**Response:** Similarly, we are committed to implementing the auditors' recommendations related to the second finding, but we must acknowledge that it will take time to reconcile security screening records for contractor personnel on existing contracts. For this reason, we propose corrective actions in collaboration with the Chief of Personnel Security, the Office of the General Counsel, and CAM that would enable IES to give priority to addressing the most pressing security needs and establish consequences for contractors if their employees do not meet the security screening requirements. Based on our proposed corrective actions, our intent is to have initiated all required security screenings for contractor personnel on existing contracts by the end of July. We will work closely with OM and our contractors to monitor the completion of these screenings.

Please let us know if you have any questions or need further information about any of our comments and responses. We appreciate the effort that went into the field work and the report and thank you for the opportunity to review and respond to the draft.

Sincerely,

Thomas Brock

Thomas Brock
Commissioner for Education Research
Delegated the Duties of the Director

Enclosures:
Corrective Actions