



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.3

Effective Date: May 31, 2012

Expiration Date: May 31,
2017

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Personnel Security (Change 2, April 29, 2013)

Responsible Office: Office of Protective Services

[| TOC](#) | [| Preface](#) | [| Chapter1](#) | [| Chapter2](#) | [| Chapter3](#) | [| AppendixA](#) | [| AppendixB](#) | [| AppendixC](#) | [| ALL](#) |

Chapter 2. NASA Personnel Security Investigations

2.1 General

2.1.1 Individuals who perform work for or on behalf of the Agency are subject to a PSI to determine whether they are:

- a. Suitable for Government employment;
- b. Eligible for logical and physical access;
- c. Eligible for access to classified information;
- d. Eligible to hold a sensitive position;
- e. Fit to perform work for or on behalf of the Government as a contractor employee.

2.1.2 A determination of both b. and e. applies to all NASA contractors.

2.1.3 An appointment will not be subject to investigation when the person being appointed has undergone a previous PSI and the appointment involves:

- a. Appointment or conversion to an appointment in a covered position if the person has been serving the agency for at least one year in a covered position subject to investigation.
- b. Transfer to a covered position, provided the person has been serving continuously for at least one year in a covered position subject to investigation.
- c. Transfer or appointment from an excepted service position that is not covered to a covered position, provided the person has been serving continuously for at least one year where the person has been determined fit for appointment.
- d. Appointment to covered position from a position as an employee working as a Federal Government contract employee provided the person has been serving continuously for at least one year in a job where the Federal agency determined that the contract employee was fit to perform work on the contract.
- e. Appointment to a covered position where there has been a break in service of less than 24 months, and the service immediately preceding the break was in a covered position, an excepted service position, or a contract employee position described in paragraphs (a) to (d) of this section.

2.1.4 NASA determines the fitness of contractor employees to perform work as a contractor. Prior favorable fitness, suitability, and national security determinations should be reciprocally accepted. There is no requirement that the prior favorable fitness, suitability, or national security determination be made within a specific time period. However, for contractor employees there should be no break in employment since a favorable determination was made.

2.1.4.1 Contractor employee means an individual who performs work for or on behalf of NASA under a contract and who, in order to perform the work specified under the contract, requires access to space, information, information

technology systems, staff, or other assets of NASA. Such contracts include, but are not limited to:

- a. Contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the Agency;
- b. Sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contracts with the Agency excepted service to the extent they are not otherwise subject to OPM appointing authorities.

2.1.4.2 Non-NASA employees performing work through Cooperative Agreements, Space Act Agreements, Grants, Enhanced Use Lease Agreements, and Funding Orders shall be adjudicated for security access as a contractor consistent with Draft NPR 1600.6, Identity and Credentialing Management.

2.1.4.3 Intergovernmental Personnel Act (IPA) employees may be identified as a civil service employee on the PIV badge. However, the IPA employee would be adjudicated for security access as a contractor.

2.1.5 An appointment to a covered position will also be subject to investigation when:

- a. The covered position requires a higher level of investigation than previously conducted for the person being appointed; or
- b. The Agency obtains new information in connection with the person's appointment that calls into question the person's suitability.

2.1.6 Federal employees from other Federal Government agencies and members of the U.S. military who are detailed to NASA or who are members of a tenant Federal Government organization are assumed to have been properly adjudicated for employment suitability or fitness to perform work on a Government contract by their respective agency. The CCS/CCPS shall coordinate with the Center OHCM personnel to validate investigative and suitability results for detailees. Upon validation, no further investigation is required unless specifically required by policy or for cause. All subsequent issues associated with personnel identified in this paragraph will be coordinated with the Center OHCM specialists or respective detailee's official agency personnel office for resolution.

2.1.7 Investigations that meet the requirements for a specified position shall be reciprocally accepted for that and lower investigations with no additional investigation provided there is no break in employment, derogatory or questionable information, or need based on change of position with a higher investigation requirement.

2.2 Public Trust Positions

2.2.1 Positions designated at the moderate-risk or high-risk level are referred to as "public trust" positions. Such positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust and involving access to or operation or control of financial or personnel records, with a significant risk for causing damage or realizing personal gain. Public trust positions are subject to periodic reinvestigation.

2.3 Designation of Risk and Sensitivity Levels

2.3.1 Position risk designations and sensitivity levels for civil service employees are made by Center OHCM in coordination with the supervisor and Center Office of Protective Services. This section refers only to non-covered positions.

2.3.2 Position risk and sensitivity level designations for contracts, grants, cooperative agreements, and MOAs or MOUs shall be made by the responsible NASA Center program office representative typically by the designated civil service project manager (sponsor), COTR, in coordination with the CCS/CCPS, and IT Security Manager(s).

2.3.3 The position risk and sensitivity level is determined by evaluating the sensitivity and risk of the work being performed, the access required by the contractor employee, and the potential for damage to NASA's mission and operations if performed inefficiently, ineffectively, or in an unsafe or unethical manner. Included is the requirement to properly identify and assign risk level designations for those individual positions directly involved in IT systems and/or application software development commensurate with the risk and the sensitivity level that will ultimately be applied to the system and or application when deployed.

2.3.4 All access factors (i.e., Center, facility, information, and IT systems) will be considered concurrently as part of the overall risk designation process. This procedure serves to avoid duplication of effort by eliminating the possibility that a single individual could be assessed numerous times for different accesses. The intended result will be that the highest level of risk designation is the designation for which the appropriate investigation will be conducted (IT = high-risk designated position compared against that same individual's need to access uncontrolled areas of the Center = low-risk) .

2.3.5 The risk and sensitivity level for each position shall be identified and designated in the statement of work of the contract. This position designation determines the investigative requirements for the contractor employees that

perform the work.

2.3.6 Fitness determinations will be made for contractor employees upon consideration of contractual requirements.

2.3.7 If an employee's duties require any overlap into a higher or lower risk level, the position risk will then be set at the highest risk level anticipated.

2.3.7.1 The COTR in consultation with the contracting officer is required to identify the employees to be processed at each risk level designation and will specify the duties of the contractors. In instances where there is a wide variance in the security risk level of the work to be performed, individual contractor employees will be processed at the risk designation commensurate with the highest risk level of their duties.

2.3.7.2 The entire contract, grant, MOA, or MOU may be designated high or moderate risk, but those NASA contractor employees whose work would be moderate or low risk will be investigated accordingly. In meeting this contingency, the contract, grant, MOA, or MOU will specifically apply controls to ensure that work of the lower risk positions does not overlap with that for the higher risk positions.

2.4 High-Risk Public Trust Positions

2.4.1 High-risk positions are those that have the potential for exceptionally serious impact involving duties especially critical to the Agency or a program mission of the Agency with a broad scope of policy or program authority.

2.5 Moderate-Risk Public Trust Positions

2.5.1 Moderate-risk positions are those that have the potential for moderate-to-serious impact involving duties of considerable importance to the Agency or a program mission of the Agency with significant program responsibilities and delivery of customer services to the public.

2.6 Low-Risk Positions

2.6.1 Low-risk positions are those that have the potential for limited impact involving duties of minimal relation to the Agency mission with program responsibilities that affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a high-risk or moderate-risk position. Positions designated at the low-risk level are not considered public trust positions.

2.6.2 Positions that do not fall in the categories high-risk or moderate-risk include all non-sensitive positions and all other positions involving IT Systems whose misuse has limited potential for adverse impact or sensitive data is protected with password and encryption. Low-risk IT positions may involve general word processing or systems containing no IT-1 or IT-2 level information.

2.6.3 The contractor program manager and COTR will identify and specify control measures to be used to ensure that there is no overlap of work duties between the lower designated positions.

2.6.4 Non-U.S. citizens, including Lawful Permanent Residents, are eligible for placement in low-risk and moderate-risk positions, but are not normally eligible for employment in positions designated as high-risk. Under specific situations the AA, OPS may authorize the placement of a non-U.S. citizen for a specific high-risk position when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization should submit a written request to the AA, OPS, via the CCS/CCPS. The request should contain the following:

- a. Specify why it is impractical or unreasonable to use U.S. citizens to perform the required work or function.
- b. Define the individual's special expertise.
- c. Define the compelling reasons for the request.

2.6.5 The CCS/CCPS will review the request for accuracy, endorse or non-endorse it, and forward it to the AA, OPS.

2.6.6 The AA, OPS, will coordinate with OIIR for concurrence, and if approved, promptly return the request to the requestor. A copy will be retained in OPS and Center security office files.

2.7 Child Care Providers

2.7.1 Child Care National Agency Check and Inquiries (CNACI) are to be completed on all child care providers prior to their working in NASA-sponsored child care facilities. Centers shall use the services of OPM to conduct these investigations.

2.7.2 Upon return of favorable OPM fingerprint results and severe operational need, personnel shall work under

regular and continuous observation by a favorably adjudicated employee, pending completion of the CNACI on the observed individual.

2.7.3 NASA child care centers shall coordinate all personnel hiring actions with the Center security office prior to entry on duty.

2.8 Lautenberg Amendment

2.8.1 Federal and contractor employees in positions that require the carrying of a firearm are affected by the Lautenberg Amendment to the Gun Control Act of 1968, effective September 30, 1996. The amendment makes it a felony for those convicted of misdemeanor crimes of domestic violence to ship, transport, possess, or receive firearms or ammunition. The amendment also makes it a felony to transfer a firearm or ammunition to an individual known or reasonably believed to have a conviction.

2.9 Personnel Security Investigations Requested by NASA

2.9.1 NASA will comply with OPM standards for requesting PSIs. Security offices will use the following chart to select the appropriate investigation:

For this Position Designation:	You will use this request format:	To request this investigation:
Risk/Sensitivity Level	Standard Form	FY 2012 OPM Investigative Product Codes
Low Risk/HSPD-12 Credential Non-Sensitive Position	SF 85 (Questionnaire for Non Sensitive Positions)	National Agency Check and Inquiries (NACI) (02B)
Moderate Risk Public Trust Position No national security sensitivity	SF 85P (Questionnaire for Public Trust Positions)	Moderate Risk Background Investigation (MBI) (15)
High Risk Public Trust Position No national security sensitivity	SF 85P (Questionnaire for Public Trust Positions)	Background Investigation (BI) (25)
Secret/Confidential (Undesignated –e.g. Military/Contractor)	SF 86 (Questionnaire for National Security Positions)	National Agency Check with Law and Credit (NACLIC) (08B)
Low Risk Noncritical Sensitive Position and/or Secret/Confidential Security Clearance	SF 86 (Questionnaire for National Security Positions)	Access National Agency Check and Inquiries (ANACI) (09B)
Moderate Risk Noncritical Sensitive Position and/or Secret/Confidential Security Clearance	SF 86 (Questionnaire for National Security Positions)	Moderate Risk Background Investigation (MBI) (15)
Any level of risk Critical Sensitive Position and/or Top Secret (TS) Security Clearance	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI) (30)
Any level of risk Special Sensitive Position and/or TS Security Clearance with Sensitive Compartmented Information (SCI)	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI) (30)
High Risk Public Trust Position Any level Sensitivity	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI) (30)

Figure 1, OPM Chart

2.9.2 If the required investigation is determined not to have been accomplished during a routine audit or review for an employee, or as mandated by changes in regulations by OPM, the CCS/CCPS will ensure the appropriate investigation is conducted as follows:

- a. The NASA program sponsoring the employee shall provide the NASA security office with the necessary funding to accomplish the required investigations.
- b. The sponsor shall notify OHCM personnel for civil service employees and the CCS/CCPS for contractor employees and whether a PSI will be initiated for the employee in e-QIP if required.
- c. The employee shall submit to fingerprinting, complete and submit the electronic forms in e-QIP, and sign the appropriate release pages.

2.9.3 The timing of security form submittal and the established risk level may dictate whether a proposed NASA

employee can begin work prior to a final access determination. The CCS/CCPS shall advise the sponsor whether the individual can commence working prior to the receipt of the completed investigation and final access determination based on the specifics of the situation and a preliminary review of the fingerprint card results and submitted forms.

2.10 Investigation and Reinvestigation Requirements for NASA Civil Service Employees and Appointees without Access to CNSI

2.10.1 Center OHCM offices shall initiate a NACI in e-QIP on a SF 85 for new civil service employees and appointees performing duties in low-risk positions. Initial investigations require the employee to complete the SF 85, an OF 306, and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87. Center security offices may initiate any investigation type in e-QIPs on behalf of OHCM upon approval of the CCS/CCPS.

a. Center security offices shall initiate a reinvestigation for low-risk civil service employees and appointees every ten years in e-QIP utilizing the NACI investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85 and submit to fingerprinting upon notification by the security office.

2.10.2 Center OHCM offices shall initiate a Moderate Background Investigation (MBI) in e-QIP on a SF 85P for new, transferred or promoted civil service employees and appointees performing duties in moderate-risk public trust positions. Initial MBI investigations require the employee to complete the SF 85P, an OF 306 and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87.

a. Center security offices shall initiate a reinvestigation for moderate-risk public trust civil service employees and appointees every five years in e-QIP utilizing the NACLIC investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85P and submit to fingerprinting upon notification by the security office of reinvestigation.

2.10.3 Center OHCM offices shall initiate a Background Investigation (BI) in e-QIP on a SF 85P for new, transferred or promoted civil service applicants and appointees performing duties in high-risk public trust positions. Initial BI investigations require the employee to complete the SF 85P, an OF 306 and to submit to electronic fingerprinting or hard copy fingerprinting on an OPM Fingerprint Card SF 87.

a. Center security offices shall initiate a reinvestigation for high-risk public trust civil service employees and appointees every five years in e-QIP utilizing the Periodic Reinvestigation (PRI) investigative product from OPM. The civil service employee or appointee will electronically complete the SF 85P and submit to fingerprinting upon notification by the security office of reinvestigation.

2.10.4 When a civil service employee or appointee experiences a change in duties due to promotion or reassignment and the risk level is higher, a new investigation commensurate to the risk should be transmitted to OPM within 14 calendar days of the effective date of the action.

2.11 Investigation and Reinvestigation Requirements for NASA Contractor Employees without Access to CNSI

2.11.1 Center security offices shall initiate a NACI in e-QIP on a SF 85 for contractor employees performing duties in low-risk positions. Investigations requested on the SF 85 also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on a FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor low-risk reinvestigations shall be initiated every ten years utilizing the NACI investigative product from OPM. The contractor employee will electronically complete a SF 85 and submit to fingerprinting upon notification by the security office of reinvestigation.

2.11.2 Center security offices shall initiate an MBI in e-QIP on a SF 85P for contractor employees performing duties in moderate-risk public trust positions with no access to CNSI. Investigations requested on the SF 85P also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on an FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor moderate-risk public trust reinvestigations shall be initiated every five years utilizing the NACLIC investigative product from OPM. The contractor employee will electronically complete the SF 85P in e-QIP and submit to fingerprinting upon notification by the security office of reinvestigation.

2.11.3 Center security offices shall initiate a BI in e-QIP on a SF85P for contractor employees performing duties in high-risk public trust positions with no access to CNSI. Investigations requested on the SF 85P also require the applicant to complete an OF 306 and to submit to electronic fingerprinting or hard copy fingerprints on an FBI Applicant Fingerprint Card (FD 258) for submission to OPM.

a. Contractor high-risk public trust reinvestigations shall be initiated every five years in e-QIP utilizing the Periodic

Reinvestigation (PRI) investigative product from OPM. The contractor employee will electronically complete an SF 85P in e-QIP and submit to fingerprinting upon notification by the security office of reinvestigation

2.11.4 When a contractor employee experiences a change in work due to promotion or reassignment and the risk level is higher, a new investigation commensurate to the risk should be transmitted to OPM within 14 calendar days of the effective date of the action.

2.12 Processing Personnel Security Investigation Requests in e-QIP

2.12.1 Electronic Questionnaires for Investigation Processing (e-QIP) is a secure Web site that is designed to transmit all PSI requests. The questionnaires processed through e-QIP include: SF 85, Questionnaire for Non-Sensitive Positions; SF 85P, Questionnaire for Public Trust Positions; and SF 86, Questionnaire for National Security Positions.

2.12.2 Every e-QIP user, both Agency staff and applicant, has specific responsibilities that correspond to e-QIP roles as follows:

- a. Agency Advocate: The highest-level official within each activity. This role is the AA, OPS.
- b. Agency Administrator: OPM-FIS's main point of contact at the Agency for e-QIP. This position is located in OPS' Security Management Division.
- c. Technical Administrators: The experts in technology available at each Agency and the Agency Chief Information Officer (CIO).
- d. User Administrator: Enters Agency users into e-QIP based upon duties and level of investigation of staff working in e-QIP.
- e. Program Manager: Serves as the day-to-day point of contact for initiators, reviewers, and approvers at each Center.
- f. Business Manager: User role with access to the View Reports option in e-QIP responsible for generating standard reports based on e-QIP data such as the Agency request status, Agency user role, and Agency request event count reports.
- g. Approver: Conducts a final review of the investigation and forwards the request to the Investigation Service Provider (ISP). The e-QIP approver shall be a Federal employee.
- h. Reviewer: Examines the investigation request and forwards it to the approver, if applicable.
- i. Initiator: Serves as the applicant's main point of contact during the investigation request process.
- j. Agency Help Desk: Able to reset Golden Questions for applicants who have active requests in their agency or within a subordinate agency and view an applicant's request summary.

2.12.3 OPM has mandated that individuals who are given roles in e-QIP are vetted as follows:

- a. Agency administrator, program manager, approver, and reviewer role: NACLIC or MBI.
- b. User administrator: SSBI or BI.
- c. Business managers, initiators, and agency help desk: NACLIC.

2.12.4 E-QIP users should access the OPM portal as a gateway to the e-QIP database. The portal is a secure, encrypted environment known as the OPM's Investigative Service (OPMIS) secure portal. The OPMIS secure portal can be used for the exchange of Sensitive but Unclassified Information (SBU), such as Privacy Act Information and Personally Identifiable Information (PII). E-QIP users and other community members with portal access can send and receive email, review and download documents, and access information on OPM products and services through the portal. In addition to e-QIP, the portal acts as the gateway to OPM-Federal Investigative Services Division (FISD) computer systems, such as Personnel Investigations Processing System (PIPS) and CVS. E-QIP users who do not use their e-QIP role assignments within a 35-day period will be deactivated from access to OPM's secure portal.

2.12.5 E-QIP Approvers must be Federal employees. They are responsible for properly annotating the appropriate Security Office Identifier (SOI) to ensure the completed SF 86s are returned by OPM to the NASA CAF for adjudication. This SOI number is available from NASA CAF personnel.

2.13 Individuals with Prior Criminal Record

2.13.1 Individuals with a criminal record (except minor traffic) shall be adjudicated for access in accordance with Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," July 31, 2008, and "Memorandum to Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, Security Clearance Decision Making Guide" January 14, 2008.

2.14 Adverse Information

2.14.1 When adverse information is self-reported, developed or received in the course of any personnel security investigation, or subsequent to such investigation and initial favorable determination, the scope of inquiry shall be expanded to the extent necessary to obtain sufficient information to make a reasonable and sound determination as to whether the employee is fit to perform work for or on behalf of the Government and/or is eligible for logical and physical access.

2.14.1.1 These expanded inquiries shall be conducted by a NASA security or OHCM official with appropriate investigative experience, NASA contracted investigators, by the original investigating agency, or by another agency of the Federal Government at NASA's request.

2.14.1.2 Any expanded investigation may consist of many different lines of inquiry including, but not limited to, interviews of the employee, supervisors, co-workers, neighbors, and physicians; records checks with various local agencies; and credit checks.

2.14.2.1 Appropriate signed releases from the employee shall be obtained when required to pursue additional leads such as medical records and credit checks.

2.14.2.2 Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center Counterintelligence Office.

2.14.3.1 A personal interview or expanded inquiry shall be held with an employee on whom significant unfavorable or derogatory information has been developed or received during the screening process. The employee shall be offered an opportunity to refute, explain, clarify, or mitigate the information in question.

2.14.3.2 The personal interview or expanded inquiries shall be conducted by a qualified NASA security official, by the original investigating agency, or another agency of the Federal Government at NASA's request.

2.14.4 Agency officials shall conduct a new fitness determination at any time adverse information is obtained that calls into question an individual's fitness based on character or conduct. This may include a new PSI or database query and adjudication. Adverse information involving civil service employees shall be referred to the Center OHCM for appropriate action.

2.15 Reciprocity of Other Agency Adjudications

2.15.1 OPM's CVS shall be checked by a NASA trusted information provider who has undergone a favorably adjudicated PSI to determine if a prior investigation will serve reciprocally for a NASA determination for contractor fitness or access to physical and logical resources. If there is no favorably adjudicated PSI identified in CVS or any other trusted government agency that will serve reciprocally, a PSI will be initiated in e-QIP for the contractor employee commensurate to the risk level associated with the contract.

2.15.2 Reciprocal recognition of fitness shall be granted for a prior favorable fitness or suitability determination when:

a. Equivalent 5 C.F.R. Pt. 731 adjudicative criteria was used for Federal employees and OPM's Final Credentialing Standards for issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008, was used for contractor employees; and

b. The individual has had no break in employment since the favorable determination was made. With regard to contractor employees, a break in employment also refers to a break in employment on a Federal contract, and not just a break in employment with a particular contractor. If the individual has stopped working on a Federal contract, but continues to work for the contractor on a non-Federal contract, this is deemed to be a break in employment.

2.15.3 NASA personnel are not required to grant reciprocal recognition for a prior favorable fitness or suitability determination when:

a. The new position requires a higher level of investigation than previously conducted for that individual; or

b. An agency obtains new information that calls into question the individual's fitness based on character or conduct; or

c. The individual's investigative record reflects conduct that is incompatible with the core duties of the new position; or

d. The investigation is out of scope.

2.16 HSPD-12 Credentialing Standards

2.16.1 OPM's Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," July 31, 2008, shall be used by trained adjudicators to

determine eligibility for physical and logical access only. PIV authorizers will be trained in adjudication by certified adjudication training providers if they perform adjudication duties. A PIV card will not be issued to a person if:

- (1) The individual is known to be or reasonably suspected of being a terrorist;
- (2) The employer is unable to verify the individual's claimed identity;
- (3) There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;
- (4) There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;
- (5) There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or
- (6) There is a reasonable basis to believe the individual will use federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

2.16.2 When a person does not require a suitability determination or a security clearance, adjudicators shall apply seven Supplemental Credentialing Standards. These standards are intended to ensure that the grant of a PIV card to an individual does not create an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; records; or to the privacy of data subjects. A PIV card will not be issued to a person if:

- (1) There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;
- (2) There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;
- (3) There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV card poses an unacceptable risk;
- (4) There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;
- (5) There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;
- (6) A statutory or regulatory bar prevents the individual's contract employment or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or
- (7) The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

2.16.3 For the purpose of this adjudicative policy, the "whole person concept" is defined for those eligible for physical and logical access. Logical and physical access shall be granted for individuals on whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicate there is no unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial or medical records; or to the privacy of data. An individual's trustworthiness, honesty, reliability, discretion, and sound judgment are fundamental to the adjudicative process. This "whole person concept" will provide a balanced assessment of positive as well as negative aspects of an individual's past and present activities.

2.16.4 Adjudicators will use the OPM's Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide," dated January 14, 2008, as a resource for deriving a reasonable conclusion or decision based on the standards outlined in OPM's Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD -12."

2.16.4.1 Adjudicators will not add or delete or modify the adjudicative standards. Final adjudications for suitability will be performed within 90 days from receipt of a ROI from OPM.

2.16.4.2 The investigation closing date and adjudicative action will be recorded in IdMAX, submitted on OPM form INV 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations or electronically annotated in OPM PIPS/CVS under Agency Menu as soon as possible after adjudication. Flat files from IdMAX may also be uploaded into OPM's PIPS/CVS system.

2.17 Reconsideration Procedures for Contractor Employees and other Agency Affiliates

2.17.1 Notice of Proposed Action - When an adjudicator determines that a PIV applicant has not provided his or her true identity, the applicant is determined unfit for Center access or to be employed in the current or applied for position based on an unfavorable adjudication, the adjudicator shall provide the individual reasonable notice of the determination including the reasons(s). The notice should state the specific reasons for the determination and that the individual has the right to answer the notice in writing within 10 working days. The notice will inform the individual of the time limits, as well as the address to which the response should be made.

2.17.2 The individual may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

2.17.3 Decision - After consideration of any documentation submitted by the PIV applicant for reconsideration of the initial determination, the CCS/CCPS or his/her designee will issue a written decision (usually within 10 days), which informs the PIV applicant of the reasons for the favorable or unfavorable decision.

2.17.4 Reconsideration - If a denial letter is provided and the PIV applicant subsequently requests an appeal, the Center Director shall appoint a Credentialing Adjudication Review Panel (CARP) to review the information surrounding the denial of access. The panel will be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members shall have a favorable PSI and only one of the panel members may be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the CARP or they may request to appeal in person to the CARP. Any approved personal appearance before the CARP will be documented by means of a written summary or recording which will be made a part of the applicant's security record.

2.17.5 Prior to finalizing the CARP determination, a CARP panel member or the CCS/ CCPS may refer the CARP proposed decision to the Center Director for an additional level of review. If no referral is made to the Center Director, the CARP decision is final. If there is a referral to the Center Director, the Director's decision is final.

2.17.6 Upon determination that a denial has been upheld, there is no further reconsideration process. The individual may be debarred from access to the NASA Center, based on the denial for a period of one to three years. The IdMAX shall reflect any debarments to the Center, based on denial or revocation of PIV.

2.18 Personnel Security File Storage and Access

2.18.1 Records and information related to this policy shall be managed in accordance with NPD 1440.6H, NASA Records Management, and NPR 1441.1D, NASA Records Retention Schedules. Personnel security files are temporary records and are destroyed in accordance with the disposition instructions NPR 1441.1D.

2.18.2 Information from personnel security files may be disclosed to a Federal agency in response to requests in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation, the classifying of a position, the reporting of an investigation of an employee, the letting of a contract, and/or the issuance of a license, grant, or other benefit by the requesting agency to the extent that the information is appropriate for release to the requesting official, relevant and necessary to the requesting agency's decision on the matter.

2.18.3 Subjects of personnel security investigations and screenings may request copies of excerpts, summaries, or any analytical extract of information from the NASA case file under the Freedom of Information Act and Privacy Act procedures. The subject may not be provided a copy of any third-party investigations (i.e., OPM, FBI). The subject should obtain copies of the third-party investigation directly from the appropriate agency.

2.18.4 The results of OPM PSIs are furnished to NASA for the limited purpose of making suitability, security, and/or fitness determinations. E-delivery investigations adjudicative actions shall be reported using the "Enter Agency Adjudication" function on the Personnel Investigations Processing System (PIPS) Agency menu, which is accessible through either a dedicated PIPS terminal or OPM FIS' Web-based Secure Portal. E-delivery information processors/users shall destroy the distributed investigative file after eligibility has been rendered and/or the data is no longer needed.

a. Requests for an OPM investigative file for any other purpose should be directed to OPM. Requests should be referred to OPM and not to a NASA Center security office. OPM's investigative files are maintained in a Privacy Act System of Records; therefore, OPM must determine if there is a statutory provision or a published routine use that permits them to release the investigative file without an individual's written authorization.

2.18.5 OPM's FISD maintains the PIPS, a system which maintains the Security/Suitability Investigations Index (SII). The SII is a repository of millions of PSI records of Federal employees, contract employees, and military personnel.

These records are maintained for a minimum of 16 years. NASA Security Specialists who are authorized by the OPS Director, Security Management Division may access these files and perform searches of the database to determine if an individual already has a PSI that may serve for hiring, credentialing, or granting a security clearance. Authorized individuals can perform SII searches, request files, and transmit messages to OPM as well as access security clearance information and HSPD-12 credentialing information through the CVS.

2.18.6 Center security office personnel shall securely maintain personnel security investigative and screening records for credentialing decisions on all NASA civil service and contractor personnel. Center security offices may use databases maintained by OHCM to confirm the position risk and sensitivity of civil service employees rather than maintaining duplicative file copies of position descriptions. These records can be stored electronically at the discretion of the CCS/CCPS at each Center as long as the information technology system allows for encryption at rest of PII. However, Center security offices should be able to convert the documents into an accessible, reproducible, legible, quality approved electronic format. Once the conversion has been completed, the contents of the document may be recognized as the official record. Paper documents such as PSIs, investigation scheduling notices, and advance National Agency Checks (NACs) that have served their purpose and are no longer needed may be destroyed via shredding or burning.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) |
[AppendixC](#) | [ALL](#) |

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
