



**ADMINISTRATIVE COMMUNICATIONS
SYSTEM
UNITED STATES DEPARTMENT OF
EDUCATION**

Handbook

Handbook OIG-1

Page 1 of 28 (11/03/1992)

Distribution:
All ACS Manual Holders

Approved by: _____/s/_____
Inspector General

Personnel Security – Suitability Program

Prepared By:

Security Program Staff,

Policy, Planning, and Management Services,

Office of Inspector General

Former directive number Handbook 11

Supersedes ACS Directive A:OIG:1-100, Personnel Security, dated 01/05/1982.

Table of Contents

Chapter 1 General..... 4
I. Purpose 4
II. Policy..... 4
III. Authority 4
IV. Relationship Between Suitability Risk Levels and
National Security Sensitivity Levels..... 4
V. Definitions..... 5
VI. Responsibilities..... 7
VII.Orientation and Information for Employees 8

Chapter 2 Suitability (Public Trust Positions) 9
I. Purpose 9
II. Policy..... 9
III. Authority 9
IV. Suitability Position Risk Criteria and Levels..... 10
General Requirements..... 10
Risk Designation System 10
Criteria and Levels - Public Trust Positions 10
V. Suitability Determinations 12
Due Process..... 13
VI. Risk Designation and Investigative Requirements 13
Risk Designation..... 13
Investigative Requirements..... 14
Suitability Reinvestigation..... 14
VII. Challenge to Risk Designation 14
VIII.Computer/ADP Risk Criteria and Levels..... 15
Security of Federal Automated Information Systems..... 15
Risk Levels and Criteria..... 15

Chapter 3 National Security Positions 18
I. Purpose 18
II Definition 18
III. Applicability 18
IV. Authority 18
V. Sensitivity Level Designation 18
General Requirements..... 18
Risk Designation System 18
National Security Sensitivity Criteria and Levels..... 19
Sensitivity Levels..... 19
National Security Risk Criteria..... 19
VI. Security Office Record on Sensitivity Designation, Access Level, and
Investigative Requirement 20
VII. Waiver Requirements 21
General..... 21

Table of Contents *(continued)*

Specific Waiver Requirements 21

VIII Exceptions to Investigative Requirements 21

IX. Periodic Reinvestigation Requirements..... 22

X. Due Process..... 22

Chapter 4 Personnel Investigations..... 22

 I. Purpose 22

 II Public Availability of Investigative Files..... 23

 III. Personnel Investigations Forms 23

Appendix A 25

 Risk Designation System 25

Appendix B 27

Appendix C 28

Chapter 1 General

I. Purpose

This temporary handbook is issued to implement 5 CFR Parts 731, 732, 736 and 754, "Suitability, Personnel Security and Related Programs, Investigations and Suitability Disqualification Actions; Interim Rule" effective May 23, 1991. This handbook will be in effect for a maximum of one year, or until such time as either the final rules are published, if there are significant changes, or the revised Federal Personnel Manual chapters are published. At that time we will prepare a departmental handbook implementing the requirements of the FPM for competitive service positions, the Department of Education's (ED) policy for excepted service positions, and for others performing services in ED.

II. Policy

This temporary handbook:

- Outlines ED's personnel security-suitability policies and procedures;
- Separates national security positions from public trust positions;
- Sets forth guidelines on personnel suitability investigations and designating risk levels for public trust positions;-
- Sets forth guidelines on personnel security investigations and designating sensitivity levels for national security positions; and,
- Provides due process procedures.

III. Authority

5 CFR Parts 731, 732, 736, and 754.

IV. Relationship Between Suitability Risk Levels and National Security Sensitivity Levels

- Chapter 3 of this handbook describes national security position sensitivity, which includes suitability considerations. With some exceptions, the national security positions, exclusive of suitability, relate to requirements for access to classified information and sensitive restricted facilities.
- Suitability is a consideration for every position. Fewer positions are subject to the national security consideration in sensitivity designations under Chapter 3. Those

positions deemed sensitive on the basis of national security requirements are subject primarily to the requirements of Chapter 3.

V. Definitions

- **Background Investigation (BI)** is used for High Risk Public Trust positions and consists of a National Agency Check, credit search, personal interviews of subject and sources, written inquiries of selected sources, and record searches covering specific areas of the subject's background for 5 years coverage. The SF-85P, Questionnaire for Public Trust Positions, is needed.
- **High Risk (HR) Public Trust Positions** have the potential for exceptionally serious impact on the efficiency of the service.
- **Limited Background Investigation (LBI)** is used for Moderate Risk Public Trust positions and noncritical-sensitive national security positions. The LBI consists of a National Agency Check, credit search, personal interviews of subject and sources, and written inquiries of selected sources covering specific areas of the subject's background for 3 years coverage. The SF-85P or SF-86, Questionnaire for Sensitive Positions (for national security), is needed.
- **Low Risk (LR) Public Trust Positions** have the potential for impact involving duties of limited relation to the agency mission, with program responsibilities which affect the efficiency of the service.
- **Minimum Background Investigation (MBI)** consists of a National Agency Check, credit search, written inquiries, and record searches covering specific areas of a subject's background in the past 5 years. Telephone inquiries are made on selected employments, and whenever initial inquiries are not returned and information is needed to resolve an issue(s). The SF-85P or SF-86 is needed.
- **Moderate (MR) Risk Public Trust Positions** have the potential for moderate to serious impact on the efficiency of the service.
- **National Agency Check (NAC)** is part of all background investigations and consists of searches of the OPM Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); FBI Identification Division fingerprint name file and fingerprint chart; and FBI Records Management Division files. The SF-85P or SF-86 is needed. A NAC is not conducted from the SF-85.
- **National Agency Check and Inquiries (NACI)** consists of a NAC, written inquiries, and record searches covering specific areas of a subject's background during the past 5 years. The SF-85 is needed.

- **National Security Position**, for purposes of this handbook, refers to positions that require regular use of, or access to, classified information or facilities.
- **Periodic Reinvestigation (PRJ)** consists of a NAC, credit search personal interview of the subject, and selected record searches used for required update under FPM Chapter 732 with an SF-86, and under FPM Chapter 731 with an SF-85P.
- **Public Trust Positions** have the potential for action or inaction by their incumbents to affect the integrity, efficiency, and effectiveness of assigned Government activities. The potential for adverse effect includes action or inaction which could diminish public confidence in the integrity, efficiency, or effectiveness of Government activities, whether or not actual damage occurs.
- **Reimbursable Suitability/Security Investigation (RSI)** consists of a concentrated investigation to provide additional information to resolve a suitability issue(s) from an SF-85 or SF-85P investigation or to resolve any suitability or security issue(s) from an SF-86 investigation, or from an issue(s) developed on an employee or contractor employee.
- **Risk Designation System** is the basic system explained in Chapter 2 that determines department, program, and position placement based on general risk level criteria.
- **Single Scope Background Investigation (SBJ)** is used for national security positions requiring access to Sensitive Compartmented and Top Secret national security information. This investigation consists of a NAC on subject and spouse/cohabitant, subject interview, certification of date and place of birth, verification of citizenship of subject and foreign-born immediate family members, personal interviews of sources, written inquiries, and record searches for 10 years coverage. The SF-86 is needed. The OF1 Form 36, Additional Data for Single Scope Background Investigations and Other Background Investigations, is needed if immediate family members, spouse/cohabitant are foreign born.
- **Suitability** refers to a determination based on an individual's character or conduct that may impact the efficiency of the service.
- **Suitability Position Risk Criteria** are used to determine the Public Trust Risk Level of a position for suitability.
- **Update Investigation** consists of the same type of case as the previous investigation (MBI, LB1, B1, and SBI) from 13 to 60 months of the previous investigation's closing date. The SF-85P or SF-86 is needed.
- **Upgrade Investigation** consists of a NAC, credit search, personal interview of the subject and selected sources, and record searches covering specific areas of

the subject's background since the last background investigation. This investigation is for movement upward in sensitivity from 13 to 60 months of the previous investigation's closing date. The SF-85P or SF-86 is needed.

VI. Responsibilities

- A. The **Secretary** (or designee) establishes and maintains an effective personnel suitability and security program for the Federal competitive and excepted service within ED, to ensure that the employment of each person will promote the efficiency of the service. The elements of this program include:
- Designating every position within ED at either a high, moderate, or low risk level, as determined by the position's potential for adverse impact to the efficiency of the service;
 - Complying with preinvestigative review and referral requirements of FPM Chapter 731;
 - Requesting required investigations corresponding to position risk levels;
 - Assisting with the implementation of suitability adjudications made by OPM;
 - Adjudicating the suitability of applicants for and appointees to HR, MR, and LR level positions;
 - Adjudicating the suitability of competitive service applicants filing outside a civil service register, and of applicants, eligibles, and employees in the excepted service;
 - Complying with the suitability program administration and reporting requirements of FPM Chapters 731 and 732;
 - Ensuring that appropriate training is provided for designating position sensitivity and adjudicating suitability;
 - Designating positions in terms of their impact on the national security to assure appropriate screening under Executive Order 10450, Security Requirements for Government Employment, April 27, 1953;
 - Requesting required entry investigations and operating a periodic reinvestigation program;
 - Making a security determination that demonstrates a reasonable expectation that the employment of each person either conforms or does

not conform to the standards set forth in Executive Order 10450 or other related national security interest authorities;

- As necessary in the interest of the efficiency of the service, taking adverse suitability action under 5 CFR 315*or 752, affording the appointee or employee such rights as may be specified therein;
 - As necessary in the interests of national security, acting under 5 U.S.C. 7532, Executive Order 10450 and other available authorities, suspending without pay, or reassigning or detailing temporarily to a nonsensitive position or position with sensitive duties withheld, and then removing any employee from a sensitive position. The determination or removal should be conclusive and final; and,
 - Granting an individual a clearance for access to information and material classified under Executive Order 12356 or predecessor order at the level of Confidential, Secret, or Top Secret, in cases where the official duties of the individual require such access. When access is no longer required, canceling the clearance and documenting the individual's security file accordingly.
- B. The **Inspector General** has been delegated the responsibility for establishing and maintaining ED's security and suitability program, as it relates to public trust positions at the high and moderate risk levels and to national security positions.
- C. The **Security Program Staff, Policy Planning and Management Services, OIG**, oversees the day-to-day operation of the security- suitability program.
- D. The **Director, Personnel Management Service, Office of Human Resources and Administration**, has been delegated the responsibility for suitability investigations and adjudication of public trust positions at the low risk level.
- E. **Principal Officers** are responsible for the Risk Designation System and for ensuring that appropriate investigative requirements are met.
- F. The **Security Representative** in each Principal Office Executive Office implements and operates the principal office's personnel security- suitability program.

VII. Orientation and Information for Employees

- A. Each Principal Office maintains a copy of the handbook for employees to review.
- B. Upon request, employees will be provided a copy of the Temporary Handbook.

- C. Any questions the employee may have regarding the content of the handbook or risk designation may be referred to their Executive Office. If an employee wants additional information, he or she may request a briefing. After the employee has had a briefing, and questions still remain, the employee may submit those remaining questions in writing to the Executive Office. The Executive Office will respond to written questions within 10 calendar days.
- D. Employees will be advised in writing when they need to complete personal history forms because of their position risk designation. They will also be reminded at that time of the location and availability of the handbook and the position designation record for their review.

Chapter 2 Suitability (Public Trust Positions)

I. Purpose

The purpose of this chapter is to establish criteria and procedures for making determinations of suitability for employment in positions in ED and for those who perform services for ED. This chapter includes positions involved either with the design, storage, retrieval, access, and dissemination of data processed through ED's ADP systems, or with ED's automated decision making systems.

II. Policy

This chapter sets out the policies for determining suitability, based on an individual's character or conduct, that may impact the efficiency of the service by jeopardizing ED's accomplishment of its duties and responsibilities.

Determinations made under this chapter are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions made under Executive Order 10450 or similar authorities. The waiver requirements under Executive Order 10450 do not apply to HR Public Trust Positions. Preappointment checks will be required prior to entrance on duty to those positions. Advisory Committee Members, because of their intermittent status, are exempt from the requirements of this handbook.

III. Authority

- 5 CFR 731;
- 5 U.S.C. 1302, 3301, 3302, 7301, 7701;
- Executive Order 10577, 3 CFR, 1954 - 1958 comp. p. 218;
- Executive Order 11222, 3 CFR, 1964 - 1965 comp. p. 306; and Executive Order 11491, 3 CFR, 1966 - 1970 comp. p. 861.

IV. Suitability Position Risk Criteria and Levels

General Requirements

Every position must be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position, as they relate to the efficiency of the service. The suitability risk levels are ranked according to the degree of adverse impact on the efficiency of the service that an unsuitable person could cause.

Risk Designation System

To determine position risk levels under this chapter, a Risk Designation System is used to assure that positions are designated uniformly and consistently throughout ED. Refer to Appendix A for further description.

In 1987, positions were designated according to OPM's Basic Installment 311. These positions will not require redesignation until positions are filled, new positions are established, position descriptions are revised, reorganizations occur, or there is a reason to adjust the risk level because of either computer related or national security requirements.

Those positions that were previously designated sensitive, but do not have national security duties and/or access to classified information, will be considered to fall under the position risk levels described in this chapter. For example:

- Special Sensitive and Critical Sensitive positions (see Chapter 3) would be considered to be at the HR Level.
- Noncritical Sensitive positions (see Chapter 3) would be considered to be at the MR Level.
- Nonsensitive positions would be considered to be at the LR Level.
- Computer/ADP positions may be considered to be at any risk level (see Section VIII of this chapter).

Criteria and Levels - Public Trust Positions

Criteria

- Most employees can affect certain Government activities. Such activities include law enforcement, public safety and health, collection of revenue, and regulation of business, industry, or finance.

- Other Government activities, not by their nature having as great an impact -upon the nation generally, include particular functions having the potential for damage. Positions having authority to commit Government funds through grants, loans, loan guarantees, or contracts would be public trust positions.
- Positions which are responsible for managing programs or operations require a high degree of public trust because of their ability to affect the accomplishment of ED's mission to a significant degree, including positions responsible for managing a significant portion of an ED program, such as a geographical district or area.

Risk Levels

The three suitability position risk levels and their adverse impacts on the efficiency of the service are as follows:

- **HR Public Trust Positions**, which have the potential for exceptionally serious impact, involving duties especially critical to the agency or a program mission with broad scope or policy or program authority, such as:
 - policy development and implementation;
 - higher level management assignments; or
 - independent spokespersons or non-management positions with authority for independent actions.
- **MR Public Trust Positions**, which have the potential for moderate to serious impact, involving duties of considerable importance to the agency or program mission, with significant program responsibilities and delivery of customer services to the public, such as:
 - assistants to policy development and implementation; mid-level management assignments;
 - non-management positions with authority for independent or semi-independent action; or
 - delivery of service positions that demand public confidence or trust.
- **LR Positions**, which involve duties of limited relation to the agency mission, with program responsibilities that affect the efficiency of the service.

In most cases, particularly at the low risk level, position risk is relatively clear, and the application of special designating procedures may not prove necessary.

Similarly, essentially identical positions may require only occasional case-by-case analysis. But in all these cases, even where risk levels appear to be "obvious," the designation should be treated by random application of specific procedures.

V. Suitability Determinations

Criteria

- *General.* In determining whether its action will promote the efficiency of the service, ED shall make its determination based on:
 - Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, efficient service in the position applied for or employed in;
 - Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, effective accomplishment by ED of its duties or responsibilities; and,
 - Whether a statutory or regulatory bar prevents the lawful employment of the individual in the position in question.
- *Specific.* When making a determination under this section, any of the following reasons may be considered a basis for finding an individual unsuitable:
 - Misconduct or negligence in prior employment that would have a bearing on efficient service in the position in question, or would interfere with or prevent effective accomplishment by ED of its duties and responsibilities;
 - Criminal conduct or dishonest conduct related to the duties to be assigned to the applicant or appointee, or to that person's service in the position or the service of other employees;
 - Intentional false statement, deception, or fraud in examination or appointment;
 - Refusal to furnish testimony as required by Civil Service Rule 5.4;
 - Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;
 - Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

- Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; or,
- Any statutory or regulatory bar that prevents the lawful employment of the person involved in the position in question.
- *Additional Considerations.* In making a determination under this section, ED will consider the following additional factors, to the extent that they are deemed pertinent to the individual case:
 - The kind of position for which the person is applying, or in which the person is employed, including the degree of public trust or risk in the position;
 - The nature and seriousness of the conduct;
 - The circumstances surrounding the conduct;
 - The recency of the conduct;
 - The age of the person involved at the time of the conduct; Contributing societal conditions; and,
 - The absence or presence of rehabilitation or effort toward rehabilitation.

Due Process

Disciplinary and/or adverse actions will be taken in accordance with ED's Personnel Management Instructions 751-1, May 27, 1981, and 752-1, March 29, 1983, and any other applicable agreements for bargaining unit employees. Any applicant, eligible, or appointee who is found unsuitable for any of the reasons cited above may appeal to the Merit Systems Protection Board under the Board's regulations.

VI. Risk Designation and Investigative Requirements

Risk Designation

Every position within ED will be designated at either an HR, MR, or LR level, as determined by the position's potential for adverse impact on the efficiency of the service. Refer to Appendices B and C.

For the purpose of this handbook, positions will be redesignated only as:

- they are filled,

- new positions are established,
- position descriptions are revised,
- reorganizations occur, or
- there are ADP or national security considerations.

Final adjustment in the designation process must take into account such factors as computer/ADP responsibilities and the need for access to classified national security information.

Investigative Requirements

- All employees at ED or from another agency selected for or moving to a position at a higher risk level than that previously occupied, must meet the investigative requirements of the new risk level (see Appendix B).
- If the risk level of the position itself is changed, the incumbent may remain in the position, but the investigation required by the new risk level must be initiated within 14 days after redesignation is final.
- If an employee has received the required investigation for placement in the new risk level, no reinvestigation is required unless updating is considered necessary because of the time elapsed since the previous investigation, or because of other special circumstances which justify additional investigation (see Suitability Reinvestigation).

Suitability Reinvestigation

Every incumbent of a position designated at an HR level will be subject to a periodic reinvestigation 5 years after placement and at least once each succeeding 5 years. Reinvestigations are also required if the individual had over a one-year break-in-service since the last investigation, even if that investigation was appropriate for the current position's risk level.

VII. Challenge to Risk Designation

- A. When an employee is notified that there is a need to complete personal history forms as indicated in Chapter 1, Section VH of this handbook, the employee may use the procedures in this section to challenge the risk designation of the position he/she occupies.
- B. Documents concerning the risk designation may be requested within 2 work days and shall be provided within 3 work days from the Executive Officer or his/her designee.

- C. Upon receipt of the risk designation information, the employee may file a reconsideration request, in writing, within 5 work days to the Executive Office or his/her designee.
- D. A written decision will be issued within 7 work days after receipt of the reconsideration request.
- E. The employee shall have 5 work days after receipt of the decision, to appeal in writing to the Security Officer or his/her designee.
- F. A final written decision will be issued within 20 work days after receipt of the appeal by the Security Officer or designee.
- G. This decision is final and will not be subject to further agency or grievance/arbitration review.
- H. The time frames in this appeal process may be extended, in writing, by mutual agreement.
- I. Except for an employee. in his or her first year of service with ED, an employee who has filed an appeal will not be required to complete a personal history form until the above administrative process has been exhausted.

VIII. Computer/ADP Risk Criteria and Levels

Security of Federal Automated Information Systems

Under OMB Circular No. A-130 (December 12, 1985), the Director, Office of Personnel Management, is to maintain personnel security policies for Federal personnel associated with, the design, programming, operation, maintenance, or use of Federal automated information systems. ED is required to establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. In accordance with OMB Circular A-130, ED policies and procedures for the security of Federal automated information systems must conform to the OPM guidance, which applies to all Federal employees.

Policies established and maintained by ED include requirements for screening all individuals (including contractors) participating in the design, development, operation, or maintenance of sensitive applications, as well as those having access to sensitive data. The level of screening required by these policies is to vary from minimal checks to full background investigations, depending on the sensitivity of the information to be handled and the risk and magnitude of loss or harm that the individual could cause.

Risk Levels and Criteria

The computer/ADP risk levels and criteria are to be used as an integral part of Suitability Position Risk Designation Systems described in Appendix A. In determining position placement, in addition to public trust criteria, any position with computer/ADP duties should have the following criteria applied.

Risk Levels

The three computer/ADP position risk levels are as follows:

- **HR Public Trust Positions**, which have the potential for exceptionally serious impact involving duties especially critical to the agency mission, with broad scope and authority, and with major program responsibilities that affect a major computer/ADP system(s).
- **MR Public Trust Positions**, which have the potential for moderate to serious impact, involving duties of considerable importance to the agency mission, and with significant responsibilities that affect large portions of a computer/ADP system(s).
- **LR positions**, which have the potential for impact involving duties of limited relation to the agency mission through the use of computer/ADP system(s).

Criteria

High Risk includes any position at the highest level of risk to the computer/ADP system. This is to include positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way as to incur a relatively high risk of causing grave damage or realizing a significant personal gain. Such positions may involve:

- Responsibility for the development and administration of ED's computer security programs, including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system that does not necessarily involve personal access to the system, but has relatively high risk of effecting grave damage or realizing significant personal gain.
- Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the

activities of the individual are not subject to technical review by higher authority to insure the integrity of the systems.

- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management -of systems hardware and software.
- Other positions, as designated by the agency head, that involve relatively high risk of effecting grave damage or realizing significant personal gain.

Moderate Risk includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the HR level to insure the integrity of the system. Such positions may involve:

- Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the HR level to insure the integrity of the systems. This level includes, but is not limited to:
 - access to and/or processing of proprietary data, and Privacy Act of 1974 and Government-developed privileged information involving the award of contracts; and,
 - accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.
- Other positions, as designated by the Secretary, that involve a degree of access to a system that creates a significant potential for damage or personal gain, but less than that in HR positions.

Low Risk includes all computer/ADP positions not falling into one of the above risk levels.

In order to establish uniformity and objectivity, ED must make computer/ADP risk designations in a systematic manner. Refer to instructions in Appendix A of this handbook and FPM chapter 731 and 732 for specific guidelines that may be applicable to the final designation.

Suitability Risk Level – Computer/ADP Risk Level Inter-Relationships

As positions may involve determinations of risk levels for both suitability and computer/ADP, the higher of the two is used to determine the possible adverse impact of the position and its final risk level.

Chapter 3 National Security Positions

I. Purpose

The purpose of this chapter is to set forth certain requirements ED shall observe for determining national security positions pursuant to Executive Order 10450, "Security Requirements for Government Employment."

II. Definition

For the purposes of this chapter, "National Security Position" includes positions in ED that require regular use of or access to classified information.

III. Applicability

The requirements of this chapter apply to competitive and excepted service positions, and to Senior Executive Service positions filled by career or non-career appointment within ED.

IV. Authority

The basic authority for investigating individuals for positions that involve national security is Executive Order 10450, 18 FR 2489, 3 CFR 1949-1953 comp., P.936, as amended unless otherwise noted, and related authorities.

V. Sensitivity Level Designation

General Requirements

All positions that have national security duties must be designated at national security sensitivity levels to assure appropriate screening under Executive Order 10450. Sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a position, could effect to the national security. The required investigation is conducted to provide a basis for insuring that employment of the individual is clearly consistent with the interests of the national security.

Risk Designation System

To determine position sensitivity levels under this chapter, the Risk Designation System in FPM Chapter 731, Appendix A, is used to assure that positions are designated uniformly and consistently. The national security criteria described in this chapter are used together with the risk designation system to arrive at the final position designation.

ED positions already designated will not require re-designation until positions are filled or new positions are established. Those positions previously designated as sensitive, including national security duties and/or access to classified information, no longer are

part of the position duties when filling existing positions or establishing new positions. The procedures in Chapter 1 of this handbook will be used.

National Security Sensitivity Criteria and Levels

There are 3 sensitivity levels for designating positions for national security related positions. These levels and the degree of risk to the national security associated with each are indicated below.

	<i>Sensitivity Levels</i>	<i>National Security Risk Criteria</i>
4	Special-Sensitive (SS)	Includes any position which the head of the agency determines to be at a level higher than Critical-Sensitive, because of special requirements under authority other than E.O. 10450 (e.g., DCID 1/14: investigative requirements and standards (Special Background Investigation - SBI) for access to Sensitive Compartmented Information (SCI) and other intelligence-related "Special Sensitive" information).
3	Critical-Sensitive (CS)	<p>Potential for exceptionally grave damage to the national security.</p> <p>Includes positions involving any of the following:</p> <ul style="list-style-type: none">• Access to Top Secret defense information;• Development or approval of war plans, plans or particulars of future or major or special operations of war;• Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or• Other positions related to national security, regardless of duties, that require the same degree of trust.
2	Noncritical-Sensitive (NCS)	<p>Potential for some damage to serious damage to the national security.</p> <p>Includes positions that involve one of the</p>

following:

- Access to Secret or Confidential national security materials, information, etc.; or
- Duties that may directly or indirectly adversely affect the national security operations of the agency.

VI. Security Office Record on Sensitivity Designation, Access Level, and Investigative Requirement

The Security Program Staff, Policy, Planning, and Management Services, OIG, will maintain a record on the following for each position in ED:

- Sensitivity level of the position and coding for personnel documents under Chapter 3:

Level	Code*
4 Special-Sensitive (SS)	4
3 Critical-Sensitive (CS)	3
2 Noncritical-Sensitive (NCS)	2
1 Non-Sensitive (NS)	1

*Identify ADP-computer positions with a "C" after the code.

Include the completed Position Designation Record (see sample, Appendix C) in the record.

- The position's level of access to classified information under Chapter 3:

Level	Code
Not Required	0
Confidential (C - E.O. 12356)	1
Secret (S - E. O. 12356)	2
Top Secret (TS - E.O. 12356)	3
Sensitive Compartmented Information (SCI - DCID 1/14)	4

- Personnel background investigation requirement under Chapter 4:

Special Background Investigation (SBI) Background Investigation (BI)

Limited Background Investigation (LBI)
Minimum Background Investigation (MBI)

VII. Waiver Requirements

General

A waiver of the preappointment investigative requirement contained in Section 3(b) of Executive Order 10450 for employment in a sensitive national security position may be made only for a limited period:

- In the case of an emergency, if the Secretary or his designee finds that such action is in the national interest; and
- When such finding is made a part of ED's records.

Specific Waiver Requirements

- The preappointment investigative requirement may not be waived for appointment to positions designated Special-Sensitive.
- For positions designated Critical-Sensitive, prewaiver checks will be conducted.
- Requests for waivers may be initiated only when the performance of ED's mission is at risk. Workload, backlogs, or administrative problems caused by vacancies will not in themselves be sufficient bases for a waiver application.
- When a waiver is authorized, the required investigation will be initiated within 14 days of placement of the individual in the position.

VIII. Exceptions to Investigative Requirements

Pursuant to Section 3(a) of Executive Order 10450, the following positions are exempt from the investigative requirements of Executive Order 10450, providing that certain checks are conducted to ensure that the employment or retention of individuals in these positions is clearly consistent with the interests of the national security:

- Positions that are intermittent, seasonal, per diem, or temporary, not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments; or,
- Other positions that ED, in its discretion, deems appropriate may be made exempt based on a written request to OPM by the Secretary.
- If there is verifiable evidence of a prior investigation, it may not be necessary to initiate a duplicate investigation. However, the investigation required by the

sensitivity level of the position applied for or appointed to must be conducted, unless the break-in-service is 12 months or less and the required investigation was conducted no more than 36 months before the date of the appointment.

IX. Periodic Reinvestigation Requirements

The incumbent of each position designated Special-Sensitive, Critical-Sensitive or Noncritical-Sensitive for national security reasons will be subject to periodic reinvestigation 5 years after placement, and at least each succeeding 5 years.

The results of this periodic reinvestigation will be used to determine whether the continued employment of the individual in a sensitive position is clearly consistent with the interest of the national security.

X. Due Process

When ED makes an adjudicative decision under this chapter based on a background investigation, or when, as a result of information in a background investigation, changes a tentative favorable, placement or clearance decision to an unfavorable decision, ED will:

- Insure that the records used in making the decision are accurate, relevant, timely, and complete to the extent reasonably necessary to assure fairness to the individual in any determination;
- Comply with all applicable administrative due process requirements, as provided by law, rule, or regulation; and
- At a minimum, provide the individual concerned:
 - Notice of specific reason(s) for the decision;
 - An opportunity to respond; and,
 - Notice of appeal rights, if any.

Chapter 4 Personnel Investigations

I. Purpose

The purpose of this chapter is to specify certain requirements for personnel investigations conducted by OPM. The requirements of this chapter apply to investigations required for public trust positions under Chapter 2 of this handbook and for national security positions under Chapter 3 of this handbook (see Appendix B).

II. Public Availability of Investigative Files

Investigative files are records subject to the Privacy Act and the Freedom of Information Act, and are made available to requestors in accordance with the provisions of those Acts.

Requests for OPM investigative records can be submitted to the Office of Personnel Management, Federal Investigations Processing Center, FOI/PA, Boyers, PA 16018.

III. Personnel Investigations Forms

The following forms are to be completed to initiate Security-Suitability investigations. The form to be used is determined by the type of position, as indicated in the form title.

- SF-85, Questionnaire for Non-Sensitive Positions
- SF-85P, Questionnaire for Public Trust Positions
- SF-86, Questionnaire for Sensitive Positions (for national security)
- OFI Form 36, Additional Data for Single Scope Background Investigations and Other Background Investigations
- SF-86A, Continuation Sheet for Questionnaires, SF-86, SF-85P and SF-85.
- SF-87, Fingerprint Chart
- FD-258, Fingerprint Chart (for contractor employees)

An SF-171, Application for Federal Employment (June 1988 or later edition), must be submitted with each set of forms.

Optional Questions. OPM has made the responses to some questions on the SF-85P optional. Those questions are:

- (18) Your police record.
- (19b) Illegal drugs and alcohol. Have you experienced problems (disciplinary actions, evictions, formal complaints, etc.) on or off the job from your use of illegal drugs or alcohol?
- (21) Your medical record.

Occupants of positions designated HR Public Trust Positions are required to respond to all of these questions.

A response to these questions is not required by occupants of MR Public Trust Positions.

All questions on the SF-86 require responses.

The Security Representative and the Principal Office Systems Security Officer (POSSO) will coordinate the completion of the Request for Security Officer Action form (ED 80-0700, see Appendix D for a sample), which will be attached to the completed forms (SF-85P, SF-86, OFI Form 36, SF-87 or 258, and SF-171) and sent to the Security Program Staff, Policy, Planning, and Management Services, OIG.

Appendix A

Risk Designation System

Introduction

This designation system provides a systematic way of obtaining uniformity in Risk Level designations:

- To Determine General Risk Criteria for placement of agency, programs, and positions.
- To Apply Criteria:

• For suitability	FPM 731 Subchapter 2 and Chapter 2 of this handbook.
• For Computer/ADP	FPM 731 Subchapter 7 and Chapter 2 of this handbook.
• For National Security	FPM 732 Subchapters 2 and 6 and Chapter 3 of this handbook.

- To Obtain Final Position Risk Level:

• High Risk	FPM 731 and Chapter 2 of this handbook.
• Moderate Risk	FPM 731 and Chapter 2 of this handbook.
• Low Risk	FPM 731 and Chapter 2 of this handbook.
• National Security Sensitivity levels	FPM 732 and Chapter 3 of this handbook.

When an agency, a program, or a position/group of positions is fully or predominantly involved in national security/access to classified information, the criteria and designation procedures in FPM Chapter 732 and Chapter 3 of this handbook may apply in full or together with the Public Trust criteria of Chapter 731 and Chapter 2 of this handbook.

The Risk Designation System

The Risk Designation System process is divided into three parts:

1. Designation of an agency and program for its impact (Major, Substantial, Moderate, or Minimal) and scope (Worldwide, Government-wide, Multi-agency, or Agency), as related to the efficiency of the service.
2. Designation of the position(s) for its degree of risk to the program, as related to the efficiency of the service. Degree of risk is divided into four categories (Major, Substantial, Limited, and

Minimal), and is calculated in five factor description areas (Degree of Public Trust, Fiduciary (Monetary) Responsibility, importance to Program, Program Authority, and Autonomy).

3. Final designation of position risk includes using parts I and 2 above to determine Position Placement, followed by adjustments that include descriptions of unique factors specific to positions and organizational uniformity or operations. These steps should be taken to arrive at the final designation of the position. When it is obvious that part 3 will place the position at a higher risk level, the other steps may not be needed.

Adjustments

Adjustments made to the Sensitivity Designation System in Basic Installment 347, September 29, 1988, FPM Chapter 731, Appendix A, will not require agencies to re- designate existing positions with the Risk Designation System in the appendix, until there is a reorganization, the positions are vacated, the position description is revised, or there is a reason to adjust the risk level because of computer or national security requirements.

The adjustments made reflect the changes to FPM Chapters 731, 732, and 136, and do not change position designation based on risk as described. The principal adjustments were made to consolidate and reduce the number of factors used to arrive at levels in part 1 and 2 above. The end result is to prevent over- or under- designation in determining low, moderate, and high risk levels and compatibility with the three levels of position sensitivity in FPM Chapter 732.

Appendix B

Which Form? Which Investigation?

National Security Investigations

Sensitivity Level	Investigative Form Used	Type of Investigation
4 Special Sensitive	SF-86	SBI
3 Critical Sensitive	SF-86	BI
2 Noncritical Sensitive	SF-86	LBI MBI
1 Non Sensitive	SF-85	NACI

Public Trust Investigations

Risk Level	Investigative Form Used	Type of Investigation
6 High Risk	SF-85P	BI
5 Moderate Risk	SF-85P*	LBI or MBI
1 Low Risk	SF-85	NACI

Note: An SF-171 must accompany any request for investigation. For the SF-85 and 85P, the SF-171 should be the June 1988, or later edition and should be updated to the date the SF-85 or SF-85P is signed. For the SF-86, the SF-171 should be a copy of the SF-171 used to make the appointment.

The letter "C" will be added after the numerical risk level to denote ADP responsibilities.

*Individual is not required to respond to optional questions.

Appendix C

Position Designation Record. The Principal Office will complete the Position Designation Record form, which will become part of the Security Program system of records.

POSITION DESIGNATION RECORD

AGENCY: _____ PROGRAM: _____

POSITION TITLE: _____

POSITION DESCRIPTION #: _____

RISK DETERMINATION SYSTEM

I. PROGRAM PLACEMENT:*

Impact on Efficiency of Service:	<u> N/A </u>
Scope of Operations for Efficiency of Service:	<u> N/A </u>
Placement (Major, Substantial, Moderate, Limited)	<u> Moderate </u>

II. POSITION PLACEMENT:

<u>Risk Factors</u>	<u>Risk Points</u>
a. Degree of Public Trust (7-1):	_____
b. Fiduciary Responsibilities (7-1):	_____
c. Importance to Program (7-1):	_____
d. Program Authority Level (7-1):	_____
e. Supervision Received (7-1):	_____
TOTAL POINTS	_____

III. POSITION PLACEMENT (HR: MR: LR):

Adjustments (Include Computer-ADP Position Risk Criteria): Comments:

FINAL PLACEMENT (Risk level/Sensitivity level/Access level):

Signature of Agency Designator

Date

*Program placement for ED has been predetermined.