

POSITION RISK AND SENSITIVITY LEVEL DESIGNATION

1. Program and Position Risk/Sensitivity Designation. The procedures in this appendix provide a systematic and uniform method for designating program and position risk or sensitivity levels. The risk level designation is the description of the degree of potential adverse impact that a position may have on the Department. The position risk level designation process involves the three steps of designating the program risk level, designating the position's risk points, and designating the position's type of background investigation. The national security sensitivity level designations are contained in 5 C.F.R. Part 732.

2. Designation of Program Risk Level - Table 1

a. With the use of the attached Table 1, the first step is to designate the program's risk level. Program risk level designation is dependent upon a program's Impact on the Department's operations. The Impact (Major, Substantial, Moderate, or Limited) equates to the degree that a program affects VA's Scope of Operations (Worldwide, Government-wide, Multi-agency, or Agency). If the "Scope of Operations" has more than one area of primary focus (Worldwide, Multi-Agency, etc.), or if questions arise concerning the appropriate program Impact description (Major, Moderate, etc.), then designating the program's risk level should always be based on the Department's best interests.

b. Program risk level is determined by identifying both the type of Impact (column 1) that a program has and its applicable and appropriate Scope of Operations (columns 2 - 5). Intersecting column 1 and columns 2 through 5 derives the program's risk level.

EXAMPLE 1: If a program's "Impact" = "Substantial" and its "Scope of Operations" = "Multi-Agency," then the appropriate program risk level designation = "Substantial"

EXAMPLE 2. If a program's "Impact" = "Substantial" and its "Scope of Operations" = "Worldwide," then the appropriate program risk level designation = "Major"

3. Designation of Position Risk Points - Table 2

a. With the use of the attached Table 2, the second step is to designate the position's risk points. The program risk levels are Major, Substantial, Moderate, and Limited. These risk levels are then evaluated in five factors or description areas which are the degree of Public Trust, Fiduciary (Monetary) Responsibility, Importance to Program, Program Authority, and Supervision Received.

b. To determine a position's risk points, the duties and responsibilities of the position must be considered in the context of the program's operations and the risk level that the position has for adversely affecting the Department.

c. Points are assigned under each of the five risk factors, to numerically reflect the degree of risk. The greater the risk, the more points are to be assigned. After points are assigned for all five risk factors, the sum is used to arrive at the position's total risk points.

EXAMPLE: Substantial Degree of Public Trust (5 points) + Substantial (Monetary) Fiduciary Responsibility (5 points) + Limited Importance to Program (1 point) + Limited Program Authority (1 point) + and Moderate Supervision (3 points) = 15 total position risk points (5+5+1+1+3=15).

4. Designation of Risk Level and Type of Background Investigation -Table 3. The results of Tables 1 and 2 are next applied to Table 3, Position Risk Level and Type of Background Investigation, to determine the appropriate type of background investigation required for each position's final designated risk level.

EXAMPLE 1: If "Program Designation" (column 1) = "Moderate" + "Position Risk Points" (column 2-7) = 22 points, then the appropriate background investigation = (MBI) for the Moderate Risk Level (found in column 4).

EXAMPLE 2: If "Program Designation" (column 1) = "Major" + "Position Risk Points" (column 2-7) = 9 points, then the appropriate background investigation = (NACI) for the Low Risk Level (found in column 2).

5. Adjustments. Some positions, by the very nature of the duties and responsibilities, will require designations at certain risk levels. Final adjustments in the risk level designation process must take into account unique factors specific to positions and program operations.

a. Unique Factors. Factors that may be considered unique include:

(1) Special investigative or criminal justice duties;

(2) Control of an automated monetary system such as key access entry;

(3) Employees who are required to complete financial disclosure forms should be minimally designated at moderate risk.

(4) Unique positions with special duties such as those of a Special Assistant to an Agency Head;

(5) Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans, but involving regular contact with an ongoing knowledge of, all or most of, such material;

(6) Any of the criteria appearing in 5 C.F.R. §732.102; and

(7) Any other factors that a manager considers relevant.

b. Uniformity. For the purpose of uniformity the risk points should be assessed at point values 1, 3, 5, and 7, as shown in Table 2. However, in some cases adjustments may result in point values of 2, 4, and 6. Adjustments will be used to upgrade risk point designation when unique factors arise in special cases. Only after careful analysis of the position in terms of unique factors and the need for uniformity should any decision on adjustment be made. Final position risk levels will be one of High Risk (HR), Moderate Risk (MR), or Low Risk (LR).

6. Position Designation Records. Human Resources Management (HRM) will maintain a record of position risk and sensitivity designations through the use of VA Form 2280, Position Sensitivity Level Designation. This form will be stored on the temporary side of the Official Personnel Folder (OPF) or, for Title 38 employees with personnel folders, on the temporary side of the Merged Records Personnel Folder (MRPF). VA Form 2280 is subject to review by OPM during periodic program appraisals or on a case-by-case basis, as required, to ensure that positions are properly designated. VA Form 2280 can be obtained through the department's intranet at the following address <http://vaww.va.gov/vaforms> and is available in Acrobat Adobe format for print and fill, or in JefForm filler for those who have JefForm software loaded on their workstations.

7. Position Risk Levels and Suitability Determinations. Appointee or employee suitability is determined commensurate with the position's designated risk level. Risk levels are designated in accordance with the degree of potential adverse impact on a program or VA as a whole. The degrees of potential adverse impact inherent to each risk level designation are as follows:

a. High Risk positions have the potential for serious adverse impact and involve duties that are critical to VA or a program mission with broad scope, policy, and program authority such as policy development and implementation; higher level management assignments; independent spokespersons; or non-management positions with authority for independent action.

b. Moderate Risk positions have potential for moderate to serious impact involving duties of considerable importance to VA or a program mission with significant program responsibilities and delivery of customer services to the public such as an assistant for 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 and trust.

c. Low Risk positions are positions with limited potential for adverse impact involving limited scope of duties without independent or semi-independent action or decision-making.

8. Position Risk Level Designations for Computer/Information Technology (IT)

Positions. The following levels are to be used as an integral part of the suitability position risk designation system described above. For each computer/IT position, the letter "C" will precede the sensitivity designation. There are three position risk levels as follows:

a. High Risk computer/IT positions have the potential for serious adverse impact involving duties critical to VA with broad scope and authority, and with major program responsibilities which affect major IT systems. These positions involve:

(1) Responsibility for the development and administration of a computer security program and include the direction and control of risk analysis and/or threat assessment.

(2) Significant involvement in life-critical or mission-critical systems.

(3) Responsibility for the preparation or approval of data for input to a system which, while not involving personal access to the system, does involve rather high risk for grave damage or realization of significant personal gain.

(4) Assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement of dollar amounts of \$10 million per year or greater or lesser amounts if the activities of the individuals are not subject to technical review by higher authority.

(5) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

(6) Other positions as designated by the agency head that involve high risk for causing grave damage or realizing significant personal gain.

b. Moderate Risk computer/IT positions have the potential for moderate to serious adverse impact involving duties of considerable importance to the Department with significant program responsibilities, which affect large portions of IT systems. These positions involve:

(1) Responsibility for system design, operation, testing, maintenance, and/or monitoring that is carried out under technical review or higher authority at the High Risk level to ensure the integrity of the system.

(2) Assignments of access to and/or processing of proprietary data that are protected by the Privacy Act, and accounting, disbursement, or authorization for disbursement from systems of dollar amounts of less than \$10 million per year.

(3) Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential threat for damage or personal gain to a lesser degree than that of the High Risk position.

c. Low Risk computer/IT positions have the limited potential for adverse impact and involve duties of limited relation to the Department's mission through the use of IT systems. These positions do not entail the same degree of threat as that of the High or Moderate Risk positions.

9. Position Sensitivity Levels and Security Eligibility Determinations. In addition to the position risk levels (suitability levels) listed in paragraph 7 of this appendix, all positions must be evaluated to determine if they possess national security considerations, as well. The three national security position sensitivity levels are listed below. Generally, in order to determine if a position possesses national security considerations and therefore merits a Special Sensitive, Critical Sensitive, or Noncritical Sensitive Determination, VA will determine whether the position will require access to Classified Information, as described in the definitions below. Positions that have access to Classified Information, the misuse of which may adversely affect not only the Department but national security as well, will be given one of these sensitive levels. Please note that the designation of one of these levels, does not replace the position risk levels, but are instead in addition to those levels. Positions that do not have these sensitivities are designated as Nonsensitive.

a. Special Sensitive (SS). These positions entail access to intelligence-related information of Sensitive Compartmentalized Information, information classified above the Top Secret level, the misuse of which may gravely affect the overall VA operations and national security.

b. Critical Sensitive (CS). These positions entail access to Top Secret information; investigative duties, the issuance of personnel security clearances or duty on personnel security boards; or other positions related to national security, and may adversely affect the overall operations of VA and national security.

c. Noncritical Sensitive (NCS). These positions entail access to Secret or Confidential information and may adversely affect the overall operations of VA.

10. Background Investigative Requirements. Listed below are the risk level and sensitivity level designations for Department positions with the corresponding types of background investigations. Note that the position risk and sensitivity levels are listed in ascending order to illustrate the increasing scope of the required background investigation levels.

a. **Low Risk and Nonsensitive Positions** require a National Agency Check with Written Inquiries (NACI). A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. A National Agency Check with Law Enforcement and Credit Check (NACLCL) investigation, used for non-citizen contract personnel in Low Risk/Nonsensitive positions, covers a period of 5 years and consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check], a credit report covering a period of 5 years, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Nonsensitive or Low Risk positions, some contract employees and the periodic reinvestigations for VA police officers.

b. Public Trust Positions

(1) A Moderate Risk position requires a Minimum Background Investigation (MBI). An MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

(2) A High Risk position requires a Background Investigation (BI). A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

c. National Security Positions

(1) **Noncritical Sensitive Positions** require a Limited Background Investigation (LBI). An LBI is conducted by OPM and covers a 3-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 3 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

(2) **Special Sensitive and Critical Sensitive Positions** require a Single Scope Background Investigation (SSBI). An SSBI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; a verification of educational degree; a spouse/cohabitant NAC excluding an FBI fingerprint check; and verification of citizenship or legal status for foreign-born immediate family members.

11. Adjusted Position Designations and Investigation Levels

a. In rare instances, an individual holding a Public Trust position may be required to access national security information. In such a case, the position may include a permanent or temporary adjusted sensitivity designation that requires an adjusted background investigation at the higher level. If National Security duties and responsibilities are no longer a part of a position, the position then reverts to its Public Trust designation. The SIC will be notified within five calendar days of such adjusted position designations and investigations as it handles all activities and processing for these adjustments.

b. In adjusting a position's designation, the basic risk level of the position needs to be determined first. 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 access to Secret documents, 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 LBI for the Noncritical Sensitive designation. The higher level of investigation prevails because of the more intensive screening required of an HR position. A BI investigation is a higher level of investigation than an LBI.

c. Examples of adjusted position designations and investigation levels are listed from left to right .

Position's Original Designation	Required Minimum Investigation	Adjusted Final Position Designation	Adjusted Investigation Level	Required Level Investigation for Adjusted Position Designation
High Risk	Background Investigation (BI)	Noncritical Sensitive (NCS/Secret)	Limited Background Investigation (LBI)	Background Investigation (BI)
Moderate Risk	Minimum Background Investigation (MBI)	NCS/Secret	LBI	MBI
Low Risk	National Agency Check with Written Inquiries (NACI)	Critical Sensitive CS/Top Secret	Single Scope Background Investigation (SSBI)	SSBI
High Risk	BI	Special Sensitive/Sensitive Compartmentalized Information (SS/SCI)	SSBI	SSBI