Mandatory Reference: **N/A**
Supplementary Reference: **566**
File Name: **adscd15/566e51s1**

PUBLIC TRUST DESIGNATIONS

The designations of positions indicat**e** the potential for action or inaction by the incumbent of the position to affect the integrity, efficiency, and effectiveness of Government operations. Public trust risk designations are used in conjunction with security clearance requirements to determine the investigative requirements for the position. Positions involving high degrees of public trust, e.g., those with broad policy making authority or fiduciary responsibilities, trigger a more thorough investigation than do positions requiring only the finding that an applicant or an incumbent has the requisite stability of character to hold Federal employment. The three public trust risk designation levels are high, moderate, and low.

a. HIGH RISK: A position that has potential for exceptionally serious impact involving duties especially critical to the **A**gency or a program mission of the **A**gency with broad scope of policy or program authority such as:

(1) **P**olicy development and implementation;

(2) **H**igher level management assignments;

(3) **I**ndependent spokespersons or non-management positions with authority for independent action;

(4) **S**ignificant involvement in life-critical or mission critical systems; or

(5) **R**elatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization of disbursement from systems of dollar 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 ensure the integrity of the system.

(6) **P**ositions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction and control of risk analysis and/or threat assessment, planning, and design of the computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with the relatively high risk for causing grave damage or realize a significant personal gain;

b. MODERATE RISK: A position that has the potential for moderate to serious impact involving duties of considerable importance to the **A**gency or a program mission of the **A**gency with significant program responsibilities and delivery of

customer services to the public such as:

(1) **A**ssistants to policy development and implementation;

(2) **M**id-level management assignments;

(3) **N**on-management positions with authority for independent or semi-independent action;

(4) **D**elivery of service positions that demand public confidence or trust; or

(5) **P**ositions with responsibility 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 ensure the integrity of the system. Such positions may include but are not limited to:

(a) **A**ccess to and/or processing of proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

(b) **A**ccounting, disbursement, or authorization for disbursement from systems of dollar amounts of less than $10 million per year; or

(c) **O**ther positions as designated by the **A**gency head that involve degree of access to a system that creates a significant potential for damage or personal gain less than that in high risk positions.

c. LOW RISK: Positions that have the potential for impact involving duties of limited relation to the **A**gency mission with program responsibilities which affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a high or moderate risk position.