Position Designation Overview

Working for America

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Message from the President

“We are serving in freedom’s cause—and that is the cause of all mankind.”

- George W. Bush

Message from the Director

“ In today’s times, there can be no question of the need for accurate, complete, timely, and relevant background investigations of those whom the American people entrust to perform important public service functions. The safety of our employees, our families, and our country is ultimately at stake, and we can have no greater priority.”

- Kay Coles James

Suitability Authority
5 CFR 731. 106(a)

REQUIREMENT:

“Agency heads shall designate every competitive service position within the agency at either a high, moderate, or low risk level as determined by the position’s potential for adverse impact to the integrity and efficiency of the service.”

Suitability Risk Levels

- **High Risk (HR)**
- **Moderate Risk (MR)**
- **Low Risk (LR)**

} **Public Trust**

Risk Designation System

- **Program Designation**
- **Position Risk Points**
- **Position Designation**
- **Adjustments**
- **Final Designation**

Items Needed To Designate Positions

- **Document(s) describing the mission and responsibilities of the agency or a program**
- **Position description and/or other documentation of the duties and responsibilities of a position**
- **Position Placement Record form**
- **Appendix B “Designation of Public Trust Positions and Investigation Requirements”**

Program Placement

IMPACT

- **MAJOR**
- **SUBSTANTIAL**
- **MODERATE**
- **LIMITED**

(See Appendix B, Table 1)

Program Placement (Continued)

SCOPE OF OPERATIONS

- WORLDWIDE
- GOVERNMENTWIDE
- MULTI-AGENCY
- AGENCY

(See Appendix B, Table 1)

Program Placement

IMPACT	WORLDWIDE	GOVERNMENTWIDE	MULTI-AGENCY	AGENCY
MAJOR	MAJOR	MAJOR	SUBSTANTIAL	MODERATE
SUBSTANTIAL	MAJOR	SUBSTANTIAL	SUBSTANTIAL	MODERATE
MODERATE	SUBSTANTIAL	MODERATE	MODERATE	LIMITED
LIMITED	MODERATE	MODERATE	LIMITED	LIMITED

Position Risk Factors and Points

DEGREE OF PUBLIC TRUST

- Provides advice and guidance to senior officials
- Conducts audits and reviews
- Analyzes, evaluates, and provides leadership in governmentwide HR programs and practices

Position Risk Factors and Points (Continued)

FIDUCIARY RESPONSIBILITY

No fiduciary responsibility is listed in the position.

Note: All point values must be between 1 and 7

A point value of 0 is not acceptable

Position Risk Factors and Points (Continued)

IMPORTANCE TO PROGRAM

- Advises, evaluates, interprets, and recommends
- Provides technical and program guidance
- Identifies, analyzes, and resolves very complex Human Capital problems

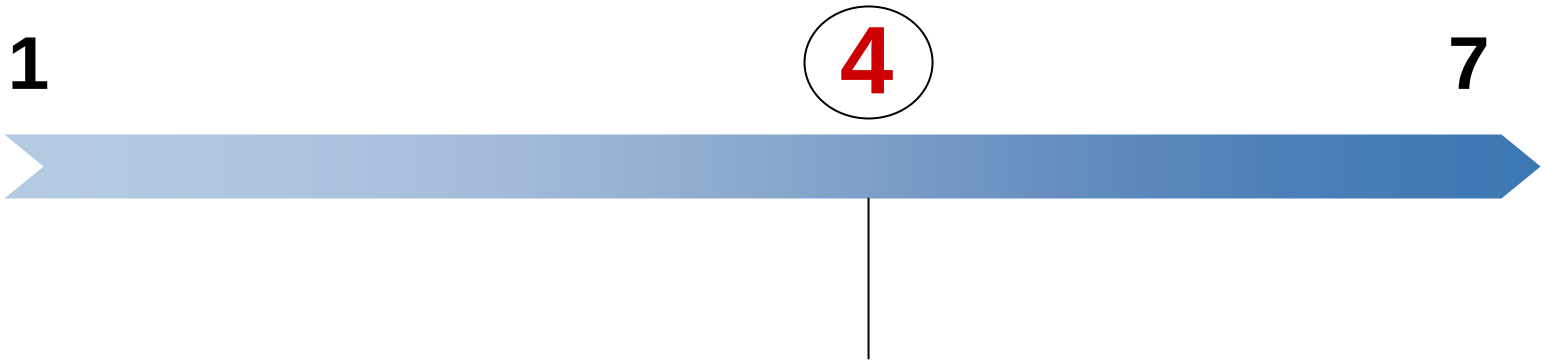
Position Risk Factors and Points (Continued)

PROGRAM AUTHORITY

- Leads team and makes assignments
- Designs the methodology needed to accomplish goals
- Manages day-to-day activities

Position Risk Factors and Points (Continued)

SUPERVISION RECEIVED



- Organizes work independently
- Defines objectives and determines short or long term goals
- Plans assignments and sets priorities

Initial Designation

Position Risk Points

Program Designation

	5-10	11-17	18-23	24-29	30-33
MAJOR	Low Risk NACI	Moderate Risk LBI	Moderate Risk LBI	High Risk BI	High Risk BI
SUBSTANTIAL	Low Risk NACI	Moderate Risk LBI	Moderate Risk LBI	High Risk BI	
MODERATE	Low Risk NACI	Low Risk NACI	Mod Risk MBI		
LIMITED	Low Risk NACI	Low Risk NACI			

Adjustments

UNIQUENESS: factors that can cause the position's designation to be elevated.

They include:

- **Public Health/Safety Duties**
- **Investigative Duties**
- **Computer/ADP**
- **National Security**

(Appendix B, page 8 has the complete list)

Uniformity

- **To assure positions at the same authority level are uniformly designated within the agency**
- **To assure the designation level of a program overrides any specific risk considerations of individual positions**

Final Designation

High Risk (HR)
Moderate Risk (MR)
Low Risk (LR)

} **Public Trust**

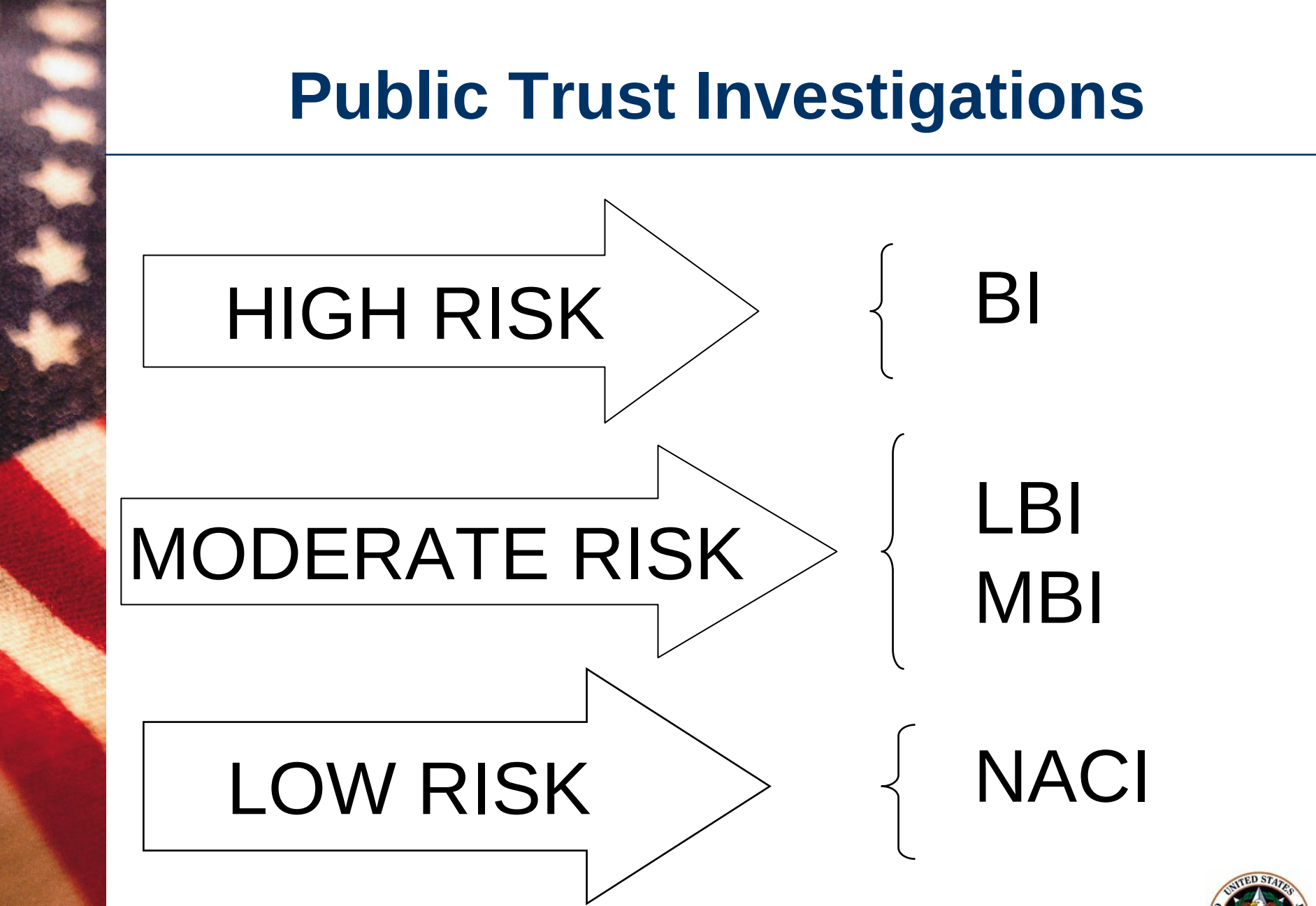
Special Sensitive (SS)
Critical-Sensitive (CS)
Noncritical-Sensitive (NCS)
Nonsensitive (NS)

} **National Security**

Investigations Defined

- **NAC – Included in all background investigations**
  - **SII - OPM's Security/Suitability Investigations Index**
  - **DCII - Defense Clearance and Investigations Index**
  - **FBIF - FBI National Criminal History Fingerprint Check**
  - **FBIN - FBI Investigative File Name Check**
- **NACI – National Agency Check w/Inquiries**
  (Minimum investigation for Federal employees)
- **MBI – Minimum Background Investigation**
- **LBI – Limited Background Investigation**
- **BI – Background Investigation**

Public Trust Investigations



Facts To Know

- **All appointments in the Federal service require the person to be investigated (E.O. 10450).**
- **Investigations should be initiated pre-appointment or, at most, within 14 calendar days of placement in a position or the date a designation is elevated.**
- **An investigation is required if there has been a break in service of greater than 2 years.**
- **At any time it is discovered that the investigation for the initial subject to investigation appointment has not been done, the required investigation must be done.**

FACTS TO KNOW (Continued)

- **A change that increases the risk level of the position requires a higher level investigation.**
- **The following actions do not require an investigation <u>unless the position designation is elevated</u>:**
  - **Promotion/Demotion**
  - **Reassignment**
  - **Conversion from career-conditional to career tenure**
  - **If the subject has served at least one year under an appointment subject to investigation (re: transfer, or an appointment or conversion within an agency) and has the appropriate investigation**

Facts To Know (Continued)

- **An investigation is not required for the following positions designated LR:**
  - **Intermittent**
  - **Seasonal**
  - **Per diem**
  - **Temporary (Not to exceed an aggregate of 180 days either in a single or series of appointments, however, agency must still screen)**

Position Designation Record

Reasons to retain the Position Designation Record form:

- **Lawsuits**
- **Employee/union challenges**
- **OPM and Agency audits**
- **Vacancy designation purposes**

Computer/ADP Positions

- **5 CFR Part 731. 106(a)**
- **OMB Circular A-130**
- **Computer Security Act of 1987**

Unique Factors For Computer/ADP Positions

High Risk (HR):

- Develops, directs, plans, and designs major systems
- Involvement in life-critical or mission-critical systems
- Authorization to disburse $10M or more yearly

Moderate Risk (MR):

- Access to Proprietary or Privacy Act of 1974 Data
- Authorization to disburse less than $10M yearly
- Potential for damage or personal gain

Low Risk (LR):

- Includes all Computer/ADP positions that do not meet the above criteria

National Security Authority E.O. 10450 Sec. 3(b) 5 CFR 732.201

REQUIREMENT:

“The head of any department or agency shall designate or cause to be designated, any position within the department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position.”

Facts To Know

- **A National Security sensitivity level designation overrides a Public Trust risk level designation.**
- **If the Public Trust risk level designation for a position requires a higher level of investigation than the investigation for the National Security access/sensitivity level, the higher level of investigation is done.**
- **Investigation type is determined by the provisions of E.O. 12968.**

Summary

- **Evaluate and review all positions using the Risk Designation System to determine the risk level for Public Trust designation (non-computer and computer)**
- **Consider any unique or uniformity adjustments**
- **Determine if National Security sensitivity designation is appropriate**
- **Select appropriate investigation**

Contact Information

For more information,
visit us on the web at
www.OPM.gov or
www.OPM.gov/extra/investigate

Karen Benson
Kimberly Lew
Investigations Program Specialists
202-606-1042

–

CHAPTER II

POSITION RISK DESIGNATION AND INVESTIGATIVE REQUIREMENTS

A. PUBLIC TRUST

1. Designation of Public Trust Positions. Agencies are responsible for designating each competitive service position within the agency based on the documented duties and responsibilities of the position. Each position will be designated at the High, Moderate, or Low risk level depending on the position's potential for adverse impact to the integrity and efficiency of the service (5 CFR 731.106). Positions at the High and Moderate risk levels are referred to as "Public Trust" positions. These positions generally involve the following duties or responsibilities:

- Policy making;
- Major program responsibility;
- Public safety and health;
- Law enforcement duties;
- Fiduciary responsibilities; and
- Other activities demanding a significant degree of public trust.

Public Trust positions also involve access to, operation or control of proprietary systems of information, such as financial or personal records, with a significant risk for causing damage to people, programs or an agency, or for realizing personal gain.

2. Risk Levels. The three suitability position risk levels are defined and explained in the table below.

RISK LEVELS	DEFINITIONS AND REPRESENTATIVE DUTIES OR RESPONSIBILITIES
HIGH **(HR)** **Public Trust Position**	**Positions with the potential for *exceptionally serious impact* on the integrity and efficiency of the service.** Duties involved are especially critical to the agency or program mission with a broad scope of responsibility and authority. Positions include: • Policy-making, policy-determining, and policy-implementing; • Higher level management duties or assignments, or major program responsibility; • Independent spokespersons or non-management position with authority for independent action; • Investigative, law enforcement, and any position that requires carrying a firearm; and • Fiduciary, public contact, or other duties demanding the highest degree of public trust**.**
MODERATE **(MR)** **Public Trust Position**	**Positions with the potential for *moderate to serious impact* on the integrity and efficiency of the service.** Duties involved are considerably important to the agency or program mission with significant program responsibility or delivery of service. Positions include: • Assistants to policy development and implementation; • Mid-level management duties or assignments; • Any position with responsibility for independent or semi-independent action; and • Delivery of service positions that demand public confidence or trust.
LOW **(LR)**	**Positions that involve duties and responsibilities of *limited relation* to an agency or program mission, with the potential for *limited impact* on the integrity and efficiency of the service.**

–

3. Risk Designation System. OPM's model for designating public trust positions is included in this handbook as Appendix B. Agencies are encouraged to use this model but may develop their own framework for designating public trust to ensure uniformity and consistency. Any alternative system an agency develops must consider the same factors that OPM's risk designation system considers, must be documented in writing, and must be used consistently by the agency.

4.Relationship of Suitability Risk and National Security Sensitivity to Investigation Type. Basic suitability screening is required for all positions. The first determination an agency must make is whether the person has the character traits and past conduct expected of someone who is to carry out the duties and responsibilities of a Federal job in order to protect the integrity and promote the efficiency of the service.

Once a suitability determination is made, if appropriate, the person then can be screened based on National Security considerations, including considerations for access to classified information and sensitive, restricted facilities (as outlined in 5 CFR 732). Because Public Trust duties and responsibilities may outweigh National Security considerations at the lower access levels (Secret and Confidential), agencies must consider both suitability and security aspects of a position in determining the appropriate type of investigation to conduct.

> For example, if a position is designated High Risk under suitability, but the incumbent of that position needs a Secret clearance, a Background Investigation (BI) is required. A BI is the minimum investigation required for a position designated High Risk. An Access National Agency Check with written inquiries (ANACI) for the Secret clearance would not be appropriate. Of the two investigation types, ANACI and BI, the BI provides the higher level of screening required for the High Risk position. The BI also meets the investigative requirement for Secret access. The ANACI does not meet the screening requirements for a High Risk position.

B. COMPUTER SECURITY

1. Security of Federal Automated Information Systems. Under OMB Circular No. A-130 (December 12, 1985, amended November 2000), 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. Agencies are instructed 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, agency policies and procedures for the security of Federal automated information systems must conform to OPM guidance in this Handbook, which applies to all Federal employees.

Policies established and maintained by agencies must include requirements for screening individuals authorized to bypass significant technical and operational controls of the system commensurate with the risk and magnitude of harm they could cause. Agencies must also incorporate controls such as separation of duties and individual accountability into the application process and application rules. When such controls cannot adequately protect the application process or system information, agencies should screen individuals commensurate with the increased risk and magnitude of the harm they could cause. Such screening must occur before the individual is authorized application access and periodically thereafter. The level of screening will 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 the individual could cause.

The Computer Security Act of 1987 (PL 100-235) requires Federal agencies to identify every computer system that contains sensitive information and to prepare a plan for the security and privacy of each. Sensitive information, as defined in OPM guidance, is any information, the loss, misuse, or modification

of which, or the unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

2. Designating Computer/ADP Risk Levels. Specific guidance for designating Computer/ADP risk levels and criteria is contained in Appendix B of this Handbook.

C. SUITABILITY INVESTIGATIONS

1. Appointments Subject to Investigation. As required in 5 CFR 731, persons appointed in the competitive service must undergo an investigation by OPM or by an agency conducting investigations under delegated authority from OPM. Except when required because of risk level changes, a person in the competitive service who has undergone a suitability investigation need not undergo another investigation simply because the person has been:

- Promoted;
- Demoted;
- Reassigned;
- Converted from career-conditional to career tenure;
- Appointed (or converted to an appointment) when that employee has been serving with that agency for at least one year in one or more positions under an appointment subject to investigation; or,
- Transferred, provided the individual has served continuously for at least one year in a position subject to investigation.

2. Reemployments. Reemployments are not one of the general exceptions to the subject to investigation rule. When individuals are reemployed in Federal service, they should complete a new Declaration for Federal Employment (OF 306). They should also complete new investigative questionnaires (or update their prior form if the public trust or sensitivity level of their new position is the same as the old one). If suitability issues are admitted on the OF 306 or investigative questionnaire, or if they are otherwise developed, they should be investigated and adjudicated.

If there are no suitability issues, and there has not been a break in service of longer than 24 months, a new investigation is not necessary unless it is required under 5 CFR 732, or other authority, or because of a higher public trust risk level. The adjudicative guidelines established by 5 CFR 731 will be used for all reemployments that are subject to investigation and adjudication.

3. Investigative Requirements. Pursuant to the authority delegated by the President of the United States under 5 U.S.C. sections 1104 and 3301, and Executive Order 10577, OPM requires individuals seeking admission to the civil service to undergo investigation to establish their suitability for employment. OPM has determined that varying levels of investigation are appropriate, depending on the responsibilities of the position. The minimum level of investigation required for entry into the Federal service is the National Agency Check and Inquiry (NACI) investigation. OPM recommends that individuals in contract and excepted service positions also be investigated appropriately in order to ensure they are suitable to carry out their duties and responsibilities in a manner that will protect the integrity and promote the efficiency of the service. The same method of determining which level of investigation to conduct on competitive service positions (i.e., Risk Designation System) should be used for contractors or excepted service positions.

The type of investigation to conduct is a product of the risk level designation of a position and, if appropriate, National Security requirements. OPM has established the following **minimum** levels of

–

required investigation for positions at the Low, Moderate, and High risk levels:

RISK LEVEL	MINIMUM REQUIRED INVESTIGATION
LOW Risk →	**NACI** – National Agency Check and Inquiries
MODERATE Risk →	**MBI** – Minimum Background Investigation
HIGH Risk →	**BI** – Background Investigation

In some cases, OPM recommends a more comprehensive investigation to take into account unique factors specific to the duties and responsibilities of a position, the organizational need for uniformity of operations, or National Security considerations. Refer to Appendix B for further guidance on determining the appropriate level of investigation.

4. Timing of Investigations. Investigations should be initiated before appointment or, at most, within 14 calendar days of placement in the position. If, at any time, it is determined that a required investigation has never been conducted for the initial subject to investigation appointment, the appropriate required investigation must be conducted, even if there have been subsequent personnel actions that would not be subject to investigation (such as transfers, promotions, or reassignments).

5. Change in Position Risk Level. All employees moving to a new position at a higher risk level than the risk level of the position they left must meet the investigative requirements of the risk level designation of the new position. It is a good practice to complete the required investigation before the individual moves to the new position. Any required higher level investigation must be initiated within 14 working days of the date the new position is occupied. If the risk level of an incumbent's position is increased due to a change in duties and responsibilities, the incumbent may remain in the position, but the investigation required by the higher risk level should be initiated within 14 working days of the effective date of the new position designation. This guidance applies to details as well as permanent reassignments.

If there are new potentially disqualifying suitability issues after such an investigation, the authority the agency uses to adjudicate will depend on the subject's employment status: 5 CFR 315, to terminate a temporary appointment; 5 CFR 752, if an adverse action under that authority is warranted; etc.

6. Exceptions to Investigative Requirements. Exceptions to the investigative requirements are made in the following positions at the Low risk level: intermittent, seasonal, per diem, or temporary, not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments. *The agency must still conduct sufficient checks to ensure that the employment or retention of the individual is clearly consistent with the integrity and efficiency of the service* (5 CFR 732.202).

7. Questionnaires for Suitability Investigations. Use the Standard Form 85 (SF 85) *Questionnaire for Non-Sensitive Positions* for all positions designated Low Risk. For positions designated Moderate or High Risk, use the Standard Form 85P (SF 85P) *Questionnaire for Public Trust Positions*. The Standard Form 86 (SF 86) *Questionnaire for National Security Positions* is to be used for positions involving the National Security with sensitivity level designations. Permission to use the SF 86 for positions with other than sensitivity level designations (i.e., public trust positions) must be obtained from OPM prior to using the form to initiate investigations. The Standard Form 85P-S (SF 85PS) *Supplemental Questionnaire for Selected Positions* contains additional questions and is used only when an agency requests, and is granted, OPM approval to use it (by Special Agreement with OPM).

If a new investigation is needed because of a risk or sensitivity level change, the person should complete a

new investigative form. A previously completed investigative form may be updated for this purpose only when the same form is required for the new investigation (and the form has not been revised or replaced with a newer version).

8. Suitability Reinvestigations. Although OPM has no authority to require agencies to conduct reinvestigations in suitability cases, we recommend reinvestigations for certain Moderate and High Risk public trust positions. Lacking a requirement to request reinvestigations, agencies must ensure they have appropriate authority, such as the Computer Security Act of 1987, OMB Circular No. A-130, agency-specific regulations, or written policy. When the authority exists, OPM recommends a minimum of a Periodic Reinvestigation (PRI) for High Risk positions, a National Agency Check with Credit (NACC) investigation for Moderate Risk positions.

Agencies may request variations in the type of reinvestigations from OPM and may make their requirements appropriate to specific positions. For example, for a position with access to money where there is a potential for theft, such as an Imprest Fund Manager or Bank Examiner, the appropriate reinvestigation could be a credit search, Subject interview, and residence coverage.

9. Coding of Position Risk Level on Personnel Documents. The code for the position risk level is required on Optional Form 8, or the equivalent agency form, and agencies are required to place the code for the position risk level in the *Remarks* section of the Standard Forms 50 and 52. The codes are these:

RISK LEVEL	**CODE**
High	6
Moderate	5
Low	1

*Identify a Computer/ADP position by placing the letter "*C*" after the code* (*i.e.*: 6C, 5C, 1C).

APPENDIX B

DESIGNATION OF PUBLIC TRUST POSITIONS AND INVESTIGATION REQUIREMENTS

A. PUBLIC TRUST DESIGNATION MODEL

Introduction. Proper position designation is the foundation of an effective and consistent suitability program. It determines what type of investigation is required and how closely an individual is screened for a position. Additionally, as the level of authority and responsibility of a position become greater, character and conduct become more significant in deciding whether employment or continued employment would protect the integrity and promote the efficiency of the Federal service.

OPM recommends the following Risk Designation System to provide a systematic, consistent, and uniform way of determining risk levels of positions. OPM strongly encourages agencies to follow this model but they are not required to do so. Agencies must have a consistent and uniform method for determining the risk level of positions in their agency. An alternative risk designation system an agency develops or adopts must include the same or similar factors as those in OPM's system. An agency can add factors as long as the factors apply to the agency's mission and the duties and responsibilities of the positions. If an agency develops or adopts a system for designation, the system must be documented and maintained, just as procedural guidance requires that OPM's system be documented and maintained.

Position Designation Records. The agency must complete and maintain the Position Designation Record or its equivalent for each agency position. Agency personnel offices will maintain the record of Public Trust suitability designations; copies should be maintained by the agency security offices, as well. The Position Designation Records are subject to review by OPM during periodic appraisals of agency suitability programs, or on a case-by-case basis, to assure that agencies are considering all pertinent factors when designating positions relative to the integrity and efficiency of the service.

The Risk Designation System. The Risk Designation System is divided into three parts:

- ***Program Designation.*** (The agency identifies both the impact and scope of an agency or agency program as related to the integrity and efficiency of the service. This determines the "program designation.")

- ***Position Risk Designation Points.*** (The agency determines the degree of risk that a position poses to the agency or an agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total "position risk designation points" for a position.)

- ***Position Designation.*** (The Program Designation and Position Risk Designation Points are applied to determine the risk level "position designation.")

  At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation will result in a higher risk level, the other steps may not be needed.

Once these are completed, the agency decides the "final designation" of the position and the type of investigation to conduct.

POSITION DESIGNATION RECORD

AGENCY: _____ **PROGRAM:** _____

POSITION TITLE, SERIES, & GRADE: _____

POSITION DESCRIPTION #: _____

RISK DESIGNATION SYSTEM

I. PROGRAM DESIGNATION

IMPACT, Integrity & Efficiency of Service…… ☐

SCOPE of Operations, Integrity & Efficiency of Service.. ☐

PROGRAM DESIGNATION (Major, Substantial, Moderate, Limited).. ☐

II. POSITION RISK DESIGNATION POINTS

RISK FACTORS & POINTS:

DEGREE OF PUBLIC TRUST…… ☐
FIDUCIARY RESPONSIBILITIES…… ☐
IMPORTANCE TO PROGRAM…… ☐
PROGRAM AUTHORITY LEVEL…… ☐
SUPERVISION RECEIVED…… ☐

TOTAL POINTS…… ☐

III. POSITION DESIGNATION

UNADJUSTED **RISK LEVEL**…… ☐

MINIMUM **INVESTIGATION**……. ☐

Note "(c)" *after the risk level if this is a Computer-ADP*

ADJUSTMENTS FOR UNIQUENESS AND UNIFORMITY? COMMENTS:

FINAL DESIGNATION (Risk level/Sensitivity level/Access level)…… ☐

MINIMUM INVESTIGATION…… ☐

_____ _____

PRINTED NAME & SIGNATURE OF AGENCY DESIGNATOR **DATE**

FILLING OUT THE POSITION DESIGNATION RECORD

Program Designation

- ***Program Designation.*** The agency identifies both the impact and scope of an agency or agency program as related to the integrity and efficiency of the service. This determines the "program designation."

Use these steps and Table 1 on the next page to complete part I –"Program Placement"

1) **Impact on the Integrity and Efficiency of the Service:** Identify the impact description in the IMPACT column of Table 1 that best describes the agency or agency program. If there is a question regarding the designation of an agency or agency program at one of two impact descriptions (such as whether it is *SUBSTANTIAL* or *MODERATE*), the decision should be based on the best interests of the agency mission.

2) **Scope of Operations in Terms of the Integrity and Efficiency of the Service:** Identify the scope of operations described in the four SCOPE OF OPERATIONS columns of Table 1.

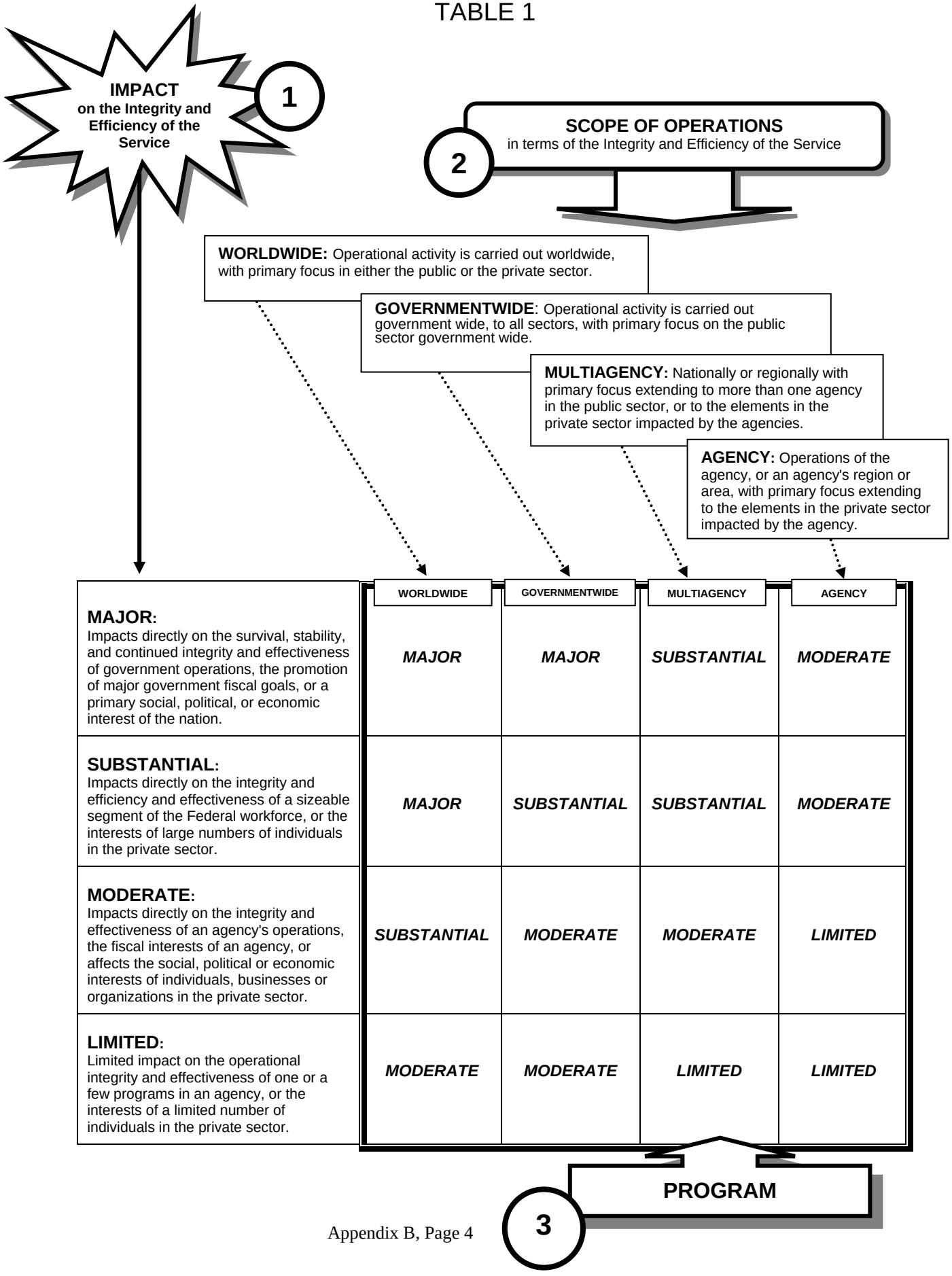
3) **Determining Program Designation:** The box at the intersection of the IMPACT row and SCOPE column identifies the program designation.

Examples:

① SUBSTANTIAL IMPACT and ② MULTIAGENCY SCOPE = ③ *SUBSTANTIAL* Program Designation.

① LIMITED IMPACT and ② WORLDWIDE SCOPE = ③ *MODERATE* Program Designation.

TABLE 1



	WORLDWIDE	GOVERNMENTWIDE	MULTIAGENCY	AGENCY
MAJOR: Impacts directly on the survival, stability, and continued integrity and effectiveness of government operations, the promotion of major government fiscal goals, or a primary social, political, or economic interest of the nation.	***MAJOR***	***MAJOR***	***SUBSTANTIAL***	***MODERATE***
SUBSTANTIAL: Impacts directly on the integrity and efficiency and effectiveness of a sizeable segment of the Federal workforce, or the interests of large numbers of individuals in the private sector.	***MAJOR***	***SUBSTANTIAL***	***SUBSTANTIAL***	***MODERATE***
MODERATE: Impacts directly on the integrity and effectiveness of an agency's operations, the fiscal interests of an agency, or affects the social, political or economic interests of individuals, businesses or organizations in the private sector.	***SUBSTANTIAL***	***MODERATE***	***MODERATE***	***LIMITED***
LIMITED: Limited impact on the operational integrity and effectiveness of one or a few programs in an agency, or the interests of a limited number of individuals in the private sector.	***MODERATE***	***MODERATE***	***LIMITED***	***LIMITED***

Designating Position Risk Points

- ***Position Risk Designation Points.*** The agency determines the degree of risk that a position poses to the agency or an agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total "position risk points" for a position.

Use these steps and Table 2 on the next page to complete part II –"Position Risk Designation Points"

1) **Risk Factors and Degree of Risk:** Using a position description, or any documented information describing the duties and responsibilities of a position, evaluate each RISK FACTOR described at the top of Table 2 in terms of the DEGREE OF RISK described in the first column.

2) **Risk Factors and Points:** Assign points (*7-6-5-4-3-2-1*) to each risk factor to numerically reflect the DEGREE OF RISK. (The greater the degree of risk, the higher the point value assigned to the risk factor.)

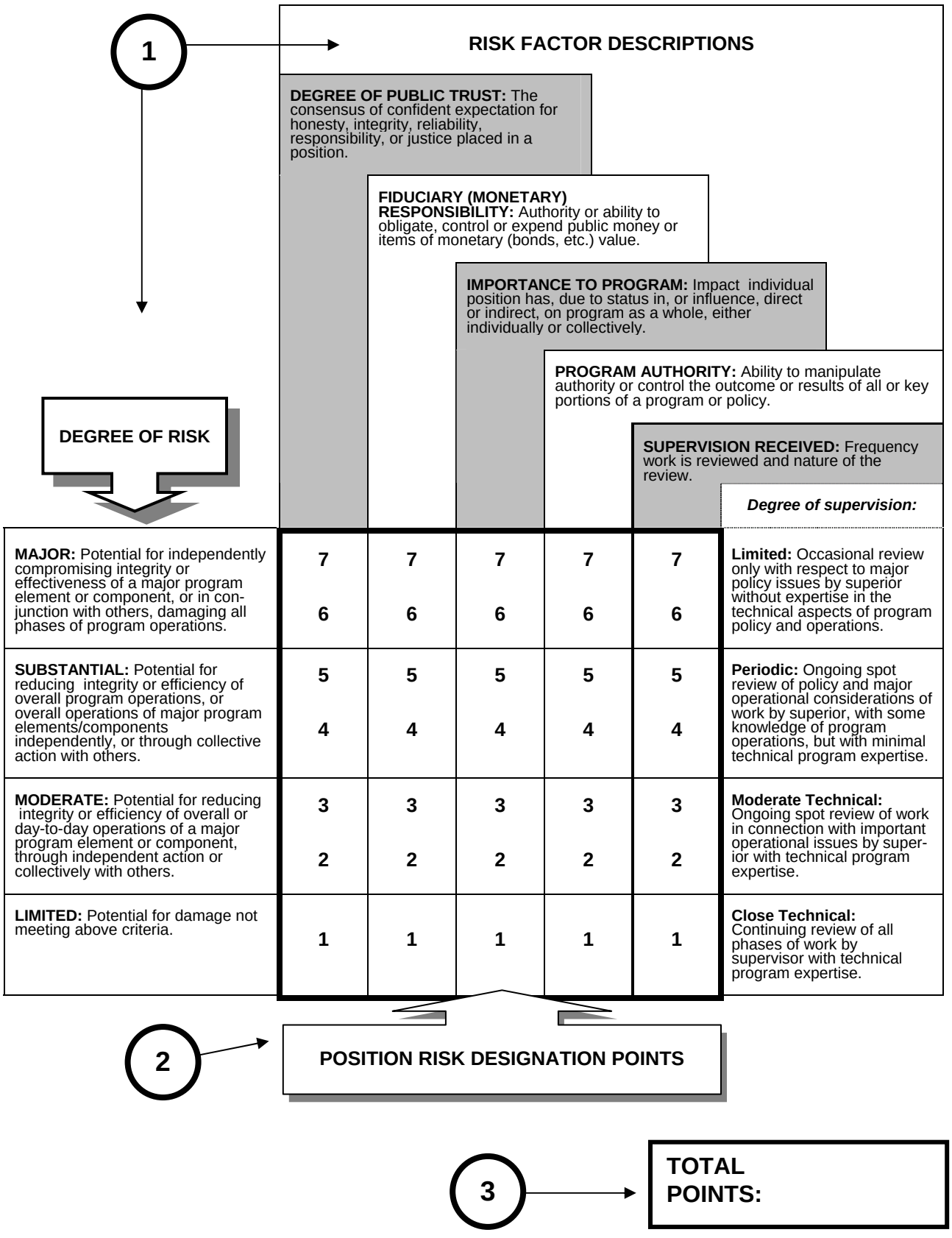
3) **Total Points:** After points are assigned to all five risk factors, total the points. The result is a numerical representation of the relative degree of risk a position poses to the agency or an agency program (as related to the integrity and efficiency of the service).

Example:

SUBSTANTIAL "Degree of Public Trust" = ② 5 points
SUBSTANTIAL "Fiduciary (Monetary) Responsibility" = ② 4 points
LIMITED "Importance to Program" = ② 1 point
MODERATE "Program Authority" = ② 2 points
MODERATE "Supervision Received" = ② 3 points

The total Position Risk Designation Points (5+4+1+2+3) = ③ **15**

TABLE 2



Position Designation

- ***Position Designation.*** The Program Designation and Position Risk designation Points are applied to determine the risk level "position designation."

  At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation will result in a higher risk level, the other steps may not be needed.

The results of part I, Program designation, and part II, Position Risk Designation Points, are next applied to Table 3 to determine the risk level of the position and to pair the risk level with the recommended minimum level of investigation for the position. The investigation recommendations are not intended to restrict an agency from conducting a more comprehensive investigation than that prescribed, when such investigation is considered warranted.

TABLE 3

II. POSITION RISK POINTS

I. PROGRAM DESIGNATION	**5-10**	**11-17**	**18-23**	**24-29**	**30-33**	**34-35**
MAJOR	**Low Risk (LR) NACI**	**Moderate Risk (MR) LBI**	**Moderate Risk (MR) LBI**	**High Risk (HR) BI**	**High Risk (HR) BI**	**High Risk (HR) BI**
SUBSTANTIAL	**Low Risk (LR) NACI**	**Moderate Risk (MR) LBI**	**Moderate Risk (MR) LBI**	**Moderate Risk (MR) LBI**	**High Risk (HR) BI**	**High Risk (HR) BI**
MODERATE	**Low Risk (LR) NACI**	**Low Risk (LR) NACI**	**Moderate Risk (MR) MBI**	**Moderate Risk (MR) MBI**	**Moderate Risk (MR) LBI**	**High Risk (HR) BI**
LIMITED	**Low Risk (LR) NACI**	**Low Risk (LR) NACI**	**Low Risk (LR) NACI**	**Low Risk (LR) NACI**	**Moderate Risk (MR) LBI**	**High Risk (HR) BI**

POSITION **RISK LEVEL** AND TYPE OF BACKGROUND **INVESTIGATION**

Minimum Investigative Requirements. The following are the **required** minimum levels:

LOW RISK - **NACI**
MODERATE RISK - **MBI**
HIGH RISK - **BI**

However, OPM recommends the levels shown in Table 3, above.

Adjustments: Some positions, by the very nature of the duties and responsibilities of the program or the position, will require designation at a certain level of risk. Final adjustment in the designation process must take into account *unique* factors specific to positions, and the organizational need for *uniformity* of operations. Adjustments serve to raise the risk level designation of a position or convert the designation from a risk level to a sensitivity level. As a consequence, the level of investigation is often raised.
Uniqueness. Some factors that can cause a uniqueness adjustment, that are unique and are not fully accounted for in the program or position designation system, are listed here:

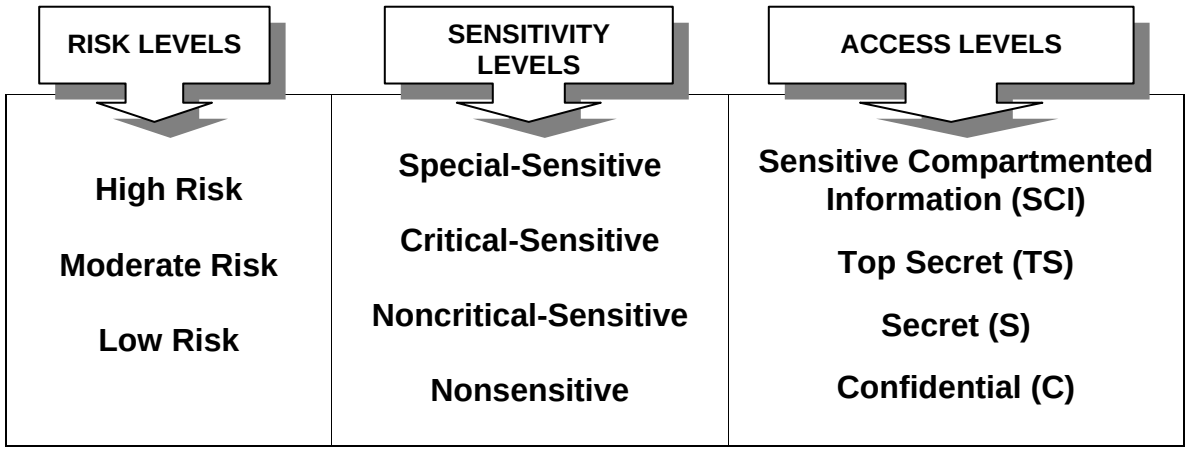
- Special investigative
- Positions requiring p

- Significant public health duties.
- Significant public safety duties.
- Access to or control of highly sensitive but unclassified information.
- Access to sensitive financial records.
- Potential for realizing significant personal gain.
- Control of an automated monetary system (such as key access entry).
- Few-of-a-kind positions with special duties (such as Special Assistant to Agency Head).
- Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans but involving regular contact with, and ongoing knowledge of, all or most of such material (such as Budget Analyst, Special Assistant).
- Any of the criteria appearing in 5 CFR 732 or E.O. 12968.
- Computer-ADP; any of the criteria under OMB Circular A-130 or the Computer Security Act of 1987.
- Any other factors the agency thinks relevant (these must be documented).

Uniformity. There may be a clearly indicated need for uniformity in position designations, because of authority level or program designation level; two examples that can cause adjustment are listed here:

- Agency head may adjust position designations at the same authority level to assure uniformity within the agency (for example, managers of major agency programs at the same level of authority may be designated at the same level of risk).
- If agency heads determine the designation levels of programs override and negate any specific risk considerations associated with individual positions within an agency or program, they may designate all positions within a program at the risk level required to protect the integrity and best promote the efficiency of the service.

Only after analysis of the position in terms of *uniqueness* and *uniformity* should any adjustment decision be made for FINAL DESIGNATION. FINAL DESIGNATION could be any one of the following:



See Adjustment examples on the next page.

EXAMPLES:

I. PROGRAM DESIGNATION	II. POSITION RISK DESIGNATION POINTS	III. POSITION DESIGNATION	MINIMUM INVESTIGATION	ADJUSTMENTS Uniqueness, Uniformity	FINAL DESIGNATION	REQUIRED INVESTIGATION

MODERATE	20	MR	MBI	Criminal Justice Duties	**HR**	**BI**
SUBSTANTIAL	29	MR	LBI	None	**MR**	**LBI**
MAJOR	25	HR	BI	TS Access (E.O. 12968)	**CS**	**SSBI**
MODERATE	30	MR	LBI	Special Assistant to Agency Head	**HR**	**BI**
MAJOR	25	HR	BI	5 CFR 732 (No Access)	**CS**	**BI**

B. COMPUTER/ADP POSITION RISK LEVELS

The Computer/ADP position risk levels are an integral part of the Risk Designation System. Determining a Computer/ADP position risk level is an adjustment factor for both uniqueness and uniformity and tends to raise the risk level designation. The three Computer/ADP position risk levels are described in the following table; in determining position designation for any position with Computer/ADP duties, apply these definition considerations:

COMPUTER/ADP RISK LEVELS	RISK LEVEL DEFINITIONS
High Risk (HR) Public Trust Position	Potential for **exceptionally serious impact** involving duties especially critical to the agency mission, with broad scope and authority, with major program responsibilities, which affect a major Computer/ADP system.
Moderate Risk (MR) Public Trust Position	Potential for **moderate to serious impact** involving duties of considerable importance to the agency mission, with significant program responsibilities that affect large portions of a Computer/ADP system.
Low Risk (LR)	Potential for impact involving duties of **limited relation** to the agency mission through the use of Computer/ADP systems.

Risk Levels.

High Risk: Includes any position at the highest level of risk to the Computer/ADP system. Such positions may involve:

- Responsibility for the development, direction, implementation, and administration of agency computer security programs, including direction and control of risk analysis or threat

assessment.

- Significant involvement in life-critical or mission-critical systems.
- Responsibility for preparing or approving data for input into a system which does not necessarily involve personal access to the system, but which creates a high risk for effecting grave damage or realizing significant personal gain.
- Assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from 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 system.
- Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of systems hardware and software.
- Access to a system during the operation or maintenance in such a way to permit high risk for causing grave damage or realizing a significant personal gain.
- Other positions as designated by the agency head that involve high risk for 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 High Risk level to insure the integrity of the system. Such positions may involve responsibility for systems design, operation, testing, maintenance, or monitoring that is carried out under technical review of higher authority at the High Risk level, to insure the integrity of the system. This level includes, but is not limited to:

1. Access to or processing of proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts.
2. Accounting, disbursement, or authorization for disbursement from systems with amounts less than $10 million per year.
3. Other positions designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in High Risk positions.

Low Risk: Includes all Computer/ADP positions not falling into one of the above risk levels.

In order to establish uniformity and objectivity, agencies must make Computer/ADP risk designations in a systematic manner. Since positions can involve determinations of risk level for both suitability and Computer/ADP, the higher of the two risk levels is used for final position designation.

C. NATIONAL SECURITY POSITI .S

All positions with National Security duties and responsibilities must have a sensitivity level designation to assure the appropriate level of investigative screening is done to comply with E.O. 10450 and E.O. 12968. Under 5 CFR Part 732, a sensitive position is defined as "…*any position within a department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the National Security.*" Consequently, sensitivity level designation is based on an assessment of the degree of damage that an individual could cause to the National Security. There are three sensitivity levels: Special-Sensitive, Critical-Sensitive, and Noncritical-Sensitive, defined in the

table that follows:

SPECIAL-SENSITIVE (SS)

Any position an agency head determines to be at **a higher level than Critical-Sensitive** due to special requirements that complement E.O. 10450 and E.O. 12968 (such as Director of Central Intelligence Directive [DCID] 6/4 that sets investigative requirements and access to Sensitive Compartmented Information [SCI] and other intelligence-related Special Sensitive information).

CRITICAL-SENSITIVE (CS)

Potential for exceptional or grave damage to the national security.

Positions that involve any of the following:

- Access to **TOP SECRET** classified information;
- Development or approval of war plans, or plans or particulars of future, major, or special operations of war, or critical and extremely important items of war;
- National security policy-making or policy-determining positions;
- Investigative duties;
- Issuance of personnel security clearances;
- Duty on personnel security boards; and
- Any other positions related to national security requiring the same degree of trust.

NONCRITICAL-SENSITIVE (NCS)

Potential for significant or serious damage to the national security.
Positions that involve any of the following:

- Access to **SECRET** or **CONFIDENTIAL** classified information, or
- Duties that may directly or indirectly adversely affect the national security operations of the agency or the government.

*NOTE: The designation of **Non-Sensitive** is not shown in the table because a Non-Sensitive position is the same as a Low Risk position; both require the same level of investigation, a NACI.*
Apply the sensitivity levels described in this part as an **Adjustment** in the Risk Designation System to arrive at a final designation. This Appendix references 5 CFR 732 as one of the *uniqueness* adjustment factors. The reference pertains to Subpart B, of the section on "Sensitivity level designations and investigative requirements." The ta[illegible]sitivity level designations as well as their definitions and examples of the types of duties and responsibilities that correspond to the Critical-Sensitive and Noncritical-Sensitive levels. An agency should consider the information displayed in this table when deciding if a position should have a sensitivity designation.

Sensitivity level designations override Public Trust (i.e., HR and MR) designations due to the national interest or security. However, the basic risk level of a position needs to be determined first. If National Security duties and responsibilities are no longer a part of a position, the position then reverts to its Public Trust designation. Additionally, if the Public Trust risk level designation requires a higher level of

investigation than the National Security sensitivity level, the higher level of investigation should be conducted. For example, if the basic position designation is HR, but the position requires Secret access, the position would have an adjusted designation of Noncritical-Sensitive because of the Secret access. The investigation required would be a BI for the HR position, and not an ANACI for the Noncritical-Sensitive designation due to Secret access. The higher level of investigation prevails because of the more intensive screening required of an HR position, a BI investigation being a higher level of investigation than an ANACI.

5 EXAMPLES:

POSITION DESIGNATION	*MINIMUM INVESTIGATION*	FINAL DESIGNATION	ADJUSTED INVESTIGATION	REQUIRED INVESTIGATION
EXAMPLE 1: **HR**	*BI*	NCS/Secret	ANACI	**BI**
EXAMPLE 2: **LR**	*NACI*	CS/Top Secret	SSBI	**SSBI**
EXAMPLE 3: **MR**	*MBI*	NCS/No Access	NONE	**MBI**
EXAMPLE 4: **HR**	*BI*	SS/SCI	SSBI	**SSBI**
EXAMPLE 5: **LR**	*NACI*	NCS/Confidential	ANACI	**ANACI**