

# Contractor Employee Personnel Security Screening Procedures for FSA

## *Introduction*

FSA information security depends heavily on individuals, and the controls placed on the individual. Each user must adhere to standards of conduct that protect the confidentiality, integrity and availability of information networks and the data they contain, transmit or process.

## *Background*

FSA follows the [Departmental Directive for Contractor Employee Personnel Security Screenings Policy Supplement, a supplement to OM:5-101](#). This document addresses how FSA has implemented the personnel security requirements as described by the Department.

## *Roles and Responsibilities*

Within FSA, various officials have responsibilities associated with contractor security. This section describes those responsibilities.

### **Computer Security Officer**

The Computer Security Officer for FSA is responsible for the creation of policy and procedures based upon existing guidance and requirements. The CSO will coordinate with associated stakeholders and provide additional support, oversight, and guidance to the SSOs on IT-related personnel security issues and activities within the Department.

### **FSA Personnel Security Officer**

When the FSA Personnel Security Officer needs to interface with the SSO and there is no SSO assigned, the FSA Personnel Security Officer will interface with the COR. The FSA Personnel Security Officer will do the following:

- Receive, process, and forward contractor employees' security forms to Office of Management Personnel Security (OM Security).
- Promptly return incomplete forms to the appropriate SSO for proper completion.
- Forward verification of clearance or other notification of the screening determination for contractor employees to the SSO.
- Notify the SSO six months in advance of when contractor employees need to renew their screenings at the five-year renewal interval.
- Process security clearances within 14 days of receipt.
- Provide guidance and support to SSO's regarding personnel security issues.

- Receive access requests and validate when contractor staff have submitted or already have the clearance levels validated for the access requested by the SSO.
- Maintain an updated list of contract positions and risk level designations covered by these policies and procedures. The list will 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 was submitted, and the date of the final screening determination.

### **Office of Management Personnel Security**

- 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 Office of Personnel Management for the purpose of determining suitability for employment in the Federal competitive service, as described in 5 CFR 731.202, and other Office of Personnel Management (OPM) guidance.
- Provide the contractor employee an opportunity to refute, explain, clarify or mitigate information in question. If, after final determination by the Department Personnel Security Officer, a decision is made that the contractor employee is not acceptable to render services on a contract and access is denied, the Office will inform the SSO (or the COR, if there is no SSO).

### **CORs**

Under the Departmental Directive, the CORs are responsible for being the liaison between the contractors and the Department for processing security paperwork. For non-system related contracts that do not have an FSA SSO, the COR will assume the SSO duties. However, all systems will have an SSO assigned.

The COR will:

- Provide sufficient background clearance forms to the Contractor Security Office to distribute to the employees on the contract. These forms can be provided as either hard or soft copies.
- Ensure the Contractor understands the requirements for contractor security clearances.
- Notify the SSO of new contractor hires, terminations, and position changes.
- Maintain a list of contractor personnel that includes: start date, clearance level, clearance status, termination date
- Upon notification of clearance results, notify the Contractor Security Contact.
- Follow-up to ensure contractor staff are not used in positions where their background screening have found them unacceptable to render services.

## **SSOs**

The system security officers will be the primary liaison between the contractor's security point of contact and FSA Personnel Security.

The SSOs will:

- Receive completed background clearance paperwork from the Contractor Point of Contact and
- Approve clearance paperwork after conducting quality assurance checks to ensure it is complete and that the proper clearance level has been identified.
- Return incomplete paperwork with SSO comments back to the Contractor Security Contact within three days.
- Provide approved paperwork to the FSA Personnel Security Officer within three days of receiving the final completed paperwork. .
- Maintain clearance information and report background clearance results to the COR.
- Notify the FSA Personnel Security Officer when background clearance results have not been reported after six months.

## **Contractor Security Contact and Program Manager**

The contractor's security contact is the liaison between the individual contractors and FSA for security clearances.

- They are responsible for transmitting the appropriate paperwork to the contractors, having them complete the paperwork and returning it to the SSOs within twenty-four hours of an assignment to a Department contract and ensure that the forms are complete.
- They are responsible for identifying by name all contract personnel and the contract labor categories. Updated lists should be provided periodically throughout the life of the contract.
- They shall ensure that the required paperwork is properly completed, reviewed for accuracy, and submitted to the SSO prior to any contract employee starting to work on the contract. The Contractor Security Contact must notify the COR if an individual's duties change within the scope of the contract.
- If an individual's new duties require a higher background clearance level, the Contractor Security Office must submit the proper clearance paperwork for that individual to the SSO.
- They are responsible for ensuring that all non-U.S. citizen contractor employees are Lawful Permanent Residents of the United States or have the appropriate work authorization documents as required by the Immigration and Naturalization Service to work in the United States.

The Contractor Security Office must notify the SSO (or COR, if there is no SSO) if an individual's departs the contract. If employees are removed from contract positions for any reason the Contractor Security Office shall:

- Notify the SSO (or COR, if there is no SSO) of the removal, the termination date, and the reason within three working days. If termination is for cause, immediately revoke system access and follow up by notifying the SSO (or COR, if there is no SSO). The system will deny access to all Department IT systems, facilities and information to a contractor employee when notified of an unfavorable personnel security adjudication determination.
- Retrieve all keys, card keys and badges allowing access to the system facilities.
- Review with the departing employee their obligation to protect system and Departmental Privacy Act data and information.
- Complete the [Departing Employee Checklist](#).

### ***Contract Language***

CORs, SSOs, and FSA managers will work with the Department's Contracting Office to ensure that the appropriate security language is included in contracts. The language should address:

- Access to Department of Education controlled facilities;
- Access to the Department's IT systems and the systems' data;
- Access to sensitive but unclassified or Privacy Act-protected information;
- Security risk levels; and
- Background clearances.

### ***Clearance Requirements:***

These requirements apply to any contractor or subcontractor staff that will have access to Department of Education facilities, systems or ED data. Requirements for personnel checks imposed by these policies vary commensurate with the sensitivity of the data handled by the employee, and the risk and magnitude of loss or harm associated with the type of position and access the employee requires to complete his/her assigned duties.

Contractors with 6C clearance applications will not be granted system access until the Office of Management Personnel Security has approved their paperwork. Contractors with 5C and 1C clearance applications will not be granted system access until their paperwork has been submitted and accepted by the FSA Personnel Security Officer.

Personnel assigned to duties under a contract will be subject to investigation by the Department of Education. The Department's investigation may include, but will not be limited to, the following:

- Investigation of criminal record
- Checking references on previous employment

- Checking previous security clearances

***Background Investigation Procedures:***

Contractor and subcontractor personnel must complete and submit the required government forms based on level of clearance and job that is performed. Definitions of the security levels are as follows:

High Risk (Level 6C) - High risk positions are those positions that have potential for exceptionally serious impact because they involve duties that are especially critical to the Department (for example, project manager and security administrator.)

Moderate Risk (Level 5C) - Moderate risk positions are those positions that have the potential for moderate to serious impact (for example, persons who are responsible for the direction, planning, design, operation, or maintenance of computer systems.)

Low Risk (Level 1C) - Low risk positions are those positions that require access to the computer systems (for example, application programmers.)

Non-Disclosure Statement Positions (NS)- Depending on job responsibility, and any related limited systems access, a signed copy of the Privacy Act Statement and Declaration for Federal Employment (OF-306) may be the only forms required. Individuals in this category perform duties that are closely monitored and supervised to ensure risk is limited (for example, data entry and documentation specialist.)

The required clearance forms are as follows:

<u>FORM</u>	<u>TITLE</u>	<u>COPIES</u>	<u>HIGH (6C)</u>	<u>Moderate (5C)</u>	<u>LOW (1C)</u>	<u>NS</u>
<a href="#"><u>SF-85P</u></a>	Questionnaire for Public Trust Positions	<u>2*</u>	<u>X</u>	<u>X</u>		
<a href="#"><u>SF-85PS</u></a>	Supplemental Questionnaire for Select Positions	<u>2*</u>	<u>X</u>			
<a href="#"><u>SF-85</u></a>	Questionnaire for Non-Sensitive Positions	<u>2*</u>			<u>X</u>	
<a href="#"><u>OF-306</u></a>	Declaration for Federal Employment	<u>2*</u>	<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>
<a href="#"><u>FD-258</u></a>	Fingerprint Card	<u>1</u>	<u>X</u>	<u>X</u>	<u>X</u>	
	Fair Credit Reporting Act Release	<u>2*</u>	<u>X</u>	<u>X</u>		
<u>NS</u>	Non-Disclosure Statement/Privacy Act	<u>1</u>	<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>

	<a href="#">High Risk 6C Checklist</a>	<u>2</u>	<u>X</u>			
	<a href="#">Moderate Risk 5C Checklist</a>	<u>2</u>		<u>X</u>		
	<a href="#">Low Risk 1C Checklist</a>	<u>2</u>			<u>X</u>	

\* Original and one copy

The following steps are required for submitting employee clearance documents:

A. If the individual will be assigned for more than thirty days to the Department contract, the Contractor Security Office must submit completed contractor employee investigative forms for each individual required to submit forms to the System Security Officer (or COR if there is no SSO) within 14 days of the date the contractor employee is placed in a position. The Principal Office will contact the Department Personnel Security Officer if it chooses to require screening for contractor employees who will require access for 30 days or less.

B. The contractor employee without previous clearance shall complete the required forms, as shown in the above table based upon the defined labor categories. (Note: EVERY employee assigned to the contract in any way must complete the Non- disclosure/Privacy Act Statement and the OF 306).

1) The applicant’s labor categories shall be detailed enough to allow the Contractor Security Office to make a decision that no authorization, need or ability to bypass security controls is involved. The ability and capability to bypass these controls is a major factor in making any security clearance level determination.

2) The Contractor Security Office will require the applicant to fill out a Non-disclosure/Privacy Act Statement and an OF 306 “Declaration for Federal Employment” form.

C. The contractor employee, with current (non-departmental) or previous clearances (including departmental), who is required to obtain a clearance for employment on this contract must complete a letter on contractor letterhead that provides:

- Employee’s full name
- Date and place of birth
- Social Security Number
- Type and Level of security clearance
- Employer Name (at time of investigation)
- Date of investigation
- Contract Number
- Agency completing the investigation

D. The contractor employee with a current or previous clearance who requires an

upgrade due to a change in labor category or system access will be required to provide the paperwork that is required for the new level.

- E. If a contractor employee is deemed not acceptable for reasonable cause then such finding(s) makes the individual ineligible for access to Department facilities or systems. The FSA Contracting Officer will make the official notification to the Contractor Security Office. A final determination cannot be appealed.
- F. Each contract must have a requirement for the timely submission of completed forms by the contractor to the Principal Office. If the individual will be assigned for more than 30 days to the Department contract, forms must be submitted to the SSO within 14 days of the date the contractor employee is placed in a position. Existing contracts must be modified to require the timely and complete submissions of forms to the COR within twenty-four hours of an assignment to a Department contract. If incomplete, forms must be resubmitted to the Department Personnel Security Office through the SSO within 10 workdays or the contractor employee must be removed from the contract.
- G. Contractor employees occupying High Risk level IT positions must undergo a periodic reinvestigation every five years, or sooner if necessary.

DRAFT

# Diagram of Personnel Contractor Security Flow

