NASA Interim Directive

Effective Date: July 20, 2011
Expiration Date: July 20, 2012

COMPLIANCE IS MANDATORY

NASA Personnel Security

Responsible Office: Office of Protective Services

Table of Contents

Preface

P.1 PURPOSE

a. This NASA Interim Directive (NID) establishes Agency-wide personnel security program implementation requirements set forth in NASA Security Policy Directive (NPD) 1600.2E, as amended.

b. This NID prescribes personnel security program responsibilities and procedural requirements for the investigation, security clearance determination, continuous evaluation, contractor fitness, adjudication and appeals of NASA federal and contractor employees.

P.2 APPLICABILITY

a. This NID is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers, herein referred to as Centers.

b. This NID is applicable to all NASA employees (civil servants and contractors), personnel completing work through Space Act Agreements or Memorandums of Agreement/ Understanding, those assigned or detailed under the Intergovernmental Personnel Act, partners, recipients of grants and cooperative agreements, and visitors.

P.3 AUTHORITY

The National Aeronautics and Space Act, 51 U.S.C. § 20113(a).

P.4 APPLICABLE DOCUMENTS

a. Suitability 5 C.F.R. pt.731

b. National Security Positions 5 C.F.R. pt.732

c. Suspension and Removal 5 U.S.C. §7532

d. e-Gov Act of 2002 Pub. L. No. 107-347, 44 U.S.C. Ch 36.

e. Privacy Act of 1974 Pub. L. No. 93-579

f. Crime Control Act of 1990, Child Care Worker Employee Background Checks Pub. L. No. 101-647

g. Intelligence Reform and Terrorism Prevention Act of 2004 Pub. L. 108-458 (Dec. 17, 2004)

h. Executive (Exec.) Order No. 10450, Security Requirements for Government Employment April 17, 1953.

i. Exec. Order No. 12829, National Industrial Security Program, as amended.

j. Exec. Order No. 12968, Access to Classified Information, as amended.

k. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors August 27, 2004

l. OMB Memo M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 -Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005.

m. OMB Memorandum, Reciprocal Recognition of Existing Personnel Security Clearances December 12, 2005.

n. Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors," March 2006, as amended.

o. OMB Memorandum for Deputies of Executive Departments and Agencies, "Reciprocal Recognition of Existing Personnel Security Clearances," November 14, 2007.

p. OMB Memorandum for Deputies of Executive Department and Agencies "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2008.

q. 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," January 14, 2008.

r. Memorandum for Heads of Departments and Agencies, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12" July 31,2008.

s. Security Executive Agent, Suitability Executive Agent, Memorandum, Approval of Federal Investigative Standards December 13, 2008.

t. Exec. Order No. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust, January 22, 2009.

u. Exec. Order No. 13467, Reforming Processes Related to Suitability for government Employment, fitness for contractor Employees, and eligibility for Access to Classified National Security Information, June 30, 2009.

v. Memorandum for Heads of Agencies Aligning OPM Investigative Levels with Reform Concepts, August 24, 2010

w. NPR 1382.1, NASA Privacy Procedural Requirements.

x. NPR 2810.A, Security of Information Technology.
y. OMB Memo M-11-11, Memorandum for the Heads of Executive Departments and Agencies, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011

z. NPR 2841.1, Identity, Credential, and Access Management

P.5 MEASUREMENT/VERIFICATION

Compliance with this NID shall be determined by Agency application of uniform suitability, security clearance, and contractor fitness and adjudication procedures for vetting by fostering reciprocity, reduce duplication of effort, ensure consistent quality and standards for adjudication procedures and; rely upon modern analytic methods rather than practices that avoid risk.

P.6 CANCELLATION

NPR 1600.1, NASA Security Program Procedural Requirements, Chapter 2, 3, and 4.

Dr. Woodrow Whitlow, Jr.
Associate Administrator for Mission Support Directorate

CHAPTER 1. Introduction

1.1 Overview

1.1.1. The NASA Administrator is responsible for implementing a comprehensive and effective personnel security program for the Agency. There are many purposes of personnel investigations. There is a need to:

a. Evaluate character and conduct of government workers with suitability determinations for positions covered by 5 C.F.R. pt.731 and continuous evaluation through reinvestigations of individuals in position of public trust as required by Exec. Order No. 13488.

b. Evaluate character and conduct of workers by making fitness determinations for contractor employment per contractual requirements.

c. Evaluate character and conduct of government workers for accepted service or other positions not covered by 5 C.F.R. pt.731 or National Security requirements.

d. Determine eligibility of federal employees for National Security Positions under Exec. Order No. 10450 and eligibility for a clearance to access classified information under Exec. Order No. 12968 and continuous evaluation through reinvestigation of individuals holding clearances under Exec. Order No. 12968.

e. Determine eligibility under Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) as mandated in Federal Information Processing Standards (FIPS) Publication 201-1 for access to Federal facilities and federally controlled information systems. Specifics for PIV processing are outlined in FIPS SP 800-79-1 and referenced in NPR 2841.1, Identity, Credential, and Access Management.

1.2 Recordkeeping

1.2.1 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.

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

1.2.3. 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 and Privacy Act procedures. The subject may not be provided a copy of

any third party investigations (i.e., OPM, FBI). The subject must obtain copies of the third party investigation directly from the appropriate agency.

1.2.4 The results of OPM background investigations are furnished to NASA for a limited purpose of making suitability, security and/or fitness determinations. Requests for an OPM investigative file for any other purpose should be directed to OPM. Refer to www.opm.gov/investigate and not NASA Center security office personnel for more information. 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 individuals' written authorization.

1.2.5 OPM's Federal Investigative Services Division maintains the Personnel Investigations Processing System (PIPS), a computer system which maintains the Security/Suitability Investigations Index (SII), a repository of millions of background investigation records of Federal and contract employees and military personnel. These records are maintained for a minimum of 16 years. NASA security specialists who are authorized by the Security Management Division Director may access these files and perform searches of the database to determine if an individual already has a background investigation that may serve for hiring, credentialing or security clearance determining. Authorized individuals can perform SII searches, request files, and transmit messages to the investigation provider. Other features include access to security clearance information through the Clearance Verification System (CVS).

1.2.6 Center Security Offices personnel shall securely maintain personnel security investigative and screening records on all NASA civil service and contractor personnel for credentialing decisions. Center security offices may use databases maintained by HR to confirm the position sensitivity on civil servants rather than maintaining duplicative files copies of position descriptions. These records can be stored electronically at the discretion of the Chief of Security/Chief of Protective Services at each Center as long as the information technology system allows for encryption at rest of personally identifiable information (PII). However, they must 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 background investigations, investigation scheduling notices, advance National Agency Checks (NACs) that have served their purpose and are no longer needed may be destroyed via shredding or burning.

1.3 Responsibilities

1.3.1 Assistant Administrator (AA) for Protective Services. The AA for Protective Services shall:

a. Establish and maintain an efficient personnel security program in accordance with federal standards consistent with current personnel security/fitness policies, procedural requirements, and guidelines as established by the Security Executive Agent, Director of National Intelligence, and the Suitability Executive Agent Office of Personnel Management.

b. Establish and maintain the NASA Central Adjudication Facility (CAF) at Headquarters. CAF personnel shall be responsible for adjudicating all investigative results for security clearances for access to CNSI for NASA civil servant employees only.

c. Serve jointly with the AA for Human Capital Management as Functional Administrator for Electronic Questionnaires for Investigation Processing (e-QIP) and be responsible for designing specific policy, program management and execution of the e-QIP system.

1.3.2 Center Directors shall:

a. Ensure the Center Chief of Security (CCS) manages the Center personnel security program in accordance with this NID.

b. Ensure full Center compliance with the provisions set forth in this chapter.

1.3.3 The CCS/Chief of Protective Services (CPS) shall:

a. Process security clearance requests for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

b. Process and submit background investigation requests to OPM electronically. Electronic Questionnaires for Investigations Processing (e-QIP) are mandated for use to submit background investigations for civil servant and contractor employees to OPM. CCS/CPS will ensure that a check of OPM databases such as PIPS/CVS is performed to identify any previous investigation that will serve reciprocally before initiating a background investigation. The acceptance of prior determinations must be based on an equivalent investigation and evidence of a favorably adjudicated investigation on the individual.

c. Notify NASA Central Adjudicating Facility (CAF) personnel of any adverse information regarding anyone at the Center who holds a security clearance.

d. Designate a federal civil servant employee with a satisfactorily adjudicated Background Investigation on file with OPM to serve in the role of Program Specialist in e-QIP, who is responsible for administering e-QIP at the Center level and training new e-QIP users.

e. Maintain close coordination with OPM Investigations Service (OPM-IS) and Federal Investigations Processing Service (OPM-FIPS) and process the appropriate requests for background investigations conducted.

f. Grant a NASA civil servant employee a security clearance access to execute a Classified Information Nondisclosure Statement (SF-312) for employees with first time access to national security information. The SF 312 must be witnessed by a NASA security official.

g. Suspend a civil servant employee's clearance access “for cause” based on developed qualifying adverse information under the Continuous Evaluation Program.

h. Perform an annual review of clearance and access requirements necessary to ensure Center personnel security clearance needs are properly managed. The CCS/CPS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

i. Make credentialing determinations for contractor employees based on OPM's July 31, 2008, memorandum entitled, "Final Credentialing Standards for Issuing Personal Identity Verification." The standards are intended to ensure that granting a PIV card does not present an unacceptable risk. These standards are equivalent to the factors in 5 C.F.R §731.202, when considered and applied consistent with OPM guidance on the evaluation of suitability concerns.

j. Ensure adjudications for credentialing are performed by senior personnel security specialists who have been trained in adjudication by an accredited provider.

k. In cooperation with Human Resource Specialists designate sensitive and National Security position sensitivity for all existing and newly established civil servant positions whose duties clearly reflect the requirement for access to CNSI.

l. Refer all employment suitability cases for NASA civil servant employees to the appropriate OHCM for review and adjudication as soon as possible after making a reasonable access determination for the issuance of a PIV credential upon receipt of the Report of Investigation (ROI).

m. Assist OHCM personnel by conducting local records checks or automated record checks such as CVS, to clarify, expand, or mitigate information that has been provided by the investigation provider or a Department of Justice, National Crime Information Center (NCIC) query when requested.

n. Maintain, in accordance with the Privacy Act and existing NASA system of records, individual personnel security files on all investigated personnel; review applicable reports with officials in the review process who shall make the determination relative to continued access or revocation of access privileges. Files must contain, at a minimum:

(1). Copies of the OPM Case Closing Transmittal, Certification of Investigation, signed e-QIP release sheets and a signed and dated copy of the OPM Form OF79A. NASA CAF personnel will maintain copies of the OPM Form OF79A for federal employees processed for security clearances

(2). Any adverse information reports on affected contractor or civil servant employees.

(3) Copies of concurrence documentation from Office of International and Interagency Relations (OIIR) for any foreign national granted access to classified information (See 4.8.6 3.c.)

(4). Signed copies of Classified Information Nondisclosure Agreements, SF 312 for NASA civil servant employees who have access to Classified National Security Information (CNSI);
1.3.4 The CCS/CPS shall establish written procedures for the following:

a. Maintaining electronic files and distributing instructions for the completion of all electronic forms for the investigation process.

b. Assuring the appropriate investigation has been conducted for each NASA federal or contractor employee.

c. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation if needed to make a credentialing decision.

d. Conducting local records checks or automated record checks when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS/CPS.

e. Making appropriate notifications for confirmation of the results of a favorable access determination or actions as a result of a non-favorable access determination.

1.3.5 The Director of Office of Human Capital Management (OHCM) at each Center shall:

a. Designate the position for each civil servant employee in a competitive service position as high, moderate or low risk as determined by the potential for adverse impact to the efficiency and integrity of the service.

b. Verify employment eligibility of a civil servant new hire. Review OPM Form OF 306 documents for new hires. Review or coordinate for the review with CCS/CPS for the review of I-9 documents.

c. Determine recognition of reciprocal suitability determinations or ensure e-QIP is initiated on a civil servant new hire as soon as possible and no later than 14 days after entry on duty (EOD) date.

d. Grant reciprocal recognition to prior suitability determinations in accordance with Exec. Order No. 13488 when:

(1). The gaining agency uses criteria from making fitness determinations equivalent to suitability standards established by OPM;

(2). The prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by OPM; and

(3). The individual has had no break in employment since the favorable determination was made.

e. Deny reciprocal recognition of a prior favorable fitness or suitability determination when:

(1). The new position requires a higher level of investigation than previously conducted for that individual;
(2). An agency obtains new information that calls into question the individual's fitness based on character or conduct; or

(3). The individual's investigative record shows conduct that is incompatible with the core duties of the new position

f. Refer medical related data in investigative files to the NASA medical authority for review and evaluation in order to adjudicate suitability.

g. Ensure that supervisors are advised on the proper processing of any personnel who may be reassigned or are the subject of other personnel actions, including termination, resulting from the revocation of security clearance.

1.3.4 The Center OHCM Organizations shall:

a. Ensure that appropriate management and supervisory personnel identify and develop the position descriptions for positions that may require access to CNSI. These position descriptions must reflect the level of National Security Access and establish clear requirements for processing as required under 5 C.F.R §§732.101, 732.401, and Exec. Order 12968.

b. Ensure no recruitment, hiring, or change of position action takes place until the appropriate position sensitivity level and risk designation has been established and the position description updated to reflect the change.

c. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this chapter.

1.3.5 Program, Line Managers, and Supervisors shall:

a. Ensure full compliance with the requirements established in this policy.

b. As a critical element of their supervisory and management duties, ensure appropriate and accurate position risk designation and sensitivity levels are assigned for all civil servants under their purview per 5 C.F.R pts. 731, 732, and Exec. Order No. 10450.

c. Assist OHCM personnel during the suitability determination process

d. Ensure that civil servant employees requiring re-investigations according to position risk levels comply with all requirements from OPS and OHCM.

1.3.6 The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NID.

1.3.7 Contract Management Officials (Contractor Management, Contracting Officer's Technical Representative (COTR), and Project Managers) shall:

a. Ensure full compliance with this chapter.

b. Coordinate with the CCS/CPS for the designation of risk for contractor employees and the timely on boarding of contractor employees.

1.4 Waivers and Exceptions.

a. Centers may occasionally experience difficulty in meeting specific security requirements established by NASA policy. The process for submitting requests for waivers or exceptions to specific elements of the NASA security program requires that the asset, program, or project manager and CCS/CPS justify the waiver request through:

(1) Security risk analysis, (e.g., cost of implementation);

(2) Effect of potential loss of capability to the Center;

(3) Compromise of national security information;

(4) Injury or loss of life; loss of one-of-a-kind capability;

(5) Inability of the CCS/CPS to perform its missions and goals.

b. Justification must also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

c. The waiver request shall be submitted to the Center Director.

1.4.2. The Center Director either recommends approval or returns the waiver request to the CCS/CPS for further study or closure. The Center Director shall forward concurrence to the Mission Support Directorate Associate Administrator.

1.4.3. The Mission Support Directorate Associate Administrator shall forward waiver requests to the Assistant Administrator for Security and Program Protection (AA for Protective Services) at Headquarters and return proposals to the Center director for further study or closure.

1.4.4. The AA for Protective Services shall return the waiver request to the appropriate Center Director with the approval wavier, for further study, or denial and closure.

1.5 Violations of Security Requirements.

1.5.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA personnel security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C.§ 799, that provides fines or imprisonment for not more than 1 year, or both.

CHAPTER 2. Access to National Security Information

2.1 General

2.1.1 Title 5, Code of Federal Regulations (C.F.R), pt.732, National Security Positions, requires each agency to follow established procedures to identify national security positions. Positions identified by this process within the National Aeronautics and Space Administration (NASA) require regular use of or access to classified information. This chapter addresses the sensitivity designation program associated only with national security; the criteria for determining national security sensitivity levels, and screening (i.e., the type of investigation) required under Exec. Order No. 10450, Security Requirements for Government Employment, and Exec. Order No.12968, Access to Classified Information, as amended.

2.1.2 Position sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a national security position, could cause to the national security.

2.1.3 Investigations are conducted to provide a basis for ensuring that the granting of a security clearance to an individual is clearly consistent with the interests of national security.

2.1.4 Personnel security reports and records shall be handled in accordance with the Privacy Act of 1974.

2.1.5 OPM conducts a range of investigations that satisfy the various requirements for the three position-sensitivity levels described in this chapter, as they relate to accessing CNSI.

2.1.6 NASA Contracts requiring the generation of and/or access to CNSI will be processed and individuals investigated in accordance with the requirements in the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

2.2 Scope

2.2.1 This chapter prescribes the procedures whereby NASA federal employees are selected, processed, investigated, and adjudicated for national security positions, consistent with adjudicative guidelines contained in White House Memo, Adjudicative Guidelines, of December 29, 2005 contained in Appendix D and the OPM's Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide.

2.2.2 This chapter does apply to contractor employees providing services under a NASA classified contract that requires access to Sensitive compartmented Information

2.3 Personnel Security Program Oversight

2.3.1 As part of its responsibility for the functional management of the NASA security program shall include personnel security program matters in functional reviews or periodic audits of Center security programs.

2.4 Basic Principles of Personnel Security Clearance Management

2.4.1 The purpose of the personnel security program is to ensure that only loyal, trustworthy, and reliable people are granted access to classified information or assigned to sensitive duties.

2.4.2 Exec. Order No. 13526, Classified National Security Information. A person may have access to classified information provided that:

a. A favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

b. The person has signed an SF 312; and

c. The person has a need-to-know the information.

2.4.3 Every person who has met the standards for access to classified information in section 2.4.2.a shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

2.4.4 Exec. Order No. 12968, Access to Classified Information, directs that background investigation and eligibility determination conducted under the Executive Order be mutually and reciprocally accepted by all agencies unless an agency has substantial information indicating an employee may not satisfy the access eligibility standards. The Executive Order directs employees who are eligible for access to classified information be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access.

2.4.5 Due to the cost and time invested in conducting the appropriate investigation, managers and supervisors must be judicious and accurate in determining an employee's position sensitivity and need for access to CNSI. Managers and supervisors must establish the access requirement during the development of the individual position description and assign the appropriate designation of position risk and sensitivity for each NASA position description. Failure to properly identify the need for access to CNSI upfront causes added expense that must be borne by the program and results in unnecessary delays.

2.4.6 Access to CNSI shall not be requested or granted solely to permit entry to, or ease of movement within NASA controlled areas when the individual involved has no need for access to classified information.

2.4.7 Requests for security clearances shall not be processed or granted based merely on a speculative need for access or as a result of any particular, grade, position, or affiliation. Requesting security clearances for contingency purposes in excess of actual official requirements is prohibited.

2.4.8 The level at which access to CNSI is requested and granted shall be limited and relate directly to the level of classified information to which access is clearly justified in the performance of official duties and the individual has a demonstrated "need to know".

2.4.9 The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

2.5 Processing Personnel Security Requests in e-QIP

2.5.1 Electronic Questionnaires for Investigation Processing (e-QIP) is a secure website that is designed to transmit all personnel background investigation requests. These questionnaires are processed through e-QIP. The Standard Form (SF 86) is the questionnaire for National Security Positions. The SF 85P is the questionnaire used for Public Trust Positions and the SF 85 is the questionnaire for Non-Sensitive Positions.

2.5.2 Every e-QIP user – both agency staff and applicant – has specific responsibilities that correspond to e-QIP roles as follows:

a. Agency Advocate is the highest-level official within each activity and this role is shared between the AA Office of Protective Services and AA for Human Capital

b. Functional Administrator is the highest -level official within each functional area of NASA.

c. Technical Administrators are the experts in technology available at each agency and the Agency Chief Information Officer (CIO).

d. Program Specialists serve as team leaders and manage day-to-day operations at each Center.

2.5.3 The Office of Personnel Management (OPM) has mandated that individuals who are given roles in Electronic Questionnaire for Investigations Processing (e-QIP) are vetted as follows:

a. NACLC (National Security) or MBI (Public Trust): Agency Administrator, Program Manager, Approver and Reviewer Role

b. User Administrator = SSBI (National Security) or BI (Public Trust): User Administrator

c. NACI : Business Manager Role, Initiator, and Agency Help Desk Role

2.5.4 e-QIP users must access the OPM portal as a gateway to the e-QIP database. The portal is a secure, encrypted environment known as the 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. In addition to e-QIP, the portal acts as the gateway to OPM-FISD's computer systems (Personnel Investigations Processing System (PIPS) and Clearance Verification System (CVS)).

2.5.5 The requirement for access to CNSI shall be clearly established during the position description development phase. Once the position has been determined to require access to CNSI and position sensitivity has been assigned the new appointee completes the SF 86 in e-QIP.

2.5.6 An annual review of clearance and access requirements is necessary to ensure Center personnel security clearance needs are properly managed. The CCS/CPS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

2.5.7 Personnel with clearances who have not had the need to access CNSI during the previous year will be given serious consideration for administrative withdrawal of their clearance as determined by supervisors during the revalidation process.

2.5.8 Clearances will not be retained merely as a stop-gap measure in the event the holder may need access to CNSI. There must be a clear demonstrable operational requirement to possess the clearance as annotated in the position description.

2.5.9 e-QIP Approvers are responsible for properly annotating the agency use block in e-QIP to include 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.

2.5.10 Results of the adjudication process are to be posted and made available to Center security personnel via the NASA Clearance Tracking System (NCTS). The employee will be notified, in writing, when an Interim or Final clearance has been granted by the center personnel security program Office. The CCS/CPS may then grant final access and execute the SF 312. The center security office shall conduct all required orientation training in conjunction with the execution of the SF 312.

2.6 Sensitive Compartmented Information (SCI)

2.6.1 Candidates for SCI access must have a favorably adjudicated Top Secret investigation

2.6.2 Requests for access to Sensitive Compartmented Information (SCI) require the submittal of Form 2018A, (Special Access Request).

2.6.3 The Form 2018A must be prepared and justified by the employee's immediate supervisor, The line supervisor through the Division Director, or higher depending on the applicant's

Organizational position shall also review and approve the submittal. The request is then forwarded along with copies of the employee's personnel security file (PSF) and an additional copy of an updated SF 86, to the HQ Special Security Office (SSO) for appropriate action.
2.6.4 The Form 2018A and the original signed SCI Non-disclosure Form shall be retained by the SSO representative at the Center.

2.6.5 *Investigative Standards for Background Investigations for Access to Classified Information*, established as a result of Exec. Order No. 12968, individuals with "Q", Top Secret (TS), or Sensitive Compartmented Information (SCI) access, are subject to periodic reinvestigations at any time following the completion of, but no later than five years from the date of the previous investigation.

2.7 One-Time Access Determinations

2.7.1 Urgent operational requirements may occur when a NASA federal employee in non-sensitive positions with no security clearance eligibility determination have a one-time or short duration requirement for access to CNSI at the Confidential or Secret level. Usually, the limited duration or nature of this access requirement does not warrant processing the individual for a personnel security investigation and final security clearance eligibility determination. One-time access determinations shall not be granted for the Top Secret level and used sparingly and only under conditions of compelling government need. CCS/CPS or an official designated by the CCS/CPS has the authority to grant one-time access determinations subject to the following terms and conditions:

2.7.2 One-time access determinations shall not be issued more than 3 times to any person within a one calendar year timeframe. The aggregate access is to not exceed a total of 60 days accumulated during a single calendar year.

2.7.3 One-time access determinations shall only be granted to U.S. citizens that have been continuously employed by the Federal Government for the preceding 24 months.

2.7.4 Access shall be limited to a single instance or only a few occasions. Repeated access requests require processing for final security clearance determination.

2.7.5 If the need for access is expected to exceed 60 days, the individual must be processed for a final security clearance determination.

2.7.6 An individual requiring one-time access must complete a NASA Form 1630, Request for Access to CNSI; have a favorable National Agency Check with Inquiries, or a criminal history and credit check, a favorable suitability determination and local records check. They must complete a SF 86 for review by a trained adjudicator.

2.7.7 Individuals must sign an official nondisclosure statement (SF 312) witnessed by a NASA Security Official.

2.7.8 One-time access determinations and subsequent debriefs shall be documented in local files and any security clearance certification (i.e., one-time clearance granted from date-to-date) properly recorded.

2.8 Coding of Position Sensitivity Level Designation for National Security Positions

2.8.1 Positions previously designated as sensitive that do not have national security-related duties are designated as "public trust" positions. National security positions are designated as non-critical sensitive, critical sensitive, or special sensitive. Low-Risk and non-sensitive are not considered designations.

2.8.2 The proper coding of position sensitivity for national security positions is required on Optional Form 8, and optional on the SF 50 and 52. (See 5 C.F.R pt.732). NASA managers and supervisors must use National Security Position Sensitivity Level Codes whenever establishing position sensitivity for access to CNSI. The following codes shall be used: "4" for Special-Sensitive, "3" for Critical-Sensitive, "2" for Noncritical-Sensitive, and "1" for Non Sensitive (no clearance required).

2.8.3 Center OHCM personnel are responsible for managing a Risk Designation System in accordance with 5 C.F.R §731-106(a). They shall coordinate, in a timely manner, with managers, supervisors, and the CCS/CPS to accomplish sensitivity designation of positions requiring access to CNSI. After the appropriate position sensitivity determination has been assigned, the Center OHCM or OPS personnel initiate the appropriate investigation in e-QIP.

2.8.4 Individuals in positions designated low risk that may have access to classified information will be processed at the level commensurate with the clearance requirements. For example, a custodian in a position designated as low risk would be processed on a SF 86 rather than a SF 85 or 85P and the investigation requested would support the clearance required.

2.8.5 SPECIAL-SENSITIVE (SS): Positions requiring access to any of the levels of classified information outlined below shall be designated Special-Sensitive. Individuals in or selected for Top Secret Sensitive compartmented Information must undergo a Single Scope Background Investigation (SSBI) using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access to a Special Access Program (SAP). SAP requirements dictate that a periodic reinvestigation be initiated every 5 years.

2.8.6 CRITICAL-SENSITIVE (CS): Positions requiring access to Top Secret (TS) or North Atlantic Treaty Organization (NATO) Top Secret shall be designated Critical-Sensitive. Individuals in or selected for these positions must undergo a Single Scope Background Investigation (SSBI), using SF-86, and be favorably adjudicated prior to being granted access to:

2.8.7 NONCRITICAL-SENSITIVE (NCS): Positions requiring access to Confidential or Secret shall be designated Noncritical-Sensitive. New Hires selected for these positions must undergo, at a minimum, an Access National Agency Check with Inquiries (ANACI), using SF-86 in e-QIP, and be favorably adjudicated prior to being granted access.

2.8.8 Pre-appointment investigation requirements shall not be waived for positions designated "SPECIAL SENSITIVE."

2.8.9 Pre-appointment waivers should be authorized by the AA for Office of Protective Services to approve any appointment or reassignment to a "CRITICAL SENSITIVE" or "NONCRITICAL SENSITIVE" position prior to completion of the required pre-appointment investigation only when clear justification exists to warrant the waiver.

2.8.10 NON-SENSITIVE: Non-sensitive positions relate to any position that is not a "National Security Position."

2.8.11 All NASA positions designated "Testing Designation Positions (TDP)" will be in accordance with Exec. Order No. 12564. Personnel holding active security clearances shall be entered into the random drug-testing program.

2.9 Temporary/Interim Access to Classified National Security Information (CNSI)

2.9.1 Senior Management Officials shall request temporary access eligibility for U.S. citizen employees, civil service employees, and/or consultants filling CS and NCS positions when essential and immediate operational requirements do not allow for waiting for a pending personnel security investigation to be completed and adjudicated.

2.9.2 Management shall submit requests for temporary access eligibility using NASA Clearance Tracking System for approval and provide compelling justification to warrant access to CNSI in advance of formal investigation and adjudication.

2.9.3 In all cases, the required personnel security investigation shall be initiated and transmitted to OPM prior to issuance of the INTERIM clearance.

2.10 Access to CNSI by Non-U.S. Citizens

2.10.1 Non-U.S. citizens (including lawful permanent resident (LPR)) are not eligible for a security clearance. However, under specific situations the AA for Protective Services may authorize the granting of a Limited Access Authorization (LAA) to a non-U.S. citizen for specific information up to the Secret level when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization submits a written request to the AA for Protective Services via the CCS/CPS. The request shall:

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.

d. Explain how access shall be limited and physical custody of CNSI precluded.

e. The CCS/CPS shall review the request for accuracy, endorse or non-endorse it, and forward it to the AA for Protective Services.

f. The AA for Protective Services shall coordinate with AA OIIR for concurrence and if approved, shall return it to the requestor. A copy shall be retained in the OPS CAF and CCS/CPS files.

g. A completed investigation and favorable adjudication are required before access is granted. The granting of Interim or Temporary access pending the completion of an investigation is prohibited.

h. Denied requests shall be returned to the requestor with an explanation of the denial.

i. Individuals with LAAs shall be placed under closely controlled supervision of appropriately cleared persons (U.S. Citizens). Managers shall be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

j. Individuals who have been granted an LAA shall not be allowed access to any classified information other than that specifically authorized under national disclosure policy. Additionally, physical custody of classified information by these individuals is not authorized.

k. Non-U.S. citizens are ineligible for access to intelligence information, communications security keying materials, Top Secret information, Restricted or Formerly Restricted Data, Critical Nuclear Weapons Design Information (CNWDI), TEMPEST information, classified cryptographic information, or NATO classified information.

l. Classified access shall be limited to that necessary to complete the task, and access shall be terminated upon completion of the task.

m. Requests for access to CNSI owned by another agency must be coordinated with and approved by that agency.

2.10.2 If the access request is initiated by a NASA-cleared contractor performing on a NASA classified contract, only the Defense Industrial Security Clearance Office (DISCO) or successor organization, has the authority to grant an LAA to non-U.S. citizens. Procedures for coordination of the request are as follows:

a. A cleared contractor's Facility Security Officer must receive the endorsement of the CCS/CPS, Center International Visitor Coordinator (IVC), Center Export Administrator (CEA), AA for Protective Services, and OIIR (Export Control).

b. The CCS/CPS must ensure the contract is current and must evaluate the justification for the request. The non-U.S. citizen nominated for the LAA must sign a nondisclosure statement executed by the CCS/CPS. The CCS/CPS shall forward the completed package to the AA for Protective Services for review, coordination, and endorsement.

c. If acceptable, the AA for Protective Services shall endorse and return it to the contractor for forwarding to the DISCO. A completed SSBI and favorable adjudication are required before access is granted.

d. Denied requests shall be returned to the contractor with an explanation of the denial.

2.11 Reciprocal Recognition of Personnel Security Clearance Determinations

2.11.1 In furtherance of Exec. Order No. 12968, and Exec. Order No. 13467, background investigations and adjudications shall be mutually accepted. An employee with an existing security clearance (not including an interim clearance) who transfers or changes employment status is eligible for a security clearance at the same or lower level without additional or duplicative adjudication, investigation, or reinvestigation, and without any requirement to complete or update a security questionnaire unless substantial information indicates that the standards of Exec. Order No. 12968 may not have been satisfied so that eligibility would not be appropriate.

2.11.2 The "substantial information" exception to reciprocity of security clearances does not authorize requesting a new security questionnaire, reviewing existing background investigations , or initiating new investigative checks (such as a credit check) to determine whether such "substantial information exists.

2.11.3 Prior investigations shall be accepted reciprocally, provided the following conditions are met:

a. There has been no break in service in excess of 24 months;

b. Prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position

c. There has been no subsequent development of potentially disqualifying derogatory information

2.11.4 Reciprocity will not be granted if the following conditions apply:

a. the individual has more than 24 months break in service and,

b. a favorable adjudication is more than five years old

c. the agency obtains new information that calls into question the individuals continued eligibility for access to CNSI.

2.12 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)

2.12.1 Access to Restricted Data (RD) and Formerly Restricted Data (FRD) outside the scope of aeronautical and space activities require clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC).

2.12.2 If such access is required solely for the performance of service for another agency, that agency normally shall initiate the required investigation. In such a case, the OPM reimbursable investigation required for the occupant of a sensitive position must not be initiated.

2.12.3 The Central Adjudication Facility (NASA CAF) shall assist the other agency by obtaining and providing the required security documents.

2.12.4 When access to RD or FRD outside the scope of aeronautical and space activities are required in the performance of NASA duties, a request for either a DOE or an NRC clearance shall be initiated by the CCS/CPS, who shall forward the necessary documents to the Special Security Officer for appropriate action.

2.13 Guiding Principles for Adjudication, Suspension, Denial, or Revocation of Personnel Security Clearances

2.13.1 The Adjudicative Guidelines for Determining Eligibility for Access to Classified Information serve as a guide for investigators and adjudicators to identify potential issues that may adversely affect an individual's eligibility for access to classified information.

2.13.2 Only the AA for Protective Services or his designee shall deny or revoke a security clearance.

2.13.3 The AA for Protective Services and CCS/CPS may grant interim and final access determinations or suspend security clearances.

2.13.4 Adjudications shall be fully documented and recorded in the subject's security file and entered into the NASA Clearance Tracking System (NCTS).

2.13.5 Information developed during the investigation process for a security clearance shall not be shared with the Center OHCM or management while the investigation is pending. The AA for Protective Services or CCS/CPS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals or is a threat to a critical mission or that the subject shall otherwise be ineligible for or lose continuation of Federal employment.

2.13.6 All reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

2.13.7 The CCS/CPS shall propose suspensions of security clearances to NASA CAF personnel for cause based on developed adverse information. This information is usually provided in written form. The AA for Protective Services shall make final denial or revocation determinations if required after consultation with the NASA CAF and OGC personnel.

2.13.8 Requests for a security clearance shall result in an adjudicative determination unless, unrelated to any potential adjudication factor, the need for the security clearance no longer exists, such as severance of the subject's employment.

2.13.9 Subjects of adjudication are allowed to refute any information developed during the investigation process that may make him or her ineligible for access to classified information.

2.13.10 In the event of a denial or revocation of a security clearance, the subject is entitled to obtain review of the decision as prescribed in Section 5.2 of Exec. Order No. 12968.

2.13.11 The Center OHCM, in coordination with the Security Office and supervisors, shall make employment suitability determinations. The Center OHCM shall coordinate and document those determinations. They are separate and distinct from security clearance adjudications (see section 5.2(f) of Exec. Order No. 12968).

2.13.12 The policies and the procedures for the suspension, denial and revocation of a security clearance must not be confused with the procedures for the removal of an employee on national security grounds as set forth in Title 5, Chapter 75, Section 7532 of the U.S. Code. A CCS/CPS may coordinate with OHCM to pursue the removal of an employee on national security grounds under Section 7532, regardless of the sensitivity of the employee's position or whether the employee has access to classified information.

2.14 Bond Amendment

2.14.1 The Bond Amendment repealed 10 U.S.C. Section 996 formerly known as the Smith Amendment, and places restrictions that are similar to the Smith Amendment, but which apply to all Federal Government Agencies. The Bond Amendment bars person from holding a security clearance for access to Special Access Programs, Restricted Data and SCI if they have been:

a. Convicted of a crime and served more than one year of incarceration

b. Discharged from the Armed Forces under dishonorable conditions

c. Determined to be mentally incompetent by a court or administrative agency

2.7.2 The Bond Amendment also prohibits all Federal Agencies from granting or renewing a security clearance for any covered person who is an unlawful user of controlled substance or is an addict; this prohibition applies to all clearance holders.

2.15 Adjudication of Security Clearances

2.15.1 The AA for Protective Services, or designee, is authorized to approve, deny or revoke an employee's security clearance.

2.15.2 Each investigation required for a specific clearance level must be complete with sufficient scope in order to adjudicate appropriately access to classified information.

2.15.3 In instances when management, for reasons unrelated to the adjudicative process, withdraws a request for a security clearance and the subject of the investigation continues his or her employment with NASA, potential issue information developed during the investigative process will be made available to OHCM to make a suitability determinations under 5 C.F.R. pt. 752.

2.15.4 The initial adjudication will be made once the adjudicator has gathered all available pertinent information.

2.15.5 The Senior Adjudicator shall review the initial adjudication for fairness, completion, and proper application of the adjudication guidelines.

2.16 Suspension of Security Clearances

2.16.1 The AA for Protective Services, Center Director, or the CCS/CPS shall suspend an individual's security clearance when information is developed that suggests the individual's continued access to classified information is not in the interest of national security. The determination to suspend should be based on thorough review of definitive derogatory information as addressed in factor consideration outlined in Appendix D. All suspensions must be reported immediately to the Central Adjudication Facility by way of the NASA Clearance Tracking System.

a. Notify the subject accordingly. However, the reason or reasons for a suspension need not be provided to the subject of a suspension.

b. Suspension of a security clearance shall not be open-ended. Every effort must be expended to complete the investigation and to adjudicate as soon as practical. All suspension actions must be resolved as soon as practical from the date of the suspension.

c. Suspension of an individual's access to classified information is not an adverse action. Suspension merely allows the agency time to investigate and adjudicate information that may affect the individual's eligibility for access to classified information.

d. Upon receipt of suspension information containing documented facts that fully support the suspension, CAF personnel will determine whether to reinstate, or revoke the clearance of the individual.

2.17 Denial or Revocation of Personnel Security Clearances

2.17.1 No individual will be given access to classified information or assigned to a sensitive position unless a favorable security eligibility determination has been made. In the event of an unfavorable adjudication action, the NASA Central Adjudication Facility (NASA CAF) shall propose documented reasons in a Letter of Intent (LOI) to deny or revoke a clearance.

2.17.2 The Director, Security Management Division, shall do one of the following after reviewing the proposed unfavorable adjudicative action by CAF personnel:

a. Remand the case for further work; or

b. Reject or uphold the proposed adjudication of the information; and

c. In consultation with the Office of General Counsel, provide written notice to the subject of the denial of the revocation of the security clearance through the CCS/CPS

2.17.3 The employee will acknowledge receipt of the LOI and determine whether he/she intends to respond within the time specified in the LOI. If the subject provides new information for consideration, CAF personnel shall review the new information provided. CAF personnel will determine whether a security clearance should be reinstated, revoked or denied. If no information is provided or no response is provided within the specified time allowed, CAF personnel will continue with the denial or revocation process. Upon completion of the process, the subject will be notified by the CAF of a final decision in a Letter of Notification (LON). The letter is served through the CCS/CPS.

2.17.4 If the subject receives a LON of denial or revocation, the subject will be afforded an opportunity to appeal the LON to the AA for Protective Services.

2.17.5 Actions of the AA for Protective Services shall be conducted in accordance with the elements of section 5.2 (a) of Exec. Order No. 12968 and shall ensure that the rights of the subject are protected and due process is accorded, including the opportunity for the subject to appear in person to present relevant documents, materials, and information prior to final determination by the AA for Protective Services. If the employee takes advantage of the opportunity to appear personally before the AA for Protective Services, the AA for Protective Services shall document such appearance by means of a written summary or recording, which shall be made a part of the subject's security record.

2.17.6 If the AA for Protective Services provides a notice of denial or revocation and the subject subsequently requests an appeal by a Security Adjudication Review Panel (SARP), the Administrator shall appoint that body. The panel shall be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members must have been the subjects of a favorable SSBI, and only one of the panel members shall 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 SARP or they may chose to appeal in person to the SARP. Any personal appearance before the SARP shall be documented by means of a written summary or recording which shall not be made a part of the subject's security record.

2.17.7 Prior to finalizing the SARP determination, a SARP panel member or the AA for Protective Services may refer the SARP proposed decision to the Administrator for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If there is a referral to the Administrator, the Administrator's decision is final.

2.17.8 Upon determination that a clearance revocation or denial has been upheld, the case then becomes one of employment suitability and shall be referred to OHCM for suitability determination.

2.18 Continuous Evaluation of Personnel Security Clearance Eligibility

2.18.1 A personnel security clearance determination is based on a continuous assessment of an individual's personal and professional history demonstrating loyalty to the United States, strength of character, trustworthiness, reliability, discretion and sound judgment, as well as freedom from conflicting allegiances and potential coercion and willingness to abide by regulations governing the use, handling, and protection of CNSI.

2.18.2 In order to ensure that all persons who have been granted a security clearance remain eligible, all U.S. Government clearance holders shall be subject to a continuous evaluation of their qualifications to meet the high standards of conduct expected of persons in national security positions.

2.18.3 Persons subject to a prior favorable personnel security determination who demonstrate behavior that places doubt on their loyalty, reliability, or trustworthiness or otherwise disqualifies that individual for continued eligibility for a security clearance shall be subject to further scrutiny and possible suspension of access to CNSI.

2.18.4 Center Directors and the CCS/CPS shall ensure that a program of continuous evaluation for security clearance eligibility is developed that relies on all levels of management and all security clearance holders to be aware of the standards of conduct for qualification to hold a security clearance and their responsibility to report adverse behavior that is disqualifying. Where employees have significant involvement with handling, storing, marking CNSI, or exercising original or derivative classification, supervisors must include these responsibilities as a critical element of the employees' annual performance communication system documentation.

2.18.5 Supervisors and managers are critical to the success of the Continuous Evaluation Program. Supervisors shall report incidents of potentially disqualifying behavior that they are aware of to the CCS/CPS and be observant to potential changes in behavior of their subordinates that could cause potential risk to the classified national security information to which the employee has been entrusted.

2.18.6 Holders of security clearances and other employees with knowledge that an employee holds a security clearance shall be advised and periodically reminded to report to their supervisor or appropriate security officials when they become involved in behavior or become aware of such behavior of another cleared individual that could impact their continued eligibility for access to CNSI. A security clearance holder who fails to report disqualifying conduct involving other cleared personnel is also subject to suspension of access to CNSI, pending a security inquiry.

2.18.7 CCS/CPS should do fact-finding and depending on the adverse impact to national security, may suspend an individual's access to CNSI for cause. CCS/CPS may request a Periodic Assessment or other background investigation to support their assessment of the employees' continued access to classified information. CCS/CPS will forward a report to the NASA CAF personnel as soon as possible after fact-finding. CAF personnel will determine if the individuals continues to be eligible for access to CNSI.

2.19. Classified Visits and Meetings

2.19.1 Classified Visits to Other Agencies. An employee who has a need to certify his/her security clearance should contact the local personnel security office.

a. An Inter-Agency clearance Verification Request can be generated by the security office from NASA Clearance Tracking System (NCTS) and forwarded to the facility or custodian 2.19.1.2. The request may be completed by the personnel security specialist or Special Security Officer who has access to NCTS.

b. Visit requests should be for no more than one year at a time. Visit requests for longer than one-year are at the discretion of the visiting agency.

c. Classified Visit Requests From Other Agencies and Classified Meetings. Employees hosting meetings involving classified information will advise the prospective attendees to have their security officers prepare and transmit certifications of the attendees' security clearances to the respective center personnel security office, or the Special Security Officer. The certifications should include the investigation record information used as a basis to grant the clearance, Center point of contact, and purpose and duration of the visit.

d. Special Access Program Visits. All visit requests involving a special access program shall be processed by the appropriate Special Security Office.

CHAPTER 3. NASA Personnel Security Program

3.1 General

3.1.1 This policy applies to NASA Headquarters and NASA Centers, Component facilities and Technical and Service Support Centers, contractors, detailees, other non civil servants regardless of affiliation to include personnel completing work through Space Act Agreements or Memorandums or Agreement/Understanding, those assigned to or detailed under the Intergovernmental Personnel Act, where appropriate in achieving NASA missions, programs, projects, and institutional requirements. IPA employees may be identified as a civil servant on the PIV badge however; the IPA employee would be adjudicated under an equivalent to 5 C.F.R pt.731 and not the same adjudicative criteria as a civil servant would be adjudicated for suitability.

3.1.2 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. Personal services contracts;

b. Contracts between any non-federal entity and another non-federal entity to perform work related to the primary contract with the agency

c. 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 Office of Personnel Management appointing authorities.

3.1.3. NASA determines the fitness of contractor employees to perform work as contractor employees, prior favorable fitness or suitability determinations should be granted reciprocal recognition, to the extent practicable. Per Exec. Order No. 13488, there is no requirement that the prior favorable fitness or suitability determination must have been made within a specific time period. However, there must be no break in employment since a favorable determination was made. Exec. Order No. 13488 gives NASA the authority to grant reciprocal recognition to prior favorable fitness or suitability determinations made by other agencies.

3.1.4. Individuals covered by Exec. Order No. 13467 who perform work for or on behalf of the agency are subject to a background investigation 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; or

e. fit to perform work for or on behalf of the Government as a contractor employee.
3.4.1. a, b, and e apply to NASA contractor employees.

3.1.5. An appointment will not be subject to investigation when the person being appointed has undergone a background investigation 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 1 year in a covered position subject to investigation.

b. Transfer to a covered position, provided the person has been serving continuously for at least 1 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 1 year where the person has been determined fit for appointment based on criteria equivalent to the factors provided at 5 C.F.R. §731.202; or

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 1 year in a job where the Federal agency determined the contract employee was fit to perform work on the contract based on criteria equivalent to the factors provided in 5 C.F.R. § 731.202

3.1.5.1. 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 under 5 C.F.R. §731.202.

3.1.5.2. Reinvestigation requirements under 5 C.F.R. § 731.202 for public trust positions are not affected by this section.

3.1.6. 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/CPS shall coordinate with the Center OHCM 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 shall be coordinated with the Center OHCM or respective Detaille's official Agency personnel office for resolution.

3.1.7. 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.

3.2 Childcare Providers

3.2.1. Child Care National Agency Checks with Inquiries (CNACI) are to be completed on all childcare providers prior to working in NASA-sponsored childcare facilities (See, OPM Federal Investigations Notice #98-06, Subject: "Child Care Provider Investigations"). Centers shall use the services of OPM to conduct these investigations.

3.2.2. If there is a pressing operation need, personnel shall work under regular and continuous observation by a favorably adjudicated employee pending completion of the CNACI on the observed individual.

3.2.3. NASA childcare centers shall coordinate all personnel hiring actions with the Center Security Office prior to entry on duty. NASA childcare center management may NOT override these requirements.

3.3 Public Trust Positions

3.3.1. Positions at the high or moderate risk levels are designated 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 position involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain.

3.4 Designation of Risk Levels

3.4.1 Risk level designations for contracts, grants, cooperative agreements, and MOA or MOU shall be made by the NASA Center program office representative (typically the designated Civil Service project manager (sponsor), COTR, in coordination with the CCS/CPS, and IT Security Manager(s).

3.4.2 The risk level is determined by evaluating the sensitivity and risk of the work being performed and accesses 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 level that will ultimately be applied to the system and or application when deployed.

3.4.3 All access factors (i.e., Center, facility, information, and IT systems) must 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 risk level designation (IT = High Risk designated position compared against that same individual's need to access uncontrolled areas of the Center = Low Risk) is the designation for which the appropriate investigation will be conducted.

3.4.4. The risk level should be determined in the statement of work of the contract and it determines the investigative requirements for the contractor employee who shall perform the work.

3.4.5. Fitness determinations will be conducted for contractor employees per contractual requirements.

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

3.5 HIGH RISK: Is a Public Trust Position.

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 broad scope of policy or program authority.

3.6. MODERATE RISK: Is a Public Trust Position.

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.

3.7 Low Risk Low Risk positions are those that have the potential for impact involving duties of limited relation to the Agency mission with program responsibilities with 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. Positions designated at the Low Risk level are not considered Public Trust positions.

3.7.1. Positions that do not fall in the categories High or Moderate 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

3.7.2. In instances where there is a wide variance in the security risk level of the work to be performed, individual contractor employees must be processed at the risk designation commensurate with the highest risk level of their duties. In meeting this contingency, the contract, grant, MOA, or MOU must specifically apply controls to ensure that work of the lower risk positions does not overlap with that for the higher risk positions.

3.7.3. The contracting officer shall identify the employees to be processed at each risk level designation and shall specify the duties of the contractors. An example of such a case is custodial work, where some NASA contractor employees may work unmonitored during working hours, in a building which houses classified information, or in a facility designated as Mission Essential Infrastructure (MEI) or other restricted area that requires a higher degree of trust.

3.7.4. The entire contract, grant, MOA, or MOU may be designated High or Moderate Risk due to the former case, but those NASA contractor employees whose work would be Moderate or Low Risk must be investigated accordingly.

3.7.5. The contractor and COTR must specify control measures to be used to ensure that there is no overlap of work duties between the lower designated positions.

3.7.6. Non-U.S. citizens (including LPR) are eligible for placement in Low and Moderate risk positions, but are not normally eligible for employment in positions designated as High Risk. Under specific situations the AA for Protective Services 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 shall submit a written request to the AA for Protective Services via the CCS/CPS. The request shall:

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.

3.7.7 The CCS/CPS shall review the request for accuracy, endorse or non-endorse it, and forward it to the AA for Protective Services.

3.7.8 The AA for Protective Services shall coordinate with the Office of International and Interagency Relations for concurrence, and if approved, shall return it to the requestor. A copy shall be retained in the OPS and center security office files.

3.8 Lautenberg Amendment

3.8.1. 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 30 September 1996. The amendment makes it a felony for those convicted of misdemeanor crimes of domestic violence to shop, 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.

3.9 Personnel Security Background Investigations Requested by NASA

3.9.1 NASA will comply with OPM standards for requesting background investigations. Use the chart to select the appropriate investigation.

For this Position Designation:	**You will use this request format:**	**To request this investigation:**
Risk/Sensitivity Level	**Standard Forms**	**You will use the following OPM Investigative Products**
Non-Sensitive Position Low Risk/HSPD-12 Credential	SF 85 (Questionnaire for Non Sensitive Positions) OF 306	National Agency Check and Inquiries (NACI)
Moderate Risk Public Trust Position (No national security sensitivity)	SF 85P (Questionnaire for Public Trust Positions) OF 306	Moderate Risk Background Investigation (MBI) (Limited Background Investigations (LBI) will be eliminated. After October 1, 2010 requests for LBI will be converted to MBI.)
High Risk Public Trust Position (No national security sensitivity)	SF 85P (Questionnaire for Public Trust Positions) OF 306	Background Investigation (BI) (Public Trust Special Background Investigations (PTSBI) will be eliminated. After October 1, 2010 requests for PTSBI will be converted to BI.)
Secret/Confidential (Undesignated – e.g. Military/Contractor)	SF86 (Questionnaire for National Security Positions)	National Agency Check with Law and Credit (NACLC)
Noncritical-Sensitive Position and/or Secret/Confidential Security Clearance (Low Risk)	SF 86 (Questionnaire for National Security Positions)	Access National Agency Check and Inquiries (ANACI)
Noncritical-Sensitive Position and/or Secret/Confidential Security Clearance (Moderate Risk)	SF 86 (Questionnaire for National Security Positions)	Moderate Risk Background Investigation (MBI)
Critical-Sensitive Position and/or Top Secret (TS) Security Clearance (Any level of risk)	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)
Special-Sensitive Position and/or TS Security Clearance with Sensitive Compartmented Information (SCI) (Any level of risk)	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)
Position Sensitivity (any level) with High Risk Public Trust	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)

3.9.2 If a required investigation is determined to not have been accomplished during a routine audit or review for an employee the CCS/CPS must ensure the appropriate investigation is conducted.

a. The sponsoring NASA program shall provide NASA security offices with necessary funding to accomplish the required investigations.

b. The sponsor shall notify the OHCM personnel for civilian employees and the CCS/CPS for contractor employees, a background investigation will be initiated for the subject in e-QIP if required.

3.9.3. The NASA employee shall submit a fingerprint and complete and submit the electronic forms in e-QIP, and sign the appropriate release pages.

3.9.4. 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. Based on the specifics of the situation and a preliminary review of the fingerprint results and submitted forms, the CCS/CPS shall advise the sponsor whether the individual can commence working prior to the receipt of the completed investigation and final access determination.

3.9.5. Pre-assignment Checks for **High Risk** Positions.

3.9.5.1. Upon selection, but prior to assignment, a check will be performed to determine if an appropriate investigation has already been completed and favorably adjudicated that will serve; or a background investigation is initiated for the employee in e-QIP.

3.9.5.2. Upon review of information in the completed e-QIP, the reviewer may:

a. Request additional information from the subject and conduct screening to resolve any issues that are found during the review process; or,

b. Release the electronic form to the e-QIP Approver to transmit the investigation to the investigation provider and await final results; or,

c. Grant interim authority to access a NASA Center pending receipt of completed investigation and final access approval determination; or,

d. Deny access and take the necessary actions.

3.10 Investigation and reinvestigation Requirements for NASA Contractor employees without access to CNSI

3.10.1. Contractor employees performing low risk work will submit a National Agency Check with Inquiries (NACI) in e-QIP on a SF 85 with a finger print card (FD 258). Contractor employees are not required to submit an application or resume. However, investigations requested on the SF 85 require the applicant to answer specific questions found on the OF 306 (2001 version): 1, 8, 9, 10, 11, 12, 13, 16, and 17a. To provide that additional information, the OF 306 may be used, or the specific questions and answers may be provided on an attachment to e-QIP. Reinvestigations for low risk contractor employees will be a NACI with a FD 258 fingerprint card every ten years or sooner if determined by the governance agency.

3.10.2. Contractor employees performing moderate risk work will submit a Minimum Background Investigation (MBI) in e-QIP on a SF 85P and a fingerprint card (FD 258). Reinvestigations with be performed every five years on a National Agency Check with Law and Credit with a fingerprint card (FD 258).

3.10.3. Contractor employees performing high risk work with no access to CNSI will submit a Background Investigation (BI) in e-QIP on a SF85P with a fingerprint card (FD 258). Reinvestigations will be performed every five years with a Periodic Reinvestigation (PRI) with a fingerprint card (FD 258).

3.10.4. 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 initiated within 14 calendar days after the promotion or reassignment is final.

3.11 Individuals with Prior Criminal Record

3.11.1 Individuals with a criminal record (except minor traffic) will be adjudicated in accordance with "Memorandum to Heads of Departments and Agencies, Chief Human and Security Clearance Decision Making Guide".

a. If an individual is still under probation/parole or incarcerated for a felony conviction, this alone serves as an immediate disqualifying factor for physical/logical access based on the unacceptable risk the criminal activity poses to a NASA. A felony is defined as a serious crime which in the US is usually punishable upon conviction either by a large fine, or by a term of imprisonment longer than one year, or by both a large fine and imprisonment, or which is punishable by death. The PIV Authorizer will notify the PIV Sponsor that processing has been suspended.

b. At such a time as the hearing, trial, criminal prosecution, sentencing, suspended sentencing, deferred sentencing, incarceration, probation, or parole has been completed; the individual may be resubmitted to the identity verification process to determine eligibility for a credential.

3.11.2 If the CCS/CPS determines that access is justified based on compelling mitigating factors, then the investigative records and a signed memorandum containing a full justification for favorable consideration will forwarded to the AA for Protective Services.

a. The AA for Protective Services via the NASA CAF, in consultation with the Headquarters (HQ) Office of General Counsel (OGC), makes the final determination and forwards the results to the Center Chief of Security.

b. Physical or logical access PIV credentials may not be granted until approval is acted upon by the AA for Protective Services.

3.12 Adverse Information

3.12.1. 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. A determination must be made that the employee is fit to perform work for or on behalf of the Government and/or eligible for logical and physical access in accordance with Exec. Order No. 13467.

3.12.1.1. These expanded inquiries shall be conducted by a NASA security 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.

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

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

3.12.2. 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 or the NASA Office of Protective Services.

3.12.3. A personal interview or expanded inquiry shall be held with 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.

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

3.12.3.2 Agency officials may conduct a new fitness or suitability 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 background investigation or database query and adjudication

3.13 Reciprocity of other agency Adjudications and Adjudication Process for Contractor Employees

3.13.1. A check will be made of OPM's Central Verification System (CVS) by a NASA trusted information provider who has undergone a favorably adjudicated background investigation 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 background investigation that will serve reciprocally, a background investigation will be initiated in e-QIP for the contractor employee commensurate to the risk level associated with the work of the contract.

3.13.2. Reciprocal recognition of fitness will be granted to a prior favorable fitness or suitability determination when:

a. equivalent adjudicative criteria was used (5 C.F.R. pt. 731 for federal employees) and (OPM's Final Credentialing Standards for issuing Personal identity Verification Cards under HSPD-12 of 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.

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

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

b. an agency obtains new information that calls into question the individuals fitness based on character or conduct; or

c. the individuals investigative record shows conduct that is incompatible with the core duties of the new position

3.13.3.1. To ensure alignment for purposes of fitness and suitability, a core duty is a continuing responsibility that is of a particular importance to the achievement of NASA's mission.

3.13.4. OPM's Final Credentialing Standards will be used by trained adjudicators when determining eligibility for physical and logical access only. PIV Authorizers must 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:

a. The individual is known to be or reasonably suspected of being a terrorist;

b. The employer is unable to verify the individual's claimed identity;

c. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;

d. 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;

e. There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or

f. 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.

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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

m. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

3.13.5. Examples of equivalent criteria include the disqualification factors provided at 5 C.F.R. §301.203 regarding the disqualifying of an excepted service applicant for employment. The following may be included as disqualifying reasons**:**

a. Dismissal from employment for delinquency or misconduct;

b. Criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct;

c. Intentional false statement or deception or fraud in examination or appointment;

d. Habitual use of intoxicating beverages to excess;

e. Reasonable doubt as to the loyalty of the person involved to the Government of the United States;

f. Any legal or other disqualification which makes the individual unfit for service; or

g. Lack of United States citizenship.

3.13.6. For the purpose of this adjudicative policy, the “whole person concept” is defined by those eligible for physical and logical access shall be granted for 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 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. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

a. the nature, extent, and seriousness of the conduct;

b. the circumstances surrounding the conduct, to include knowledgeable participation;

c. the frequency and recency of the conduct;

d. the individual's age and maturity at the time of the conduct;

e. the extent to which participation is voluntary;

f. the presence or absence of rehabilitation and other permanent behavioral changes;

g. the motivation for the conduct;

h. the potential for pressure, coercion, exploitation, or duress; and

i. the likelihood of continuation or recurrence

3.13.7. Adjudicators will use the OPM's Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide, January 14, 2008 as a resource for deriving a reasonable conclusion or decision based on the standards outlined in OPMs' Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD -12. Adjudicators will not add or delete or modify the adjudicative standards. Final adjudications will be performed within twenty days from receipt of a Report of Investigation (ROI) from OPM. The investigation closing date and adjudicative action will be recorded in IdMAX, OPM form INV 79A or electronically annotated in OPM PIPS under Agency Menu as soon as possible after adjudication. Batch files from IdMAX may also be uploaded into OPM's PIPS system.

3.14 Reconsideration Procedures for Contractor Employees and other Agency Affiliates

3.14.1 Notice of Proposed Action - When an adjudicator determines that a PIV applicant has not provided his or her true identity or is otherwise not suitable 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 individual has been determined to not have provided his or her true identity or is otherwise unsuitable. The notice shall 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 shall inform the individual of the time limits (usually 10 days for response), as well as the address to which such response should be made.

3.14.2 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.

3.14.3 Decision – After consideration of the determination and any documentation submitted by the PIV applicant for reconsideration of the initial determination, the Center Chief of Security or his/her designee will issue a written decision (usually within 10 days), which informs the PIV applicant of the reasons for the decision.

3.14.4 Reconsideration – If a denial letter is provided and the subject subsequently requests an appeal, the Center Chief of Security /Chief of Protective Services shall appoint a panel to review the Credentialing Adjudication Review Panel (CARP) surrounding the denial or revocation. The panel shall be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members must have been the subjects of a favorable background investigation, and only one of the panel members shall 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 shall be documented by means of a written summary or recording which shall not be made a part of the subject's security record.

3.14.5 Prior to finalizing the CARP determination, a CARP panel member or the center Chief of Security 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.

3.14.6 Upon determination that a clearance revocation or 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 will reflect any debarments to the center based on denial or revocation of PIV.

Appendix A. Definitions

A.1 Access - The ability to obtain and use information and related information processing services; and/or enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances)

A.2 Adjudication - A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, fit to perform work for or on behalf of the Government as a contractor employee or access to NASA facilities, information, or IT resources, is in the best interest of National security or efficiency of the Government.

A.3 Asset - A system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

A.4 Automated Record Checks (ARC) – A centralized and integrated set of information technology (IT) services to request, collect, and validate electronically accessible, adjudicative-relevant data using the most efficient and cost-effective technology and methods available. ARC are a lawfully acceptable replacement of legacy and non-automated record checks. Ultimately, ARC entails fully automatic machine-to-machine interaction to request, collect, and validate machine-readable data and inform subsequent steps in an end-to-end electronic case management system.

A.5 Center Chief of Security (CCS) - The senior Center security official who is responsible for management of the Center security program.

A.6 Central Adjudication Facility - Facility established at the Security Management Division level responsible for adjudicating all requests for clearances to access CNSI.

A.7 Certification - A formal process used by the Certifying Official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

A.8 Classified Material - Any physical object on which is recorded, or in which is embodied, CNSI that shall be discerned by the study, analysis, observation, or other use of the object itself.

A.9 Classified National Security Information (CNSI) - Information that must be protected against unauthorized disclosure in alignment with Exec. Order No. 12938, "Classified National Security Information," as amended, and is marked to indicate its classified status when in documentary form. See definition for "Classification Category" above.

A.10 Cohabitant – an individual with whom the Subject resides in a spouse-like relationship.

A.11 Compromise - The improper or unauthorized disclosure of or access to classified information.

A.12 Continuous Evaluation – Reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial and Government databases and other lawfully available information) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information

A.13 Contractor Employee - For the purpose of this NID, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology; an expert or consultant (not appointed under section 3109 of title 5, United States Codes) to any agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors, a personal services contractor, or any other category of person who performs work for or on behalf of any agency (but not a Federal employee). In order to perform the work specified under the contract, will require access to space, information, information technology systems, staff or assets of NASA.

A.14 Core Duty – means a continuing responsibility that is of a particular importance to the relevant covered position or the achievement of an agency's mission

A.15 Corroborate – Comparing information from any investigative source with that provided by the Subject to confirm the information or identify discrepancies.

A.16 Covered individual – a person who performs work for or on behalf of the executive branch, or show seeks to perform work for or on behalf of the executive branch, but does not include the President or Vice President

A.17 Covered Positions -define the types of government jobs subject to 5 C.F.R. pt. 731 procedures. These positions are as follows: position in the competitive service; positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service.

A.18 Credential – A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials are presented to access control systems in order to gain access to assets

A.19 Critical-Sensitive (CS) - One of the three levels for designating National security-related positions and the degree of risk involved. Includes any position involving access to TOP Secret information; investigative requirements for this position are covered under NSD-61.

A.20 Debarment – A determination by the Agency or OPM to prohibit an applicant or appointee from being examined for or appointed to a Federal position for a period of up to 3 years..

A.21 Denial - The adjudication that an individual's initial access to classified information would pose a risk to National security, after review procedures set forth in Exec. Order No. 12968 have been exercised.

A.22 Enhanced Subject Interview – An in-depth discussion between a trained and certified investigator and the Subject conducted as a required part of an investigation, or to offer the Subject an opportunity to explain refute, or mitigate issue or discrepant information.

A.23 Electronic Questionnaires for Investigation Processing System (e-QIP) – A web-based tool for self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct investigations

A.24 Excepted service – those positions: (a) not in the competitive service, (b) not in the Career Senior Executive Service, and (c) not in the intelligence community unless covered by OPM appointing authorities.

A.25 Executive Order – (Exec. Order) Official documents, numbered consecutively, through which the President of the United States manages the operation of the Federal Government.

A.26 Federally Controlled Facility – has meaning prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107-347 and Homeland Security Presidential Directive 12)

A.27 Fitness – The level of character and conduct determined necessary for an individual to perform work for or on behalf of a federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee

A.28 Fitness Determination – a decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than in an excepted service position subject to suitability) or as a contractor employee.

A.29 Foreign National - For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States including lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee status to the United States. See definition of Lawful Permanent Resident (LPR) in this Chapter.

A.30 Formerly Restricted Data (FRD) - Information developed by the Department of Energy (DOE) related to National Nuclear programs with strict access restrictions "Restricted Data (RD)" but that has subsequently been downgraded to a lower level of control and accountability.

A.31 Immediate family - The spouse, parents, siblings, children, and cohabitant of the Subject. This includes any step parents, half and step siblings, and step children of the Subject

A.32 Information Technology System (ITS) - An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

A.33 Intelligence Community - The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services; the Federal Bureau of Investigation; the Department of Homeland Security; the Department of the Treasury; the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

A.34 Intergovernmental Personnel Act (IPA) - Individuals on temporary assignments between Federal agencies and State, local, and Indian Tribal Governments, institutions of higher education, and other eligible organizations.

A.35 Investigative Record – The official record of all data obtained on the Subject from Trusted Information Providers, from suitability and/or security applications and questionnaires, and any investigative activity conducted under federal standards

A.36 Lawful Permanent Resident (LPR) - Replaces the term "Permanent Resident Alien (PRA)" - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 C.F.R. pt.7, §7.4), and access to classified national security information. (NOTE: LPR's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign Nationals under immigration laws.)

A.38 Logical Access – Access to information records, data, information technology systems and applications

A.39 NASA Employee - NASA Civil Service personnel.

A.40 National Security Positions - Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

a. Confidential - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

b. Secret - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

c. Top Secret - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

A.41 Nondisclosure Agreement - Standard Form 312 (SF 312) is a non-disclosure agreement required under Exec. Order No.13292 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the Information Security Oversight Office of the National Archives and Records Administration and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. The SF 312 replaces the earlier forms SF 189 or the SF 189-A. Enforcement of SF-312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion or removal, in addition to the likely loss of the security clearance."

A.42 Periodic Reinvestigation (PRI) - The PRI consists of a National Agency Check, a credit search, a Personal Subject Interview, selected record searches (for example, law enforcement, personnel security files, and official personnel files (OPF)). Coverage is for a 3-year period. A PRI is required for all High Risk positions.

A.43 Permanent Resident Alien (PRA) - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 3 C.F.R. pt. 7, § 7.4), and access to classified national security information. (NOTE: PRA's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign Nationals under immigration laws.)

A.44 Physical Access – Access to federally controlled facilities, other than on an occasion or intermittent basis.

A.45 Position Designation – The assessment of the potential for adverse impact on the efficiency and integrity of the service, and the degree to which, by the nature of the position, the occupant could bring about a material adverse effect on the national security.

A.46 Position Sensitivity – The designation of the level of risk associated with a position

A.47 Public Trust - Public Trust positions has the meaning provided in 5 C.F.R. pt 731.

A.48 Reciprocity - The reciprocal recognition of suitability or fitness determinations is intended to simplify and streamline investigative and adjudicative processes where prior determinations are based on equivalent investigations and adjudicative criteria. Reciprocity limits the need to conduct a new fitness determination when an individual moves, without a break in employment, from a pso9tion in the Federal government to an excepted service or contractor position, or from a contractor position to an excepted service position or anther contractor employee position

A.49 Revocation - The removal of an individual's eligibility to access classified information based upon an adjudication that continued access to classified information poses a risk to national security and after review procedures set forth in Exec Order No, 12968 have been exercised.

A.50 Risk Acceptance - An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate a risk.

A.51 Risk Assessment - The process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

A.52 Risk Management - A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

A.53 Security Clearance - A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to National security.

A.54 Security Violation - an act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (for example, loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; security area violations). (NOTE: Does not include incidents of criminal activity, theft, assault, DUI and others)

A.55 Senior Management Official - Agency or Center management personnel at Division Chief or higher level.

A.56 Sensitive Compartmented Information (SCI) - Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

A.57 Special Access Program (SAP) - Any program established and approved under Exec. Order No. 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

A.58 Suitability A determination based on an individual's character or conduct that may impact the efficiency of the service.

A.59 Suspension - The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

A.60 Trusted Information Provider – An authorized individual working for or on behalf of the Government who may contact references or otherwise corroborates or verifies Subject data, such as citizenship, education and former employment. These individuals may include Government

and contract employees or military personnel, working in human resources or security offices, or equivalent organizations

A.61 Unauthorized Disclosure (Exec. Order No. 12958) - A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

A.62 Verification – Validating at the actual source (an individual or place of record – such as employers, courts, law enforcement agencies – or their authorized repositories) the correctness and accuracy of information listed on the e-QIP/e-Application or provided by the Subject or references to the Trusted Information Provider

A.63 Waiver - The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

APPENDIX B. Acronyms

CAF - Central Adjudication Facility

CCS - Center Chief of Security

CPS – Chief of Protective Services

CEP - Continuous Evaluation Program

CNSI - Classified National Security Information

CS - Critical-Sensitive

DAA - Designated Approving Authority

SMD - Director, Security Management Division

e-QIP - Electronic Questionnaires for Investigation Processing

FRD - Formerly Restricted Data

OHCM - Office of Human Capital Management

IPA - Intergovernmental Personnel Act

ITAR - International Traffic in Arms Regulation

ITS - Information Technology System

LPR - Lawful Permanent Resident

MBI - Minimum Background Investigation

NAC - National Agency Check

NCI - NASA Critical Infrastructure

NCIPP - NASA Critical Infrastructure Protection Program

OPS - Office of Protective Services

PIV - Personal Identity Verification

PPO - Program Protection Office
PRA - Permanent Resident Alien

PRI - Periodic Reinvestigation

SAP - Special Access Program

SCI - Sensitive Compartmented Information

APPENDIX C. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

Issued by President George W. Bush on December 29, 2005

1. *Introduction.* The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitment to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

2. *The Adjudicative Process*

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent, and seriousness of the conduct;

(2) the circumstances surrounding the conduct, to include knowledgeable participation;

(3) the frequency and recency of the conduct;

(4) the individual's age and maturity at the time of the conduct;

(5) the extent to which participation is voluntary;
(6) the presence or absence of rehabilitation and other permanent behavioral changes;

(7) the motivation for the conduct;

(8) the potential for pressure, coercion, exploitation, or duress; and

(9) the likelihood of continuation or recurrence.

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.

(c) The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(1) Guideline A: Allegiance to the United States

(2) Guideline B: Foreign Influence

(3) Guideline C: Foreign Preference

(4) Guideline D: Sexual Behavior

(5) Guideline E: Personal Conduct

(6) Guideline F: Financial Considerations

(7) Guideline G: Alcohol Consumption

(8) Guideline H: Drug Involvement

(9) Guideline I: Psychological Conditions

(10) Guideline J: Criminal Conduct

(11) Guideline K: Handling Protected Information

(12) Guideline L: Outside Activities

(13) Guideline M: Use of Information Technology Systems

(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a

recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) voluntarily reported the information;

(2) was truthful and complete in responding to questions;

(3) sought assistance and followed professional guidance, where appropriate;

(4) resolved or appears likely to favorably resolve the security concern;

(5) has demonstrated positive changes in behavior and employment;

(6) should have his or her access temporarily suspended pending final adjudication of the information.

(f) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Guideline A: Allegiance to the United States

1. *The Concern.* An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

2. *Conditions that could raise a security concern and may be disqualifying include:*

(a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;

(b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

(1) overthrow or influence the government of the United States or any state or local government;

(2) prevent Federal, state, or local government personnel from performing their official duties;
(3) gain retribution for perceived wrongs caused by the Federal, state, or local government;

(4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

3. *Conditions that could mitigate security concerns include:*

(a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(b) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(c) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(d) the involvement or association with such activities occurred under such unusual circumstances, or so much times has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

Guideline B: Foreign Influence

6. *The Concern.* Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

7. *Conditions that could raise a security concern and may be disqualifying include:*

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;
(d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) failure to report, when required, association with a foreign national;

(g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

8. *Conditions that could mitigate security concerns include:*

(a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;

(c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;
(d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

(e) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country;

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

Guideline C: Foreign Preference

(9) The Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

(10) Conditions that could raise a security concern and may be disqualifying include:

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) possession of a current foreign passport;

(2) military service or a willingness to bear arms for a foreign country;

(3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;

(4) residence in a foreign country to meet citizenship requirements;

(5) using foreign citizenship to protect financial or business interests in another country;

(6) seeking or holding political office in a foreign country;

(7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

(11) *Conditions that could mitigate security concerns include:*

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) the individual has expressed a willingness to renounce dual citizenship;

(c) exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) use of a foreign passport is approved by the cognizant security authority;

(e) the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated;

(f) the vote in a foreign election was encouraged by the United States Government.

Guideline D: Sexual Behavior

13. *The Concern.* Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in the Guideline may be raised solely on the basis of the sexual orientation of the individual.

14. Conditions that could raise a security concern and may be disqualifying include:

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(d) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

15. *Conditions that could mitigate security concerns include:*

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(c) the behavior no longer serves as a basis for coercion, exploitation, or duress;

(d) the sexual behavior is strictly private, consensual, and discreet.

Guideline E: Personal Conduct

16. *The Concern.* Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. Conditions that could raise a security concern and may be disqualifying also include:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness

to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

17. Conditions that could mitigate security concerns include:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors

that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) association with persons involved in criminal activities has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Guideline F: Financial Considerations

18. *The Concern.* Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

19. *Conditions that could raise a security concern and may be disqualifying include:*

(a) inability or unwillingness to satisfy debts;

(b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) a history of not meeting financial obligations;

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern.

(g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

20. *Conditions that could mitigate security concerns include:*

(a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

(c) the person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control;

(d) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) the affluence resulted from a legal source of income.

Guideline G: Alcohol Consumption

21. *The Concern*. Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

22. Conditions that could raise a security concern and may be disqualifying include:

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;
(d) diagnosis by a duly qualified medical professional (physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

23. *Conditions that could mitigate security concerns include*:

(a) so much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);

(c) the individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;

(d) the individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

Guideline H: Drug Involvement

24. *The Concern.* Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(a) Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and (2) inhalants and other similar substances;

(b) drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

25. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Any drug abuse (see above definition);

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

26. *Conditions that could mitigate security concerns include:*

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) dissociation from drug-using associates and contacts;

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation;

(c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

Guideline I: Psychological Conditions

27. *The Concern.* Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

28. Conditions that could raise a security concern and may be disqualifying include:

(a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;

(c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, failure to take prescribed medication.

29. *Conditions that could mitigate security concerns include:*

(a) the identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;

(b) the individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;

(c) recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;

(d) the past emotional instability was a temporary condition (one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;

(e) there is no indication of a current problem.

Guideline J: Criminal Conduct

30. *The Concern.* Criminal activity creates doubt about a person's judgment, reliability and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

31. Conditions that could raise a security concern and may be disqualifying include:

(a) a single serious crime or multiple lesser offenses;

(b) discharge or dismissal from the Armed Forces under dishonorable conditions;

(c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) individual is currently on parole or probation;

(e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

32. *Conditions that could mitigate security concerns include:*

(a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;

(c) evidence that the person did not commit the offense;
(d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

Guideline K: Handling Protected Information

33. *The Concern.* Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

34. Conditions that could raise a security concern and may be disqualifying include:

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) collecting or storing classified or other protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, game board, handheld, "palm" or pocket device or other adjunct equipment;

(d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need to know;

(g) any failure to comply with rules for the protection of classified or other sensitive information;

(h) negligence or lax security habits that persist despite counseling by management;

(i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

35. *Conditions that could mitigate security concerns include:*

(a) so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training.

Guideline L: Outside Activities

36. *The Concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. *Conditions that could raise a security concern and may be disqualifying include:*

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;

(3) a representative of any foreign interest;

(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) failure to report or fully disclose an outside activity when this is required.

38. *Conditions that could mitigate security concerns include:*

(a) evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) the individual terminates the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

Guideline M: Use of Information Technology Systems

39. *The Concern.* Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all

related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

40. Conditions that could raise a security concern and may be disqualifying include:

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

(g) negligence or lax security habits in handling information technology that persist despite counseling by management; counseling by management;
(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

41. *Conditions that could mitigate security concerns include:*

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Bloxon, Deborah F. (HQ-LP030)

From: Bloxon, Deborah F. (HQ-LP030)
Sent: Wednesday, July 20, 2011 3:00 PM
To: 'dfbloxon@gmail.com'
Subject: RE: Requested Expedited Review of Proposed NASA Interim Directives

I am sorry this took me so long to get back to – I concur in the last set of revisions and have no further legal objection or comment.

James A. Reistrup
Senior Attorney
Office of the General Counsel
HQ NASA
300 E Street., S.W.
Washington, D.C. 20546-0001
Main (202) 358-2465
Desk (202) 358-2027
Fax (202) 358-4355

From: Dodson, Michele D. (HQ-ED000)
Sent: Wednesday, June 15, 2011 9:30 AM
To: Matthews, Lakeesha S (HQ-LP021)
Subject: Fw: Requested Expedited Review of Proposed NASA Interim Directives

Procurement
--Sent via BlackBerry

From: POWERS, MICHAEL L. (GSFC-1800)
To: Ebron, Enzie M. (HQ-IP000); Dodson, Michele D. (HQ-ED000); Burns, Laura (HQ-MA000)
Cc: Bloxon, Deborah F. (HQ-LP030); Meredith, Shelley J. (HQ-IM030)
Sent: Tue May 24 13:35:35 2011
Subject: RE: Requested Expedited Review of Proposed NASA Interim Directives

Hi Michelle,

I just finished reviewing the two proposed directives. OP concurs to the proposed directives.

Thanks Mike

From: Ebron, Enzie M. (HQ-IP000)
Sent: Tuesday, May 24, 2011 2:29 PM
To: Dodson, Michele D. (HQ-ED000); Burns, Laura (HQ-MA000); POWERS, MICHAEL L. (GSFC-1800)
Cc: Bloxon, Deborah F. (HQ-LP030); Meredith, Shelley J. (HQ-IM030)
Subject: RE: Requested Expedited Review of Proposed NASA Interim Directives

Hi Michelle:

The OCFO concurs

From: Dodson, Michele D. (HQ-ED000)
Sent: Friday, May 20, 2011 9:33 AM
To: Burns, Laura (HQ-MA000); Ebron, Enzie M. (HQ-IP000); POWERS, MICHAEL L. (GSFC-1800)
Cc: Bloxon, Deborah F. (HQ-LP030)
Subject: RE: Requested Expedited Review of Proposed NASA Interim Directives
Importance: High

Hello to all,

OPS requested your response to the action below by yesterday. Please let me know if your office concurs or have any comments to submit. Although OPS is attempting to meet a deadline that is fast approaching, please contact me ASAP if you need to request additional time.

Thanks.

Michele D. Dodson
Aeronautics Resource
Management Office (ED000)
ofc: 6D52
ph: 202.358.1049
pda: 202.420.8386
fax: 202.358.3238
mdodson@nasa.gov

From: Dodson, Michele D. (HQ-LP021)
Sent: Monday, May 16, 2011 11:56 AM
To: Burns, Laura (HQ-MA000); Ebron, Enzie M. (HQ-IP000); Schuffert, Tiffany (HQ-LE050); POWERS, MICHAEL L. (GSFC-1800)
Cc: Bloxon, Deborah F. (HQ-LP030)
Subject: Requested Expedited Review of Proposed NASA Interim Directives
Importance: High

Requested Review Offices:
Office of the Chief Financial Officer
Office of the General Counsel
Office of Human Capital Management
Office of Procurement

Hello to all,

The Office of Protective Services (OPS) requests your office's review of the attached policies:

1. NASA Personnel Security and
2. NASA Identity and Credential Management.

OPS intends to issue these documents as NASA Interim Directives in order to meet required critical certifications and system accreditations. These certifications and accreditations cannot occur until

some policy is in place. Due to the exigent circumstances, the drafts are to be approved as NIDs and then concurrently worked for submission to the official NODIS review no later than July 2011.

OPS requests an expedited review. Please review the attached and return comments to me on Thursday, May 19, 2011. Please contact me if there are any questions or concerns.

Thank you for your assistance with this action and your understanding with this short turn around.

Michele D. Dodson
ofc: 6D52
ph: 202.358.1049
pda: 202.420.8386
fax: 202.358.3238
mdodson@nasa.gov

Bloxon, Deborah F. (HQ-LP030)

To: Matthews, Lakeesha S (HQ-LP021)
Subject: RE: NPR/NID

From: Jennings, Nanette (HQ-LP030)
Sent: Thursday, June 16, 2011 9:51 AM
To: Vanarsdel, Catherine V. (HQ-LP021)
Cc: Matthews, Lakeesha S (HQ-LP020); Parker, Cheryl E. (HQ-LP030); Bloxon, Deborah F. (HQ-LP030)
Subject: NM 1600-XX, NID: NASA Personnel Security Procedural Requirements

Cathy,

The subject NID is awaiting OGC concurrence. As soon as they concur, my team will publish the NID to issue requirements for the Agency. Be advised that NIDs are only good for one year. Prior to leaving OPS, Michele Dodson submitted a 184 form (NPR 1600.Draft 7) to get the process started with incorporated the NID's language into an NPR. Lakeesha will assist you for the remainder of the process. So, please review the 184 form to ensure its completeness. Since the NID already received union approval, I recommend that OPS target the July schedule. When the NPR is approved, it will cancel the NID, along with Chapters 2-4 of NPR 1600.1 NASA Security Program Procedural Requirements.

Lakeesha, contact Deborah if you have questions.

Nanette Jennings
Team Lead, NASA Directives and Regulatory Program
Office of Institutions and Management, Office of Internal Controls and Management Systems
Phone: 202/358-0819
Fax: 202/358-3848
Cell: 202/631-2536
E-mail: nanette.jennings@nasa.gov

"Faith is taking the first step even when you don't see the whole staircase." MLK, Jr

---

From: Matthews, Lakeesha S (HQ-LP021)
Sent: Wednesday, July 20, 2011 3:00 PM
To: Bloxon, Deborah F. (HQ-LP030)
Subject: FW: NPR/NID

LaKeesha Matthews-Williams
NASA Headquarters

Office of Protective Services (LP020)
300 E Street, SW 9U70
Washington, DC 20546

Department: (202) 358-2010 Direct: (202) 358-4729
PDA (301) 523-1523 Fax: (202) 358-3238
E-mail: lakeesha.matthews@nasa.gov

From: Dodson, Michele D. (HQ-ED000)
Sent: Wednesday, June 15, 2011 8:39 AM
To: Schuffert, Tiffany (HQ-LE050); Matthews, Lakeesha S (HQ-LP020)
Subject: Re: NPR/NID

Great, please relay that to the OPS directives manager, because it seems that information was not relayed to her when I spoke to her yesterday. Thanks.

Lakeesha, please contact Tiffany and Nannette for further status on this NID.

--Sent via BlackBerry

From: Schuffert, Tiffany (HQ-LE050)
To: Dodson, Michele D. (HQ-ED000)
Sent: Wed Jun 15 07:17:57 2011
Subject: RE: NPR/NID

Sorry, I don't have that email any more. I was cleaning some things up and now I can't find it :/

I did talk to Nanette… so the Directive folks know what's going on and that OPS can proceed.

From: Dodson, Michele D. (HQ-ED000)
Sent: Wednesday, June 15, 2011 8:15 AM
To: Schuffert, Tiffany (HQ-LE050)
Subject: Re: NPR/NID

Yes, the NPR will be introduced as a NID. Since this needs to be sent to the directives office, can you reply to my original NID request in order to have a "clean" concurrence? I'll then forward that (and the other concurrences) to the new OPS Directives manager.

Thanks.
--Sent via BlackBerry

From: Schuffert, Tiffany (HQ-LE050)
To: Dodson, Michele D. (HQ-ED000)
Cc: Raimond, Robert W. (HQ-LP021)
Sent: Wed Jun 15 07:08:57 2011
Subject: NPR/NID

Hi Michele!

I got your voicemail and just wanted to close the loop with you on this.

We have fulfilled our obligation with Labor on the NPR. I understand the need to put this in place quickly, so you are going to introduce the NPR as an NID, correct? I believe that's what you said. If that's the case, as long as the language in the NID is EXACTLY the same as what we just finalized with labor on the NPR, you're good to go.

Hope that makes sense. If not, give me a call. My schedule is crazy today and I'm on leave the rest of the week, but if you can't get a hold of me, I'll try to call you back this afternoon.

Tiffany M. Schuffert, PMP
Workforce Management and
Development Division
Mail Suite 4O79
NASA - Headquarters
300 E Street, SW
Washington, DC 20546
202- 358- 4513
202- 358- 4164 - Fax