ADMINISTRATIVE
COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

Distribution:
All Department of Education employees

Approved by: /s/
Winona H. Varnon
Principal Deputy Assistant Secretary
for Management

Contractor Employee Personnel Security Screenings

Table of Contents

For technical questions regarding this Administrative Communications System (ACS) document, please contact the Chief of Personnel Security on 202-260-7727.

This ACS document supersedes OM:5-101 "Contractor Employee Personnel Security Screenings" dated 01/29/2008.

I. Purpose

The purpose of this Directive is to establish the U.S. Department of Education's (ED) policy regarding the personnel security screening requirements for all contractor and subcontractor employees (referred to as 'contractor employees') assigned to positions that require personnel security screenings. These contractor and subcontractor employees will not have access to classified national security information.

If a contractor or subcontractor employee will require access to classified national security information in order to provide a contractual service at ED, the Security Services, Office of Management, must be contacted for guidance.

II. Policy

It is the policy of ED to ensure that all contractor and subcontractor employees undergo personnel security screenings if required for performance under a contract (see Part IV, Applicability).

III. Authorization

A. Executive Order 13467, Reforming Processes Related to Suitability, Fitness for Contractor Employees, and Eligibility for Access to Classified Information, July 17, 2008.

B. Homeland Security Presidential Directive Number 12 (HSPD-12), "Policy for Common Identification Standard for Federal Employees and Contractors."

C. Privacy Act of 1974, 5 U.S.C. 552a, as amended.

D. U.S. Code Title 42, The Public Health and Welfare, Chapter 132, Subchapter V – Child Care Worker Employee Background Checks, Section 13041

E. Appendix III to OMB Circular No. A-130 – Security of Federal Automated Information Resources.

F. NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March 2006.

G. Federal Information Security Management Act (FISMA), Title III of the E-Government Act (Public Law 107-347).

IV. Applicability

A. All ED contractor and subcontractor employees must undergo personnel security screenings if, during the performance of the contract, they will:

1. Require an ID badge granting unescorted access to ED facilities;

2. Require ED 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.

V. Definitions

Chief of Personnel Security	A management official within OM Security Services responsible for making personnel security adjudication determinations on the access of contractor employees to ED facilities, unclassified sensitive information, and IT systems, or to schools or locations at which they perform duties where children are present.
Computer Security Officer	An individual formally designated by the head of a PO to be responsible for the implementation and management of the Information Technology (IT) Security Program within his or her organization.
Contractor Employee	For the purpose of this Directive, a non-Federal employee working on an ED contract, including a subcontractor employee, who (1) requires an ID badge granting unescorted access to ED facilities; (2) requires ED IT system access; (3) requires access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary or other sensitive information and data; or (4) performs duties in a school or location where children are present.
Contracting Officer	An individual with the authority to enter into, administer, or terminate contracts and execute related determinations and findings within the limits of the authority delegated. Only a contracting officer has the authority to contractually bind the government.
Contracting Officer's Representative (COR)	A program office representative responsible for monitoring the programmatic or technical requirements of a particular contract, and performing all contract management duties as assigned. The COR serves as the technical liaison between the contracting officer and the contractor, and provides technical advice to the contracting officer for necessary contract administration actions. An individual is appointed as a COR on a particular contract by written delegation of authority from the contracting officer.
e-QIP	*Electronic Questionnaires for Investigations Processing (e-QIP)* – A web-based automated system that has been developed by the Office of Personnel Management (OPM), Center for Federal Investigative Services, and approved by the Office of Management and Budget (OMB) for public use, to provide a means to facilitate the processing of the questionnaires for background investigations commonly known as Standard Forms (SF) SF 86, SF 85P, or SF 85.

Escort Access	Requires the contractor employee to be escorted and supervised at all times by an authorized ED employee or by a cleared contractor employee who has been authorized by an ED manager.
Information Technology (IT)	The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information for the use of the Federal government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. IT is used synonymously with Automated Data Processing (ADP), Federal Information Processing (FIP) resources, and Automated Information Systems (AIS).
Lawful Permanent Resident	Any person not a citizen of the United States who is residing in the United States under legally recognized and lawfully recorded permanent residence as an immigrant. Also known as "Permanent Resident Alien," "Resident Alien Permit Holder," and "Green Card Holder."
Personnel Security Adjudication Determination	A decision made about whether a person is an acceptable security risk after examining a sufficient period of his or her life following a Personnel Security Screening.
Personnel Security Screening	The process of conducting a background investigation through written, electronic, telephone, or personal contact to determine the suitability, eligibility, or qualifications of a person for Federal employment, work on Federal contracts, or for National Security purposes.
Position Risk and/or Sensitivity Level Designation	Evaluating and assigning sensitivity and/or a risk designation commensurate with the duties and responsibilities of a position related to national security and/or to the efficiency of the service.
Preliminary Personnel Security Screening	A review of completed security forms, a credit check, fingerprint check, record checks, and file reviews. A preliminary personnel security screening is conducted before a contractor employee can be assigned to a High Risk level IT position.
Senior Agency Official for Privacy (SAOP)	An individual who oversees ED activities related to the development, implementation, maintenance, and adherence to ED policies and procedures covering the privacy of and access to personally identifiable information, in compliance with Federal laws and ED information privacy practices.
System Security Officer	Refers to an individual responsible for the security of a particular IT system; with responsibility to report problems to the Computer Security Officer if there are incidents with that IT system.

Unclassified Sensitive Information	Includes such information as relates to the privacy of US citizens, payroll and financial transactions, and proprietary information.
Unfavorable Adjudication Determination	The final determination that results in adverse action relative to a person's employment acceptability or suitability, retention in a sensitive or public trust position, access to National Security Information, materials, or areas, or incumbency in a sensitive position.
Up-To-Date Investigative Forms	Forms that are received by Chief of Personnel Security within 30 days of signature by contractor employee.

VI. Procedures and Responsibilities

A. Principal Office (PO)

The PO is responsible for performing the functions described below to implement this Directive. Each PO 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, without altering the primary duties as specifically noted in this Directive or in ED's Handbook for Information Assurance Security Policy.

A PO has the option to deny contractor employees access to their controlled facilities, unclassified sensitive information, or IT systems, until the Chief of Personnel Security has made personnel security adjudication determinations. The Chief of Personnel Security must approve in advance exceptions to this policy.

A PO also has the option to modify **research and data collection contracts** and require those contractors whose employees will have direct access to minors and/or access to sensitive personal information other than publicly available directory information, e.g., social security numbers, to conduct criminal background checks on those individuals prior to those personnel being permitted access to such minors or personal information; this would be in lieu of ED conducting the criminal background checks. The contract must specify that the contractor will maintain records of all checks conducted on such personnel and certify to ED that these checks have been conducted. Contracts should also require contractors to assure that they have engaged in additional screening appropriate to the responsibilities of the individuals employed under the contract.

The Executive Officer of each PO is that Office's liaison and key point of contact with the Chief of Personnel Security, Security Services, Office of Management, for all personnel security matters.

1. Each PO must establish and maintain on file with the Chief of Personnel Security, its own procedural document for complying with this Directive. The document will identify the responsible officials; e.g., CORs, Computer Security Officers, or

System Security Officers, with the PO who will be performing key duties. All modifications to the PO Procedures Document must be forwarded to the Chief of Personnel Security for review. Each PO must include in its procedures the requirements for screening contractor employees serving 30 calendar days or more on an ED contract or project, if they will:

a. Have an ID badge granting unescorted access to ED facilities;
b. Have ED IT system access;
c. Access to unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary or other sensitive information and data; or,
d. Perform duties in a school or location where children are present.

2. The PO must coordinate with the Contracting Officer during the preparation phase of the contract solicitation and acquisition process to implement these procedures.

3. Each PO must determine the risk levels for each contractor position. This process requires coordination with the Computer Security Officers of each PO and the Chief of Personnel Security. Each PO must maintain a current position risk level designation record for each contractor position to which this Directive applies. The three position risk levels and their investigative requirements are:

HIGH RISK (HR)	Positions with the potential for exceptionally serious impact on the efficiency of ED. This includes access to ED 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 (BI) is the type of investigation required.
MODERATE RISK (MR)	Positions with the potential for moderate to serious impact on the efficiency of ED, 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 (MBI) or a Limited Background Investigation (LBI) if the NACI plus credit check investigation develops information that the Chief of Personnel Security considers potentially actionable.
LOW RISK (LR)	Includes all other positions to which this policy applies (see applicability in Section IV). A National Agency Check with Written Inquiries (NACI) is the type of investigation required.

4. Each PO must assign a position risk level to each applicable contractor employee position, before the solicitation is released, consistent with Appendix I of this document. This information will be recorded on the Position Designation Record for Contractor Positions form (see Appendix II). These records can be maintained on file with either the COR or Contracting Officer for that PO. The PO's Computer Security Officer must concur in writing with the designated risk level. If the duties of a position involve more than one risk level, the higher of the two risk levels will be assigned to the position. The PO must maintain status update on contractor duties as they change – say from Moderate Risk to High Risk, and is

responsible for commensurate paperwork and elevation of position risk level and commensurate background investigation requirement.

5. ***High Risk Level Positions***: 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. The PO must deny the contractor employee High Risk level access to IT systems, or ED sensitive or Privacy Act-protected information, until the Chief of Personnel Security notifies the COR that the preliminary security screening was completed favorably.

Additional considerations for High Risk Level Positions Regarding:

Citizenship

ED may grant a non-U.S. Citizen High Risk IT (6C) system access. 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 three (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.

Preliminary Personnel Security Screening (Required for High Risk IT (6C) Level System Access)

All Contractor employees assigned or transferred into positions determined to be at the High Risk IT (6C) level must undergo a preliminary personnel security screening before:

- They are authorized to bypass significant technical and operational security controls of general support IT systems, or major applications; or

- They are authorized to access applications where controls such as separation of duties, least privilege, and individual accountability cannot adequately protect the application or the information in it.

The preliminary personnel security screening may include a review of completed security forms, credit check, record checks, and file reviews. The PO must deny the contractor employee High Risk level access to IT systems until the Chief of Personnel Security notifies the PO that the preliminary personnel security screening was completed favorably. The inquiries for the preliminary personnel security screening will be initiated within 5 working days after receipt of the completed security forms. Within 5 working days after receiving the results of those inquiries, a determination will be made regarding a contractor employee's

acceptability. As necessary, a Background Investigation (BI) will be conducted following the completion of the preliminary personnel security screening.

While awaiting a preliminary personnel security adjudication determination for High Risk level IT (6C) positions, you may request an exception to the policy from the Chief, Personnel Security, for contractor employees who require immediate physical access to ED controlled sensitive areas or facilities, or to High Risk sensitive information or IT systems, must be escorted and supervised by an authorized ED employee or authorized cleared contractor employee at all times. Escort access may not be used for contractor employees after notification of an unfavorable personnel security adjudication determination about the contractor employee from the Chief of Personnel Security.

An ED manager must authorize the escort access. Contractor employees who will have physical access to ED controlled facilities, sensitive information or IT systems (excluding any actual log-on access to ED IT systems), for less than 30 days (e.g. a one or two week project), or have infrequent access (e.g. three times a month), do not require investigation provided they are escorted. Escort access requires the contractor employee to be escorted and supervised by an authorized ED employee or authorized cleared contractor employee at all times.

Reinvestigations for High Risk (IT) (6C) Level Positions

Contractor employees occupying High Risk level IT positions must undergo reinvestigation every 5 years for the duration of their contract at ED, or if there is a break-in-service to an ED contract of 365 days or more. Each PO must ensure a complete investigative forms package is submitted within 14 days of the Chief of Personnel Security's direct request.

6. *All Other Positions*: As necessary, each PO must have the COR submit completed contractor employee investigative forms for each individual required to submit forms, and a "Request for Personnel Security Officer Action" form for each individual, 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. **No contractor employees are permitted unescorted/unsupervised access to ED facilities, unclassified sensitive information or IT systems, until they have submitted applicable investigative forms.**

7. Each PO COR must ensure that the Contracting Officer, and if necessary the Computer Security Officer, is kept informed during the contractor employee screening process, including notification of the screening determination.

8. Each PO COR must notify the contractor of the personnel security adjudication determination and maintain a copy for its records. If any attributes of the position change, including the need for a higher risk level, the PO will send a new "Request for Personnel Security Officer Action" form, showing the new position risk level, to the Chief of Personnel Security. *The* Chief of Personnel Security

*will promptly notify the PO if the contractor employee has not met the investigative requirements for the **higher** position risk level.*

9. Each PO must maintain an up-to-date list of all contract positions and risk level designations covered by these policies and procedures. 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. *The PO COR must also 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 Computer Security Officer.*

10. Performance-Based Contract: The risk level associated with the contract requirement shall be designated within the Performance Work Statement (PWS) or Statement of Work (SOW), prior to the Request for Proposal (RFP) being released. All position risk levels must be assigned prior to contract award.

11. Each PO COR must notify the Chief of Personnel Security within three 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.

12. Each PO will have the COR inform the Contracting Officer that a contractor employee is deemed not acceptable for reasonable cause, upon notification by the Chief of Personnel Security, and such finding(s) makes the individual ineligible for access to ED facilities or IT systems. *The Contracting Officer will make the official notification to the contractor.* A final determination cannot be appealed.

13. Each PO must immediately deny a contractor employee access to all ED IT systems, facilities and information, when notified by the Chief of Personnel Security that a contractor employee is deemed not acceptable for reasonable cause.

14. The PO must contact the Chief of Personnel Security if the PO chooses to require screening for contractor employees who will require access for less than 30 days, rather than have to provide escort access.

15. POs are permitted to develop more stringent contractor personnel security screening policies if they determine that their organization or offices require it. However, the PO must clear any such policy with the Chief of Personnel Security prior to implementation.

B. Senior Procurement Executive

1. The Senior Procurement Executive (SPE) in the Office of the Chief Financial Officer must ensure that personnel security screening requirements for contractor employees (as defined by this Directive) are included in all solicitations and

contracts issued by ED. The SPE must ensure that potential offerors and contractors are aware of all personnel security requirements for contractor employees at the earliest stages of the acquisition. Except for performance-based contracts, the SPE, in coordination with the Contracting Officer, the PO, and others, as needed, must ensure that each contractor employee position is assigned an appropriate risk level during the acquisition process and that this information is included in the solicitation.

2. Performance-Based Contracts: The SPE, in coordination with the Contracting Officer, the PO and others, as needed, must ensure that contractor employee positions are assigned risk designation levels at the earliest possible time during the acquisition and that this information is communicated to the contractor for performance-based contracts.

3. All active solicitations and contracts meeting the requirements of this Directive will include personnel security screening requirements for ED contractor employees.

4. The SPE, in coordination with the Contracting Officer, must ensure that all contractor employees are screened in a timely manner and that procedures of this Directive are fully implemented throughout the performance of the contract. The SPE will ensure that annual reviews of contracts are conducted to ensure continued compliance with this Directive, and that the SPE and the Contracting Officer act upon instances of non-compliance. The Contracting Officer may take official action against a contractor for non-compliance, including, but not limited to, withholding of payment, or termination of the contract.

5. The SPE will ensure that the Contracting Officer requires each contractor to timely submit completed forms to the PO. Contracts that do not currently have this requirement must be modified to require the timely and complete submission of forms to the COR within two business days of a contractor employee's assignment to an ED contract.

6. The SPE, through the Contracting Officer, must officially notify a contractor if a contractor employee is deemed not acceptable for reasonable cause and such finding(s) makes the contractor employee ineligible to render service(s) or otherwise perform under the contract. A final determination cannot be appealed.

C. ED Requirements for Contractor/Contractor Employees

As contained in each solicitation or contract meeting the requirements of this Directive, contractors and/or their employees at ED have the following responsibilities:

1. 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 documents required by the Department of Homeland Security, Bureau of Immigration and Appeals, to work in the United States. Non-US

citizen contractors living and working outside the U.S., and not legally authorized to work in the U.S., will not be granted access to ED IT systems or unclassified sensitive information, such as Privacy Act-protected, personally identifiable, proprietary, or other sensitive information and data.

2. 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. Contractor employees requiring access to ED facilities or IT systems as part of a contract managed by another Federal Agency such as the General Services Administration (GSA), Federal Protective Service (FPS), or the Department of Homeland Security (DHS), will be required to show proof of personnel security screening for validation to allow for such access. All contractors must comply with the Principal Office (PO) Executive Office or Computer Security Officer's pre-processing requirements for personnel security screening and granting access privileges.

3. Each contractor must ensure that its contractor employees submit all required personnel security forms to the COR within two 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.

4. Each contractor must ensure that a contractor employee is not placed in a higher risk position than that for which he or she was previously approved, unless approved by the Contracting Officer, the COR, the Chief of Personnel Security and the Computer Security Officer.

5. Each contractor must report to the COR all instances of individuals seeking to obtain unauthorized access to any ED IT system, or unclassified sensitive and/or Privacy Act-protected information.

6. Each contractor must report to the COR any information that would raise a concern about whether a contractor employee's continued employment would promote the efficiency of the service or violate the public trust.

7. Each contractor must report to the COR within two business days any removal of a contractor employee from a contract; within one business day if removed for cause. The contractor is responsible for returning an ED ID badge to the COR within 7 business days of the contractor employee's departure. Also, the contractor must report to the COR, within two business days, any instance of a contract employee being moved into, or out of, an ED facility.

8. Each contractor will officially notify its contractor employee if he or she will no longer work on an ED contract.

9. Each contractor is responsible for the protection of sensitive or Privacy Act-protected information from unauthorized use or misuse by its employees,

subcontractors, or temporary workers, and for preventing access to others, who are not authorized and have no need to know such information.

10. Contractors may be required to conduct criminal background checks (for a period of not less than 10 years) of their personnel who will have direct access to minors and/or access to sensitive personal information other than publicly available directory information, e.g., social security numbers, before their personnel are permitted access to such minors or personal information if they will be employed on a **research and data collection contract**. These contractor employees will not require routine physical access to federally controlled facilities or logical access. In such instances, contractors must keep records of all checks conducted, and provide certification to ED that they have conducted the checks. Contractors must also assure that they have engaged in any additional screening appropriate to the responsibilities of the individuals employed under the contract.

D. Chief of Personnel Security

1. The Chief of Personnel Security, an employee of the Office of Management, provides oversight and guidance for all matters relative to these policies and procedures.

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

3. The Chief of Personnel Security shall promptly return incomplete forms to a PO for proper completion by the contractor employee.

4. The Chief of Personnel Security must notify the PO COR promptly of the results of a contractor employee's preliminary personnel security screening for High Risk IT (6C) Level positions. The preliminary personnel security screening may include a review of completed security forms, credit check, record checks, and file reviews. The inquiries for the preliminary personnel security screening must be initiated within 5 working days after receipt of the completed security forms. Within 5 working days after receiving the results of those inquiries, a determination must be made regarding a contractor employee's preliminary acceptability. As necessary, a Background Investigation (BI) must be conducted following completion of the preliminary personnel security screening.

5. The Chief of Personnel Security will request the expansion of background investigations to obtain additional information to the extent necessary to make personnel acceptability or suitability determinations**.** These determinations will be made using criteria established by the OPM for the purpose of determining suitability for employment in the Federal competitive service, as described in 5 CFR 731.202, and other OPM guidance. The Chief of Personnel Security determines whether a contractor employee is acceptable for the position from a personnel security standpoint.

6. The Chief of Personnel Security will usually provide the contractor employee with an opportunity to refute, explain, clarify, or mitigate information in question.

7. The Chief of Personnel Security will inform the PO COR when he or she determines that a contractor employee is not acceptable to render service(s) or, if appropriate, to otherwise perform under a contract. If, after final determination by the Chief of Personnel Security, a decision is made that the contractor employee is not acceptable to render services on a contract and access is denied, the COR will inform the Contracting Officer. The Contracting Officer must inform the contractor (i.e. employing firm) that the contractor employee is not acceptable to render services in this particular position, or, if appropriate, to otherwise perform under the contract. The contractor will notify the contractor employee. A final determination cannot be appealed.

8. The Chief of Personnel Security will forward verification of a personnel security adjudication determination or other notification of the personnel security screening determination for contractor employees to the PO COR for distribution to the Contracting Officer, Computer Security Officer, and/or the System Security Officer.

9. The Chief of Personnel Security will coordinate with the Principal Office COR when contractor employees require periodic screenings at five-year intervals.

E. Chief Information Officer (CIO)

The ED CIO will coordinate and provide additional support, oversight, and guidance to the Chief of Personnel Security on IT-related personnel security issues and activities within ED.

F. Senior Agency Official for Privacy (SAOP)

The ED SAOP oversees ED activities related to the development, implementation, maintenance of, and adherence to ED's policies and procedures covering the privacy of, and access to, personally identifiable information in compliance with Federal laws and ED's information privacy practices. The SAOP has the following responsibilities:

1. Ensure privacy is considered within ED's IT security programs;

2. Provide development guidance and assist in the identification, implementation, and maintenance of ED's privacy policies and procedures in coordination with the Chief Information Security Officer and the Office of the General Counsel, as applicable; and

3. Ensure delivery of privacy training to all employees and contractors.

Appendix I: Position Risk Designation for Contractor Positions

Risk Level & Code	Criteria for Determining Risk Level
High Risk (6/6C)	Position involves one or more of the following attributes: 1. Responsibility for the development, direction, implementation, and administration of ED computer security programs, including direction and control of risk analysis or threat assessment. 2. Significant involvement in mission-critical IT systems. 3. Responsibility for preparing or approving data for input into an IT system which does not necessarily involve personal access to the IT system, but which creates a high risk for effecting grave damage or realizing significant personal gain. 4. Assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from IT systems of amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to insure the integrity of the IT system. 5. Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of the IT systems hardware and software. 6. Access to an IT system during the operation or maintenance in a way that bypasses incorporated controls, to permit high risk for causing grave damage or realizing a significant personal gain. 7. Any other positions that involve high risk for effecting grave damage or significant personal gain.
Moderate Risk (5/5C)	A position whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the information or IT system. Position involves one or more of the following attributes: 1. Access to or processing of proprietary data or information protected under the Privacy Act of 1974. 2. Accounting, disbursement, or authorization for disbursement from IT systems with amounts less than $10 million per year. 3. Other positions that involve a degree of access to an IT system that creates a significant potential for damage or personal gain less than that in High Risk positions.
Low Risk (1/1C)	Includes all other positions to which this Directive applies (see Part IV, Applicability). This does apply to Part IV.A.4, as well as any other “applicable” position not falling into High Risk (6/6C) or Moderate Risk (5/5C) Levels above.

Position Risk Level and Required Investigation and Forms

Risk Level & Code	Investigation Requirement	Forms Required (See *Note 1*: Description of Forms)
High Risk (6 or 6C)	BI (Background Investigation) and PRIR (Periodic Reinvestigation) After 5 years, and each succeeding 5 years	e-QIP SF 85P (See *Note 2, 3*) e-QIP SF 85P-S (See *Note 2, 3*) FD-258 Fair Credit Reporting Act Release
Moderate Risk (5 or 5C)	NACIC (National Agency Checks with Written Inquiries and Credit) Note: If a contractor NACIC investigation develops potentially actionable information the background screening will be expanded to a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI), at the discretion of the Chief of Personnel Security.	e-QIP SF 85P (See *Note 2, 3*) FD-258 Fair Credit Reporting Act Release
Low Risk (1 or 1C)	NACI (National Agency Check with Inquiries)	e-QIP SF 85 (See *Note 2*) Limited OF 306 items (See *Note 4*) FD-258

Note 1: Description of the Investigative Forms Required:
1. SF 85, Questionnaire for Non-Sensitive Positions
2. SF 85P, Questionnaire for Public Trust Positions (Revised 9/95)
3. SF 85P-S, Supplemental Questionnaire for Select Positions
4. OF 306, Declaration for Federal Employment (http://www.opm.gov/forms/html/of.asp)
5. FD-258, Fingerprint Chart (ED requires all Headquarter contractor employees receiving ID badges to have their fingerprints taken electronically)
6. Fair Credit Reporting Act Release (ConnectEd, Forms, Personnel Security)

Note 2: ED requires the completion of the SF 85, SF 85P, and SF 85P-S in e-QIP, OPM's Electronic Questionnaire Investigations Processing System (see Definitions). Only the signature pages of each form will be submitted to Office of Management, Security Services, through the COR and the PO Executive Officer or Computer Security Officer, along with other applicable forms.

Note 3: DO NOT SUBMIT the "Authorization for Release of Medical Information" form, which is part of the SF 85P form, unless you were required to complete the SF 85P-S form and you answered "YES" to Item 5 on the SF 85P-S form.

Note 4: The contractor employee will complete items 1, 2, 8 through 13, 16 and 17a. If the official form is not available, the specific questions may be duplicated on a separate attachment and completed by the contractor employee.

Summary of Investigative Types and Coverage

		Investigation Item	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 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