NASA Procedural Requirements

NPR 1600.1
Effective Date: November 03, 2004
Expiration Date: November 03, 2014

COMPLIANCE IS MANDATORY

NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

NASA Interim Directive: NASA Identity and Credential Management, NM 1600-95

Safeguarding Sensitive But Unclassified Information, NM 1600-54

NASA Interim Directive: 5.24 Sensitive But Unclassified (SBU) Controlled Information, NM 1600-55

Change History

Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 References
P.5 Cancellation

Chapter 1. Introduction

1.1 Security Responsibilities
1.2 Best Practices
1.3 Waivers and Exceptions
1.4 Violations of Security Requirements
1.5 Terms, Abbreviations, and Acronyms

Chapter 2. NASA Personnel Security Program: Requirements, Investigations, and Adjudication Process for Positions (National Security Positions) Requiring Access to Classified National Security Information (CNSI)

2.1 General

2.2 Scope
2.3 Responsibilities
2.4 Personnel Security Program Oversight
2.5 Basic Principles of Personnel Security Clearance Management
2.6 Processing Personnel Security Clearance Requests
2.7 Coding of Position Sensitivity Level Designations for National Security Positions
2.8 Temporary/Interim Access To CNSI
2.9 Access to CNSI by Non-U.S. Citizens
2.10 Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations From Other Government Agencies and Organizations
2.11 Prior Personnel Security Clearance Determinations by NASA Authorities
2.12 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)
2.13 Guiding Principles for Adjudication, Suspension, Denial, or Revocation of Personnel Security Clearances
2.14 Adjudication of Personnel Security Clearance Status
2.15 Denial or Revocation of Personnel Security Clearances
2.16 Suspension of Personnel Security Clearances
2.17 Continuous Evaluation of Personnel Security Clearance Eligibility
2.18 Classified Visits and Meetings
2.19 Recordkeeping

Chapter 3. NASA Personnel Security Program: Position Risk Designation Process, Background Investigations, and Employment Suitability Determinations for NASA Employees

3.1 General
3.2 Applicability
3.3 Responsibilities
3.4 Submitting Requests for Suitability Investigations
3.5 Position Risk Levels
3.6 Suitability Investigations
3.7 Coding of Position Risk Level on Personnel Documents
3.8 Forms Required to Request Suitability Investigations for NASA Employees
3.9 Suitability Determination Procedures for NASA Civil Service Employees
3.10 Adverse Information
3.11 Reinvestigation Requirements
3.12 Recordkeeping

Chapter 4. NASA Personnel Security Program: Risk Designation Process, Background Investigations, and Access Determinations for NASA Contractor Employees

4.1 General
4.2 Applicability
4.3 Responsibilities
4.4 Designation of Security Risk Levels

4.5 NASA Contractor Employee Position Risk Criteria and Designation Process
4.6 Contractor Coordinated Background Investigations for U.S. Citizen Employees
4.7 NASA Coordinated Personnel Security Investigations for Contractor Personnel
4.8 Forms Required for Requesting an Investigation
4.9 Adjudication Process for Access
4.10 Escort Requirements In Lieu of Completed Favorable Background Investigations
4.11 Adverse Information
4.12 Tenant Organization Personnel Access
4.13 Reinvestigation Requirements
4.14 Recordkeeping

Chapter 5 was cancelled by NPR 1600.2 on October 11, 2011

5.1 General
5.2 Responsibilities
5.3 Agency Information Security Program Data Report, SF-311
5.4 Classifying, Marking, and Declassifying CNSI
5.5 Access to CNSI
5.6 Accountability and Control of CNSI
5.7 Page Checks
5.8 Working Papers
5.9 Storage of CNSI and Material
5.10 Reproduction of CNSI
5.11 Hand Carrying and Receipting of Classified Material
5.12 Transmission of Classified Material
5.13 Release of Classified Information to Foreign Governments
5.14 Receipt System
5.15 Managing and Handling COMSEC Material
5.16 Defense Courier Service Reimbursement Program
5.17 Disposition or Destruction of Classified Material
5.18 Destruction Procedures
5.19 Security Violations and Compromise of CNSI
5.20 CNSI Meetings and Symposia
5.21 Security Container, Vault, and Strong Room Management
5.22 Classified Material is NOT Personal Property
5.23 Security Classification Reviews for NASA Programs and Projects
5.24 Sensitive But Unclassified (SBU) Controlled Information
5.25 Use, Protection, and Accountability of Department of Energy (DOE) Unclassified Controlled Nuclear Information (UCNI)

Chapter 6. Industrial Security Program

6.1 General
6.2 Department of Defense (DoD) Support
6.3 Scope
6.4 Responsibilities
6.5 Suspension, Revocation, and Denial of Contractor Access to Classified Information
6.6 Periodic Review of DD Form 254

Chapter 7. Physical Security Program

7.1 Security Control at NASA Centers
7.2 NASA Photo Identification (Photo-ID) Badge Program
7.3 NASA Photo-ID Issuance Criteria
7.4 NASA Photo-ID Color Coding
7.5 Inspection of Persons and Property
7.6 Security Areas
7.7 Facility Security
7.8 Airfield and Aircraft Security
7.9 Control and Issuance of Arms, Ammunition, and Explosives (AA&E)
7.10 Standards for Secure Conference Rooms
7.11 Threat Assessment
7.12 Threat and Incident Reporting
7.13 Reportable Incidents
7.14 NASA Security Office Special Agent Badges and Credentials (B&C)
7.15 Technical Surveillance Countermeasures (TSCM)
7.16 Dealing with Demonstrations
7.17 Threat Condition (THREATCONS) Program
7.18 Hazardous Material Security

Chapter 8. Program Security

8.1 General
8.2 Responsibilities
8.3 Acquisition Systems Protection (ASP)
8.4 NASA Critical Infrastructure and Key Resources - Mission Essential Infrastructure (MEI) Protection Program
8.5 Operations Security (OPSEC)
8.6 Risk Management Process
8.7 Special Access Programs
8.8 Secure Compartmented Information (SCI) Programs
8.9 NASA Security Program Education, Training, and Awareness
8.10 Self-Inspections

Chapter 9. Federal Arrest Authority and Use of Force Training and Certification

9.1 General
9.2 Applicability
9.3 Responsibility

Chapter 10. Glossary of Terms, Abbreviations, and Acronyms

Appendices

Appendix A - Security Policy Board (SPB) Issuance 1-97 -

Investigative Standards
Appendix B - Adjudicative Guidelines for Determining Eligibility for Access to Classified Information
Appendix C - SPB Issuance 3-97 - Investigative Standards for Temporary Eligibility for Access
Appendix D - NASA Federal Arrest Authority and Use of Force Qualifications and Training
Appendix E - NASA Firearms Qualification Courses
Appendix F - NASA Serious Incident Report Format
Appendix G - Security Area Signs
Appendix H - Identifying and Nominating NASA Assets for the NASA Mission Essential Infrastructure Protection Program (MEIPP)
Appendix I - NASA Photo-Identification Badge Standards
Appendix J - NASA Foreign National Visitor Security/Technology Control Plan Sample Template
Appendix K - NASA Security Program Statistics Format
Appendix L - NASA THREATCON Actions
Appendix M - Designation of Public Trust Positions and Investigation Requirements
Appendix N - Process Flow Chart for Determining Position Risk and Sensitivity Levels
Appendix O - Process Flow Chart for Determining Classification and/or Sensitivity Level of Program/Project Information and/or Technology

Change History
NPR 1600.1, NASA Security Program Procedural Requirements w/Change 1 (4/1/2009)

Change Number	Date	Change Description
2	4/1/2009	With the issuance of HSPD-12, Chapters 3 and 4 were corrected to remove all references to and requirements for Mission Critical Space System Personnel Reliability Program. Directive was revalidated for another 5 years.
1	11/8/2005	Administrative corrections made throughout directive.

Preface

P.1. Purpose

a. This NASA Procedural Requirements (NPR) establishes Agency-wide security program implementation requirements set forth in NASA Security Policy Directive (NPD) 1600.2, as amended.
b. This NPR prescribes NASA Security Program procedural requirements to assist NASA Centers and component facilities in executing the NASA security program to protect people, property, and information. It establishes security program standards and specifications necessary to achieve Agency-wide security program consistency and uniformity, while allowing for reasonable flexibility in implementing risk management principles, where appropriate. It also provides for the assignment of management security responsibilities.

P.2. Applicability

This NPR is applicable to NASA Headquarters and all NASA Centers including Component Facilities, the Jet Propulsion Laboratory (JPL) and other NASA Contractors, grant recipients, and other partners to the extent specified in their contracts or agreements.

P.3. Authority

42 U.S.C. 2455, 2456, 2456a, and 2473(c) - - Sections 304 and 203(c), respectively, of the National Aeronautics and Space Act of 1958.

P.4. References

a. 5 U.S.C. 552, (b)(1)-(9), Exemptions, Freedom of Information Act (FOIA).
b. 5 U.S.C. 7312, Employment and clearance, individuals removed for reasons of national security.
c. 5 U.S.C. 7511, Definitions; Application.
d. 5 U.S.C. 7512, Actions covered.
e. 5 U.S.C. 7532, Suspension and Removal.
f. 18 U.S.C. 799 Violation of Regulations of National Aeronautics and Space Administration.
g. 40 U.S.C. 1441, et seq., Computer Security Act of 1987, as amended.
h. 42 U.S.C. 13041, Child Care Worker Employee Background Checks.
i. 50 U.S.C. 435, Access to Classified Information - Procedures.
j. EO 10450, Security Requirements for Government Employees, as amended.
k. EO 12356, National Security Information, as amended.
l. EO 12829, National Industrial Security Program, as amended.
m. EO 12958, Classified National Security Information, as amended.
n. EO 12968, Access to Classified Information, as amended.
o. 5 CFR Part 731, Suitability
p. 5 CFR Part 732, National Security Positions
q. 14 CFR, Parts 1203, 1204, and 1214.
r. 22 CFR Parts 120-130, International Traffic in Arms Regulations (ITAR).
s. 32 CFR 2001, Classified National Security Information.

t. Security Policy Board (SPB) Issuance 1-97, Investigative Standards, 3/24/97.
u. SPB Issuance 2-97, Adjudicative Guidelines, 3/24/97.
v. SPB Issuance 3-97, Investigative Standards for Temporary Eligibility for Access.
w. National Security Directive (NSD) 63, Single Scope Reliability Investigation.
x. OMB Circular A-130, Security of Federal Automated Information Resources, (Appendix III).
y. Director, Central Intelligence, Directive (DCID 6/9), Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFS), November 18, 2002.
z. National Security Decision Directive (NSDD) 84, Safeguarding National Security Information (Nondisclosure Agreement), 3/11/83.
aa. NSDD-145, National Policy on Telecommunications and Automated Information Systems Security, 9/17/84.
bb. FIPS 201, Federal Information Processing Standards, "Personnel Identity Verification (PIV) of Federal Employees and Contractors."
cc. NSDD 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, 9/21/85
dd. NSDD-298, National Operational Security Program, 1/22/88.
ee. DoD-56, MOU, Defense Investigative Service and NASA, Kennedy Space Center, 5/07/87, as regards the Industrial Security Program.
ff. DoD-86, MOU, Defense Investigative Service and NASA, 12/17/90, as regards access to Defense Clearance and Investigative Index (DCII) and Larsen System.
gg. DOT/ Federal Arrest Authority, AC 108-3, Screening of Persons Carrying U.S. Classified Material.
hh. Presidential Decision Directive (PDD) 39, Counterterrorism Policy.
ii. PDD 62, Combating Terrorism.
jj. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.
kk. PDD 67, Enduring Constitutional Government and Continuity of Government.
ll. HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors
mm. Department of Justice (DOJ) Report, Vulnerability Assessment of Federal Facilities, June 1995.
nn. General Accounting Office Report (GAO-03-8), Security Responsibilities for Federally Owned and Leased Facilities, October 2002.
oo. NPD 1371.5, Coordination and Authorization of Access by Foreign Nationals and Foreign Representatives to NASA.
pp. NPD 1440.6, NASA Records Management.
qq. NPD 1660.1, NASA Counterintelligence (CI) Policy.
rr. NPD 1600.2, NASA Security Policy.
ss. NPD 2190.1, NASA Export Control Program.
tt. NPD 2810.1C, NASA Information Security Policy.
uu. NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities.
vv. NPR 1441.1, NASA Records Retention Schedules.
ww. NPR 1600.6, Communications Security Procedural Requirements.
xx. NPR 2190.1, NASA Export Control Program.
yy. NPR 2810.1, Security of Information Technology.
zz. NPD 9800.1, NASA Office of Inspector General Programs.

P.5. Cancellation

NPR 1620.1A, Security Procedural Requirements--w/Change 2

NPD 1620.2, NASA Badging System

REVALIDATED APRIL 1, 2009, ORIGINAL SIGNED BY
/S/
David A. Saleeba
Assistant Administrator for Security
and Program Protection

Chapter 1: Introduction

1.1 Security Responsibilities

1.1.1. The NASA Administrator is responsible for implementing a comprehensive and effective security program for the protection of people, property, and information associated with the NASA mission. The Administrator shall appoint an Assistant Administrator for Security and Program Protection (AA/OSPP).

1.1.2. Security is the direct, immediate, and inherent responsibility of all NASA personnel, contractors, and others granted access to NASA Centers, facilities, information and technology. General security responsibilities are set forth in this chapter. Specific procedural requirements are cited in each subsequent chapter of this NPR.

1.1.3. The AA/OSPP shall:

1.1.3.1. Oversee Agencywide implementation, integration of, and compliance with the NASA Security Program by providing executive management policy direction and ensuring, through Agencywide advocacy, adequate resources are identified and committed to accomplish the security mission in support of the overall NASA mission, NASA Strategic Plan, and National level security requirements.

1.1.3.2. In collaboration with the Chief Information Officer (CIO), develop and implement Agency Information Technology Security policy via NPD 2810 and NPR 2810, and serve as the Agency Certification and Accreditation (C&A) authority for NASA IT.

1.1.3.3. Serve as the Agency Risk Acceptance Authority (RAA) for all NASA Security Program risk management determinations that require a waiver of Agency security requirements. This does not include IT Security RAA, which falls under the CIO.

1.1.3.4. Develop and implement a program to ensure certification and accreditation of Information Technology (IT) resources identified for processing classified national security information (CNSI) and data.

1.1.3.5. Serve as the focal point for Agency Special Access Program (SAP) and Sensitive Compartmented Information (SCI) security activity.

1.1.3.6. Serve as the Agency point of contact with the intelligence community for intelligence matters and ensure development and issuance of policy and requirements related to NASA's counterintelligence program.

1.1.3.7. Ensure law enforcement and investigative activity performed in conjunction with OSPP security responsibilities at NASA installations is developed and implemented consistent with authorities granted under the Space Act, and in concert with the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.3.8. Appoint a qualified senior security professional as Director, Security Management Division (DSMD).

1.1.3.9. Serve as the Agency Critical Infrastructure Assurance Officer (CIAO) responsible for approving all Center proposals for additions and deletions to the Mission Essential Infrastructure

(MEI) Inventory List when such proposals are concurred on by the respective Mission Directorate Associate Administrator.

a. Comply with the requirements of Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.
b. Effectively collaborate with the CIO to ensure critical cyber assets are identified and included in the Mission Essential Infrastructure (MEI) inventory, as appropriate.

1.1.3.10. Establish and implement organizational standards that ensures NASA security programs are appropriately configured, properly staffed with qualified security professionals, and adequately funded to enable each NASA Center to properly and efficiently manage day-to-day security operations while allowing for transition to increased threat environments and emergency scenarios, including appropriate continuity of operations capabilities.

1.1.3.11. Develop and issue, under separate NPR, asset specific physical security vulnerability risk assessment requirements and physical and procedural security standards to ensure consistency and uniformity in application of security measures appropriate for the vulnerabilities identified.

1.1.3.12. Establish and disseminate staffing, equipment, training, and performance standards for security services contractor organizations to ensure security services obtained are professional, comprehensive, uniform, and consistent with NASA requirements.

1.1.3.13. Develop and disseminate Agency antiterrorism program standards and procedures necessary to ensure appropriate response to threats and acts of terrorism on NASA installations and component facilities.

1.1.3.14. Implement and manage procedures for certifying and obtaining accreditation of IT resources that process CNSI and data.

1.1.3.15. In coordination with the NASA Office of General Counsel, ensure development and dissemination of appropriate policy and procedures regarding use and deployment of covert surveillance equipment (CCTV, etc.).

1.1.3.16. Develop and issue interim policy and procedural requirements as necessary to address specific issues.

1.1.4. The NASA CIO is responsible for the NASA-wide Information Technology Security (ITS) program, and shall:

1.1.4.1. Provide advice and assistance to the Administrator and other Senior Management Officials to ensure that Agency ITS goals, priorities, and requirements are effectively and efficiently addressed to protect the Agency's investment in Information Technology (IT).

1.1.4.2. Develop and implement NASA IT Security policy via the issuance of IT Security Procedural Requirements, architectures, standards, and best practices. This includes common security classification schema, which contribute to open, standard, scaleable, interoperable, yet secure IT environments and assess, with the assistance of the Competency Center for ITS, the state of the Agency's ITS posture, and the effectiveness of its IT Security policies.

1.1.4.3. Except as noted in subsection 1.1.5 below, appoint Agency representatives to Federal groups concerned with ITS.

1.1.4.4. Appoint a Competency Center for IT Security (CCITS) responsible for developing ITS architectures, standards, and best practices for the Agency on behalf of the NASA CIO.

1.1.5. Director, Security Management Division (DSMD) shall:

1.1.5.1. Provide overall focus and direction for the NASA security program.

1.1.5.2. Serve as the Agency oversight official for implementation and management of the Agency Federal Arrest Authority Program and Use of Force policy in compliance with 42 U.S.C. 2456a, and 14 CFR part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

1.1.5.3. Develop and implement Agencywide policy and procedural requirements to ensure investigation activity is coordinated and/or referred to the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.5.4. Establish and maintain a Central Adjudication Activity at the Headquarters level charged with adjudicating all Agency requests for security clearances for access to CNSI.

1.1.5.5. Deny or revoke security clearances in accordance with the provisions of EO 12968 in strict accordance with due process.

1.1.5.6. Develop and promulgate, subject to coordination with and concurrence by the Office of the General Counsel (OGC), all NASA security policy and procedures.

1.1.5.7. Through periodic site visits, evaluate compliance with this NPR and overall effectiveness of the NASA security program, including effectiveness of NASA IT Security policy and procedures.

1.1.5.8. Manage the Mission Essential Infrastructure Protection Program (MEIPP).

1.1.5.9. Serve as the Senior Agency Official for implementing procedures for managing and safeguarding CNSI.

1.1.5.10. Ensure that the NASA security program operates in compliance with National security policy, homeland security program directives, and other National level regulations.

1.1.5.11. Coordinate, as appropriate, with the Office of the Chief Medical Officer on all matters related to the Mission Critical Space Systems Personnel Reliability Program screening process requiring evaluations and medical determinations from NASA or outside medical authorities.

1.1.5.12. Ensure appropriate physical security and antiterrorism construction standards are developed and published in cooperation with NASA Facilities Engineering Division personnel.

1.1.5.13. Serve as the focal point for NASA representation on all security and national security policy development forums and committees.

1.1.6. Center Directors shall:

1.1.6.1. Provide current and effective security of personnel, property, facilities, operations, and activities at NASA Centers.

1.1.6.2. Ensure the development and management, through the Center Chief of Security (CCS), of written Center specific security program policy and procedural requirements that implement, to the fullest extent possible, the requirements of this NPR.

1.1.6.3. Appoint, with coordination and concurrence of the AA/OSPP, a qualified and experienced CCS with sufficient authority and resources to accomplish National, Agency, and Center security goals and objectives. Minimum qualifications include:

a. Relevant experience in the law enforcement, military intelligence, or security professions.

b. Leadership and managerial experience at a proven level commensurate with the expectations of the CCS position.
c. Ability to obtain and maintain a Top Secret security clearance.

1.1.6.4. In accordance with this NPR, establish, fund, and maintain a comprehensive security program through the CCS. This includes:

a. Personnel, facilities, and equipment necessary to implement and sustain an effective security program.
b. Appropriate training and professional certification of security personnel, as established by the AA/OSPP.

1.1.6.5. When recommended by the CCS and Center CIAO, propose, as appropriate, Critical Infrastructure (CI) and Key Resource (KR) assets for inclusion in the Mission Essential Infrastructure (MEI) Inventory, to the Mission Directorate Associate Administrator.

1.1.6.6. Act as the Risk Acceptance Authority (RAA) for Center security program risk management determinations that do not require waiver of national security requirements.

1.1.6.7. Grant or suspend eligibility for security clearances up to and including Top Secret, with proper coordination with the NASA Central Adjudication Activity. This authority shall be delegated, in writing, to the CCS.

1.1.6.8. Appoint, in writing, a Certifying Authority (CA) responsible for certifying to the Agency Designated Approval Authority (DAA), Center IT resources identified to process classified information.

1.1.7. The CCS shall:

1.1.7.1. Act as the principal advisor and authority to the Center Director in all matters relating to the NASA security program, as established and defined in NPD 1600.2C.

1.1.7.2. With coordination and concurrence of the AA/OSPP, ensure that the Center Security Office is appropriately staffed with qualified and experienced security personnel.

1.1.7.3. To ensure continuity of operations capability, establish the necessary processes and procedures to cross-train staff into other disciplines of the Center's security program, as practical.

1.1.7.4. Develop, implement, and maintain written Center-specific security program policy and security procedural requirements that implement the requirements of this NPR.

1.1.7.5. Direct, plan, control, and evaluate the overall Center security program, regardless of the specific security discipline and processes involved.

1.1.7.6. Through periodic assessments, determine the adequacy of physical security, loss prevention, and antiterrorism programs and recommend improvements to the Center Director.

1.1.7.7. Using all available sources of intelligence information (i.e., NASA CI Program, Local Law Enforcement, NASA Office of Inspector General (OIG), other Federal agencies), continuously evaluate Center and program-level criticality and vulnerabilities, local threats, and prepare appropriate countermeasures tailored to the resources requiring protection, specifically identifying Center Critical Infrastructure and Key Resources, in coordination with the Center CIO and CIAO, for inclusion in the MEI Protection Program.

1.1.7.8. Establish priorities for the effective deployment of Center security resources and processes

during routine and emergency situations.

1.1.7.9. Direct and control Center investigative efforts related to NASA security program operations. Ensure appropriate notifications and referrals to local and supporting Federal law enforcement agencies and the NASA OIG are conducted in accordance with this NPR and established formal agreements. [NOTE: Investigations conducted under NPR 1660, NASA Counterintelligence Program Procedural Requirements, are excluded from the requirements of this NPR.]

1.1.7.10. Exercise Original Classification Authority (OCA).

1.1.7.11. Upon written approval by the AA/OSPP, perform duties as the Center Declassification Authority for all Center declassification and classification downgrading activity, as required. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management.

1.1.7.12. Initiate the appropriate personnel security investigation and grant interim security clearances up to and including Top Secret, based on information contained in the investigative request, and grant final clearance upon notification from the NASA CAF that an individual has been adjudicated and determined eligible for the clearance requested or suspend security clearances on behalf of the Center Director and the AA/OSPP.

1.1.7.13. Designate a Center Personnel Security Officer who shall:

a. Properly adjudicate all requests for interim clearances per chapter 2.
b. Properly determine contractor employee security reliability per chapter 4.
c. Successfully complete a minimum of two specified personnel security adjudication courses prior to conducting adjudications and maintain current qualifications.
d. Ensure that designated Senior Adjudicators successfully complete three specified personnel security adjudication courses, one of which must be an advanced adjudicator's course, and maintain current qualifications.

1.1.7.14. Ensure Federal Arrest Authority is properly administered at their respective Center and act as the Center Certifying Official for the authority to carry and use concealed or unconcealed firearms by security forces, both NASA civil service personnel and contractor.

1.1.7.15. Notify the OIG of all suspected criminal activity, when appropriate.

1.1.7.16. Integrate and maintain oversight of all Center security activity, including those of tenant organizations to the extent practical.

1.1.7.17. Ensure appropriate training and professional certifications for security staff and armed security force personnel, commensurate with their assigned tasks, weapons, and equipment, as established by the AA/OSPP.

1.1.7.18. Act as the Center Director's primary staff advisor during any security-related crisis or serious incident and as primary point of contact with all external Law Enforcement agencies.

1.1.7.19. Establish and maintain annual security awareness and training programs for Center employees.

1.1.7.20. Participate as a principal member of Center teams dealing with resolution of workplace violence and protection issues.

1.1.7.21. Serve as a member of property survey boards.

1.1.7.22. Maintain a Center map of the precise jurisdictional boundaries of Center geographical areas, as determined by the Chief Counsel.

1.1.7.23. Develop and maintain personnel identification programs in accordance with established requirements.

1.1.7.24. Provide operational support to the NASA counterintelligence (CI) program, as appropriate.

1.1.7.25. Participate in all facility design reviews and on Center Master Planning Committees to ensure facility physical security and antiterrorism design criteria are appropriately incorporated into individual facility designs and Center Master Plans.

1.1.7.26. Maintain Center security program statistics and provide quarterly reports to the DSMD under the standards set forth in Appendix L.

1.1.7.27. Establish and maintain all organization informational and operational files pursuant to NPD 1440.6G, NASA Records Management and NPR 1441.1D, NASA Records Retention Schedules.

1.1.7.28. Designate, with coordination and concurrence of the AA/OSPP, a qualified and experienced Center Information Assurance Officer (IAO) who shall:

a. Have relevant experience in IT security and information assurance. Note: Having at least one of the following certifications is highly desired:
(1). Information Systems Audit and Control Association (ISACA) as a Certified Information Security Manager (CISM) or Certified Information Systems Auditor (CISA)
(2). International Information Systems Security Certification Consortium (ISC)2 Certified Information System Security Professional (CISSP)

b. Leadership and communication experience at a proven level commensurate with the expectations of the CIAO position.

c. Ability to obtain and maintain a Top Secret security clearance.

d. Fulfill the specific roles and responsibities for a CIAO described in NPR 2810.1.

e. Support Center Security Offices in certification, auditing, and inspection of unclassified IT systems

f. Support Center Security Offices in investigations of IT security incidents as appropriate. [Note: Center IAOs will not possess federal arrest authority credentials and will not be designated as investigators.]

g. Not have concurrent duties as part of the Center IT security staff.

1.1.8. Program, Line Managers, and Supervisors shall:

1.1.8.1. Support the CCS in the implementation of comprehensive security programs and mission-oriented protective services for the Center, along with individual programs and projects.

1.1.8.2. Effectively manage the level of "cleared" personnel and immediately advise the CCS of any changes in the requirements for access to classified national security information or eligibility for security clearance.

1.1.8.3. Employ CCS recommended security and loss-prevention measures within their programs or organizations.

1.1.8.4. In coordination with the CCS, employ Systems Security Engineering processes at program inception and throughout the individual program life cycle as necessary to ensure appropriate protection and accountability of program resources.

1.1.9. The Center CIO shall:

1.1.9.1. Ensure implementation of IT Security policies and develop and implement local IT Security Procedural Requirements, as deemed appropriate.

1.1.9.2. Coordinate with and support the CCS in the protection of classified and unclassified but sensitive information residing on automated systems.

1.1.9.3. Report IT security incidents to the CCS to ensure appropriate action and necessary referral is effected.

1.1.9.4. Provide technical assistance during investigations as requested by the CCS.

1.1.10. Individual employees shall:

1.1.10.1. Report suspicious activity, criminal activity, violations of national security, and other Center security responsibilities to the Security Office.

1.1.10.2. Be aware of and comply with individual responsibilities and roles in maintaining the Agency and Center security program.

1.1.10.3. Protect Government property, CNSI, and sensitive information in accordance with the requirements of this NPR.

1.1.10.4. Cooperate with Center and Agency Security Officials during inquiries and investigations.

1.1.11. The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NPR, as appropriate.

1.2 Best Practices

1.2.1. This NPR seeks to establish uniform security program standards across NASA. One way in which to accomplish "standardization" is to develop, implement, qualify, and share "Best Practices." "Best Practices" serves as a model for other NASA security organizations to learn and, where possible, benefit through adoption for use in improving or enhancing their security program. "Best Practices" occur inside and outside the NASA family, in Government or private industry.

1.2.2. The DSMD and CCS shall develop and share "Best Practices" programs and processes, where appropriate.

1.3 Waivers and Exceptions

1.3.1. Centers may occasionally experience difficulty in meeting specific requirements established

in the series of NASA Security Program NPRs. The process for submitting requests for waivers or exceptions to specific elements of the NASA Security Program is as follows:

1.3.1.1. The asset, program, or project manager and CCS shall justify the waiver request through security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; inability of the CCS to perform its missions and goals, etc. (a) Justification must also include an explanation of any compensatory security measures implemented in lieu of specific requirements. (b) The waiver request shall be submitted to the Center Director.

1.3.1.2. The Center Director shall either recommend approval or return the waiver request to the CCS for further study or closure. The Center Director shall forward concurrence to the Center's Mission Directorate Associate Administrator.

1.3.1.3. The Mission Directorate Associate Administrator shall forward waiver requests to the Assistant Administrator for Security and Program Protection (AA/OSPP) at Headquarters or return proposals to the Center Director for further study or closure.

1.3.1.4. The AA/OSPP shall return the waiver request to the appropriate Center Director with an approved waiver, for further study, or denial and closure.

1.4 Violations of Security Requirements

1.4.1. Center Directors, Headquarters Operations Director, the AA/OSPP, the DSMD, or the CCS, shall order the removal or debarment of any person who violates NASA Security requirements or whose continued presence on NASA property constitutes a security or safety risk to persons or property. Any determinations to reconsider granting access subsequent to the removal action must receive the concurrence, in writing, of the AA/OSPP.

1.4.2. Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA 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 for fines or imprisonment for not more than 1 year, or both.

1.5 Terms, Abbreviations, and Acronyms

Terms, Abbreviations, and Acronyms used throughout the family of NASA Security program NPRs are defined in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2009

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 1 (11/08/2005)

Responsible Office: Office of Security and Program Protection

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 2: NASA PERSONNEL SECURITY PROGRAM: REQUIREMENTS , INVESTIGATIONS , AND ADJUDICATION PROCESS FOR POSITIONS (NATIONAL SECURITY POSITIONS) REQUIRING ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI)

2.1 General

2.1.1. Title 5 Code of Federal Regulations (CFR), Part 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 Executive Order (E.O.) 10450, Security Requirements for Government Employment, and E.O. 12968, Access to Classified Information.

2.1.2. This chapter does not address other aspects of the position risk designation program which include Personnel Suitability described in Title 5 CFR, OPM Part 731, Suitability; HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors , and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors," Automated Information System Security defined in the Office of Management and Budget (OMB) Circular A-130; and numerous laws.

a. These programs, outlined in chapters 3 and 4 respectively, require a determination of a position's risk level (i.e., Low Risk, Moderate Risk, or High Risk) using criteria that are separate and distinct from the national security criteria. Designation of position risk level

must occur prior to establishment of sensitivity level. See Appendix M.

b. Information regarding Personnel Suitability may be obtained from the Office of Human Resources.

c. NPR 2810.10, NASA Automated Information Systems Security, establishes the policy, assigns responsibilities, and prescribes standards and procedures for the management of the Information Technology (IT) security program for NASA

2.1.3. 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.

2.1.4. 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.

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

2.1.6. The Office of Personnel Management (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.

2.1.7. NASA Contracts requiring the generation of and/or access to CNSI will be processed and individuals investigated in accordance with the requirements established in chapter 6 of this NPR, and the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

2.2 Scope

2.2.1. This chapter prescribes the procedures whereby employees are selected, processed, investigated, and adjudicated for national security positions, consistent with U.S. Security Policy Board (SPB) Procedures contained in SPB Issuance 1-97, SPB Issuance 2-97, and SPB Issuance 3-97.

2.2.2. This chapter does not apply to contractor personnel providing services under a NASA classified contract that requires access to CNSI. Refer to chapter 6, "Industrial Security," for requirements on NASA classified contract processes and procedures.

2.3 Responsibilities

2.3.1. The DSMD shall establish a Central Adjudication Facility (CAF) at the Headquarters level responsible for adjudicating all investigative results for security clearances for access to CNSI. The CAF shall process and manage all requests for security clearance, adjudicate all investigative results, grant clearance eligibility, and deny, revoke, or suspend security clearances in accordance with the provisions of EO 12968 due process considerations.

2.3.2. Center Directors shall ensure the CCS manages the Center personnel security program in accordance with this NPR.

2.3.3. The CCS shall:

2.3.3.1. Process security clearances for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

2.3.3.2. Ensure only the on-line e-QIP version of the SF 86 is used when it becomes available.

2.3.3.3. Grant a NASA employee a security clearance or suspend an employee's clearance for cause.

2.3.3.4. Delegate these responsibilities to a senior personnel security specialist who is a

civil service employee, who has attended a recognized Personnel Security Suitability and Security Adjudication course, and who has maintained currency in that field.

2.3.3.5. In cooperation with Center Human Resources Organizations, management, and supervisory personnel, implement these procedures for appropriate designation of National Security position sensitivity, per section 2.7, for all existing and newly established positions whose duties clearly reflect the requirement for a security clearance and access to CNSI, in accordance with the requirements set forth in this chapter. This collaborative approach is essential if NASA is to effectively comply with established national security position sensitivity designation requirements outlined in 5 CFR 732.101 - 732.401 and the requirements of EO 12968.

2.3.4. Center Human Resources Organizations shall:

2.3.4.1. Ensure that position descriptions are developed by the appropriate management and supervisory personnel, and that they accurately reflect National Security position sensitivity and establishes clear requirements for access to CNSI, as required under 5 CFR 732.101 - 732.401 and EO 12968.

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

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

2.3.5. Program, line managers, and supervisors shall ensure full compliance with the requirements established in this chapter.

2.4 Personnel Security Program Oversight

As part of its responsibility for the functional management of the NASA Security Program, the DSMD shall include personnel security program matters in periodic audits of Center security programs.

2.5 Basic Principles of Personnel Security Clearance Management

2.5.1. EO 12958, Classified National Security Information, clearly emphasizes the requirement to establish procedures to prevent unnecessary access to classified information, including procedures that require that a demonstrable need for access to classified information be established. EO 12968, Access to Classified Information, directs that when such access is no longer required, it shall be administratively withdrawn.

2.5.2. 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 need to access CNSI. Following the requirements established in Appendix M of this NPR, 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 and risk level designation 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 for the Agency as it must then change or cancel previously submitted investigative requests with OPM.

2.5.3. No individual is deemed eligible for access to CNSI merely by reason of right or privilege or as a result of any particular title, grade, position, or affiliation.

2.5.4. 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, and such access may be reasonably prevented.

2.5.5. Requests for security clearances shall not be processed or granted based merely on a speculative need for access. Requesting security clearances for contingency

purposes in excess of actual official requirements is prohibited.

2.5.6. The level at which access to CNSI is requested and granted shall be limited and shall relate directly to the level of classified information to which access is clearly justified in the performance of official duties.

2.6 Processing Personnel Security Clearance Requests

2.6.1. As stated in subparagraph 2.5.2, the requirement for access to CNSI shall be clearly established during the position development phase. Once the position has been determined to require access to CNSI and position sensitivity assigned, the Center HRO shall ensure the new appointee receives access to and completes the on-line (e-QIP) SF 86 per section 2.7.

2.6.2. If an incumbent employee has been determined to require a security clearance up to the Top Secret level, a NASA Form 1630, Request for Access to CNSI, shall be prepared and appropriately justified by the employee's immediate supervisor, reviewed by the line supervisor through the Division Director, or higher depending on the applicant's organizational position, and forwarded to the Center Personnel Security Office for appropriate action.

2.6.2.1. The NASA Form 1630 shall be retained in local personnel security files, with a copy forwarded to the CAF.

2.6.2.2. A recertification (New NASA Form 1630) must be conducted only when a person changes position. However, annual review of clearance and access requirements is necessary to ensure Center personnel security clearance needs are properly managed. The CCS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

a. 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.
b. 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.

2.6.3. All required investigative forms shall be completed in a timely manner, by the employee and submitted to the CCS for appropriate action. Completion of electronic web-based investigative forms (e-QIP) shall be made mandatory as they become available online. (NOTE: Failure to complete the necessary forms in a timely manner will result in a significant delay in initiating the appropriate investigation and granting of an Interim clearance up to and including the SECRET level.)

2.6.4. The CCS shall ensure the forms are properly completed and submitted to OPM for investigation using the NASA Central Adjudication Facility (NASA CAF) Security Office Identifier (SOI) number provided by the NASA CAF. [NOTE: Use of the NASA CAF SOI number will ensure completed investigations are returned by OPM to the Central Adjudication Facility (NASA CAF) for adjudication.]

2.6.5. Results of the adjudication process shall be posted and made available to Center security offices via the Clearance Verification System (CVS) Database. The NASA CAF shall notify Center security offices when information on processed employees has been entered into the CVS. The CCS may then grant final clearance. The employee will be notified, in writing, when an Interim or Final clearance has been granted. Use of NASA Form (NF) 1730, "Obtaining and Maintaining a Security Clearance for Access to Classified National Security Information (CNSI)," is mandatory for communicating clearance status and requirements to employees.

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

2.6.6.1. Personnel Requesting SCI access must have a completed TS investigation.

2.6.6.2. 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, and forward it, 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.

2.6.6.3. The Form 2018A and the original signed SCI Non-disclosure Form shall be retained by the SSO representative at the Center. A copy of the signed SCI Non-disclosure Form shall be forwarded to the NASA HQ SSO.

2.6.7. One-Time Access Determinations

2.6.7.1. Occasionally, urgent operational requirements may occur where NASA civil service personnel employees in nonsensitive 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 or are required to possess a Secret clearance to access other Government agency secure sites even though the purpose for their visit is of an unclassified nature. 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. One-time access determinations shall be used sparingly and only under conditions of compelling government need. The CCS has the authority to grant one-time access determinations subject to the following terms and conditions:

a. One-time access determinations shall not be issued more than 3 times per person and shall not exceed 60 days in total accumulated duration during a single calendar year.
b. One-time access determinations shall only be granted to U.S. citizen civil service personnel that have been continuously employed by the Federal Government for the preceding 24 months.
c. Whenever possible, access shall be limited to a single instance or only a few occasions. Repeated access requests shall require processing for final security clearance determination.
d. If the need for access is expected to exceed the original request of 60 days, the individual must be processed for a final security clearance determination.
e. An individual requiring one-time access must complete a NASA Form 1630, Request for Access to CNSI; have a prior completed "no access" National Agency Check or other comparable personnel security investigation, or a criminal history and credit check, a favorable suitability determination and local records check; present a completed SF 86 or 86C, if applicable; and be personally interviewed by the CCS or qualified designee.
f. 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.

2.7 Coding of Position Sensitivity Level Designations for National Security Positions

2.7.1. The proper coding of position sensitivity for national security positions is required on Optional Form 8, Position Description, or NASA Form 692, Position Description, and optional on the SF 50 and 52. (See 5 CFR part 732). NASA managers and supervisors must use the following codes whenever establishing position sensitivity for access to CNSI: National Security Position Sensitivity Level Codes:

Special-Sensitive: 4

Critical-Sensitive: 3
Noncritical-Sensitive: 2
Non-Sensitive: 1 (No clearance required).

2.7.2. Center Human Resources Offices are responsible for managing a Risk Designation System in accordance with 5 CFR 731-106(a). They shall coordinate, in a timely manner, with managers, supervisors, and the CCS to accomplish sensitivity designation of positions requiring access to CNSI. After the appropriate position sensitivity determination has been assigned, the Center HRO or Security Office shall initiate the appropriate investigation.

2.7.2.1. 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 these positions 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. Top Secret SCI
b. NASA Special Access Program

2.7.2.2. CRITICAL-SENSITIVE (CS): Positions requiring access to any of the levels of classified information outlined below shall be designated Critical-Sensitive. Individuals in or selected for these positions 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. Top Secret (TS)
b. NATO Top Secret

2.7.2.3. NONCRITICAL-SENSITIVE (NCS): Positions requiring access to any of the levels of classified information outlined below shall be designated Noncritical-Sensitive. Individuals in or selected for these positions must undergo, at a minimum, an Access National Agency Check with Inquiries (ANACI), using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access. Exceptions to classified access investigative requirements for these positions shall be made only as provided for in section 2.6 above.

a. a. Secret or Confidential
b. b. NATO Secret/Confidential

2.7.2.4. Pre-appointment investigation requirements shall NOT be waived for positions designated "SPECIAL SENSITIVE."

2.7.2.5. Pre-appointment waivers may be authorized by Center Directors and the Assistant Administrator for Security and Program Protection to approve an emergency 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.

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

2.7.3. All NASA national security position descriptions (PD) shall be "Testing Designation Positions (TDP)." Personnel holding active clearances shall be entered into the Agency's random drug testing program.

2.8 Temporary/Interim Access to CNSI

2.8.1. Senior Management Officials shall request temporary access eligibility for U.S. citizen employees, civil service employees, contractors, and/or consultants filling CS and

NCS positions when essential operational requirements do not allow for waiting for a pending personnel security investigation to be completed and adjudicated. Management shall submit requests for temporary access eligibility using NASA Form 1630 and provide compelling justification to warrant access to CNSI in advance of formal investigation and adjudication. The CCS shall serve as the appropriate adjudication authority and shall issue temporary access eligibility and grant the appropriate interim security clearance up to the Secret Level only, provided the provisions of SPB Issuance 3-97 (See Appendix C) are met. In all cases, the required personnel security investigation shall be initiated prior to issuance of the INTERIM clearance. Temporary/interim access eligibility and issuance of an INTERIM security clearance shall be recorded on NASA Form 346, Notification of Completion of Investigation, under Executive Order 10450. A copy of the NASA Form 346 shall be forwarded to the DSMD and local Office of Human Resources for inclusion in the subject's Official Personnel File (OPF).

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

2.9.1. Non-U.S. citizens (including lawful permanent resident (LPR)) are not eligible for a security clearance. Under specific situations the AA/OSPP 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 shall submit a written request to the AA/OSPP via the CCS. The request shall:

2.9.1.1. Specify why it is impractical or unreasonable to use U.S. Citizens to perform the required work or function.

2.9.1.2. Define the individual's special expertise.

2.9.1.3. Define the compelling reasons for the request.

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

2.9.1.5. The CCS shall review the request for accuracy, endorse or nonendorse it, and forward it to the AA/OSPP.

2.9.1.6. The AA/OSPP shall coordinate with the Office of External Affairs for concurrence (Export Compliance), and if approved, shall return it to the requestor. A copy shall be retained in the OSPP and CCS files.

2.9.1.7. 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.

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

2.9.1.9. 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.

2.9.1.10. 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.

2.9.1.11. 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.

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

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

2.9.2. 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) in Columbus, Ohio, or successor organization, has the authority to grant an LAA to non-U.S. citizens. Procedures for coordination of the request are as follows:

2.9.2.1. A cleared contractor's Facility Security Officer must receive the endorsement of the CCS, Center International Visitor Coordina , tor (IVC), Center Export Administrator (CEA), AA/OSPP, and Office of External Relations (Export Control), as appropriate.

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

2.9.2.3. If acceptable, the AA/OSPP 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.

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

2.9.2.5. Controls outlined in subparagraphs 2.9.1.9 through 2.9.1.12 shall be implemented and strictly monitored.

2.10 Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations from Other Government Agencies and Organizations

2.10.1. Reciprocity is a key component of current Federal personnel security philosophy, rules, and guidelines. NASA shall accept personnel security investigations and favorable determinations for access to CNSI conducted and adjudicated by other Federal agencies in accordance with the guidelines set forth herein.

2.10.2. Normally, prior investigations conducted in connection with actual or contemplated prior Federal service (civilian or military), the granting of a clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC) for access to Restricted Data (RD) or Formerly Restricted Data (FRD), or the granting of a security clearance under the Department of Defense (DoD) National Industrial Security Program (NISP), shall be accepted as meeting the investigative requirements prescribed herein, provided the following conditions are met:

2.10.2.1. There has been no break in service in excess of 24 months, and the prior investigation was completed within the timeframe established by SPB Issuance 1-97 for the level of access required.

2.10.2.2. The prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position.

2.10.2.3. The prior investigation discloses no unresolved information that reflects adversely on the applicant's eligibility for a security clearance. If it is determined that prior investigation does not meet the provisions of paragraph 2.10.2 above, an appropriate update or upgrade investigation shall be requested to bring the total combined investigative effort up to standard.

2.11 Prior Personnel Security Clearance Determinations by NASA Authorities

Personnel security clearance eligibility granted by the NASA CAF and security clearances granted by the respective NASA Centers shall be mutually and reciprocally accepted by all

Centers without requiring additional investigation, unless there has been a break in the individual's employment in excess of 24 months or unless derogatory information that occurred subsequent to the last security determination becomes known.

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 requires 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 is required in the performance of NASA duties, a request for either a DOE or an NRC clearance shall be initiated by the CCS, who shall forward the necessary documents to the NASA CAF 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 (Appendix B) 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/OSPP or designee shall deny or revoke a security clearance.

2.13.3. The AA/OSPP, DSMD, and CCS may grant interim and final clearances or suspend security clearances, as appropriate.

2.13.4. Each adjudication shall be fully documented and recorded in the subject's security file and the Central Adjudication Activity (NASA CAF) personnel security database.

2.13.5. Information developed during the investigation process for a security clearance shall not be shared with the Center HRO or management while the investigation is pending. The DSMD or CCS 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 shall propose denials and revocations of security clearances to the NASA CAF. The AA/OSPP shall make final denial or revocation determinations after consultation with the NASA CAF and the OGC, and as provided for under paragraph 2.15.4 of this NPR.

2.13.8. Requests for a security clearance (NASA Form 1630) 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 must be allowed to review and refute any information developed during the investigation process that may make him or her ineligible for access to classified information, unless release of that information jeopardizes national security.

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 EO 12968.

2.13.11. The AA/OSPP, Center Director, CCS, or the DSMD may suspend a security clearance for cause.

2.13.12. The Center HRO, in coordination with the Security Office and supervisors, shall make employment suitability determinations under EO 10450 and other regulations. The Center HRO shall coordinate and document those determinations. They are separate and distinct from security clearance adjudications (see section 5.2(f) of EO 12968). See chapter 3 for requirements regarding employment suitability.

2.13.13. 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 may 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 Adjudication of Personnel Security Clearance Status

2.14.1. The AA/OSPP, or designee, is empowered to deny or revoke an employee's security clearance.

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

2.14.3. 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 must be documented in the employee's security file and suitability determinations made under the continuous evaluation program. The Center HRO and supervisory personnel, with the advice of the Security Office, shall make all suitability determinations under the continuous evaluation program. Refer to chapter 3, section 3.11, for requirements on processing suitability issues.

2.14.3.1. In cases where sufficient investigative information may not exist to complete the adjudication for a security clearance, the subject of an incomplete investigation must be apprised of any adjudicative issue information in accordance with E.O. 10450 and afforded an opportunity to comment on that information related to suitability for continued employment.

2.14.3.2. Explanations or mitigating information provided by the subject must also be documented in his or her security file.

2.14.4. Upon completion of an investigation that develops potential adjudicative issues, a personal interview of the subject shall be conducted by the appropriate security official.

2.14.4.1. During this interview the subject shall be advised of any issues and provided an opportunity to present relevant information to refute or mitigate the issues.

2.14.4.2. In isolated instances, when a personal interview is not practical, a written interrogatory shall be sent by the NASA CAF to the subject or the CCS shall be tasked to coordinate the reply.

2.14.4.3. The subject may be accompanied during the interview by counsel or other representative. All costs associated with such representation are at the subject's expense.

2.14.4.4. At the onset of a subject interview, the subject must be advised of the provisions of the Privacy Act of 1974 (5 U.S.C. 552a).

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

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

2.15 Denial or Revocation of Personnel Security Clearances

2.15.1. In the event of an unfavorable adjudication action, the NASA Central Adjudication Facility (NASA CAF) shall forward a documented proposal to deny or revoke a clearance to the AA/OSPP.

2.15.2. The AA/OSPP shall do one of the following after reviewing the file and the recommendation of the NASA CAF:

2.15.2.1. Remand the case to the NASA CAF for further work; or

2.15.2.2. Make a favorable adjudication of the information; or

2.15.2.3. In consultation with the Office of General Counsel, provide written notice to the subject of the denial or the revocation of the security clearance.

2.15.3. If the employee subsequently requests a review of the proposed action, or the subject provides new information for consideration, or both, the NASA CAF shall review the case, taking into consideration any new information provided. If no review is requested, or if the NASA CAF continues to recommend denial or revocation, after the review is conducted, the complete case file and the NASA CAF recommendation shall be forwarded to the AA/OSPP for action.

2.15.4. Actions of the AA/OSPP shall be conducted in accordance with the elements of section 5.2 (a) of EO 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 the AA/OSPP' final determination. If the employee takes advantage of the opportunity to appear personally before the AA/OSPP, the AA/OSPP shall document such appearance by means of a written summary or recording which shall be made a part of the subject's security record.

2.15.5. If the AA/OSPP provides 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.

2.15.6. Prior to finalizing the SARP determination, a SARP panel member or the AA/OSPP 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.

2.15.7. Upon determination that a clearance revocation or denial has been upheld, the case then becomes one of employment suitability and shall be referred to HRO for suitability determination per chapter 3, section 3.10.

2.16 Suspension of Personnel Security Clearances

2.16.1. The AA/OSPP, DSMD, Center Director, or the CCS 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.

2.16.1.1. Normally, an individual subject to a suspension action is advised of the

suspension. However, there shall be instances when the suspending authority, working with management and the NASA Director, Security Management Division, and Director, Safeguards Division shall terminate an individual's access to new classified information, without the individual's knowledge, in order to preserve the integrity of an investigation.

2.16.1.2. The reason or reasons for a suspension need not be provided to the subject of a suspension.

2.16.1.3. 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.

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

2.16.1.5. As a result of the temporary status of a suspension, the subject of a suspension is not entitled to the review procedures required for denial or revocation of a security clearance.

2.16.1.6. All suspensions enacted by Center Security Offices must be coordinated with the NASA CAF.

2.17 Continuous Evaluation of Personnel Security Clearance Eligibility

2.17.1. A personnel security clearance determination is based on a continuous assessment of an employee'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.

2.17.2. 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 qualification to meet the high standards of conduct expected of persons in national security positions.

2.17.3. 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.

2.17.4. Center Directors and the CCS shall ensure 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 shall be disqualifying. Where employees have significant involvement with handling, storing, marking CNSO, or exercising original or derivative classification, supervisors must include these responsibilities as a critical element of the employees' annual performance communication system documentation.

2.17.5. Supervisors and managers are critical to the success of the evaluation of the security clearance eligibility program. Supervisors shall report incidents of potentially disqualifying behavior that they are aware of to the CCS and be observant to potential changes in behavior of their subordinates that could cause potential risk to the national security information to which the employee has been entrusted.

2.17.6. 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.

2.17.7. Personnel holding a Security Clearance are subject to random drug testing.

2.17.8. All reports of behavior that may impact continued eligibility to hold a security clearance shall be forwarded by the CCS to the NASA CAF, as appropriate.

2.18. CLASSIFIED VISITS AND MEETINGS

2.18.1. Classified Visits to Other Agencies . An employee who has a need to certify his/her security clearance for a visit to an agency or facility must initiate the appropriate visit form, letter, or telephonic action with the respective Center Personnel Security Office or Special Security Officer.

2.18.1.1. The request shall be signed by the Center Personnel Security Officer or designated representative, the Special Security Officer, or member of the Security Management Division.

2.18.1.2. Completed Visit Requests will be faxed, mailed, or e-mailed, by the Center Security Office, to the appropriate external Agency Security Office for processing.

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

2.18.1.4. Only those clearances granted by the Security Management Division and contained in the automated listing of the Clearance Verification System may be certified.

2.18.2. 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, Security Management Division, or the Special Security Officer. The certifications should include the investigation record information used as a basis to grant the clearance, Center POC point of contact, and purpose and duration of the visit request.

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

2.19 Recordkeeping

2.19.1. Center Security Offices shall create and securely maintain personnel security investigative and screening records on all NASA civil service and contractor personnel security cases.

2.19.1.1. Files shall be maintained for a minimum of two (2) years after the individual's employment or access to NASA facilities or IT systems is terminated.

2.19.1.2. Files shall include the original forms submitted to initiate the investigation and screening, a summary of the results of any investigative and screening activity, a record of the final decision, and any subsequent actions.

2.19.1.3. Security offices shall safeguard these files pursuant to NPD 1440.6G, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules.

2.19.2. 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, DSS, FBI). The subject must obtain copies of the third party investigation directly from the appropriate agency.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov

---

Chapter 3: NASA Personnel Security Program: Position Risk Designation Process, Background Investigations, and Employment Suitability Determinations for NASA Employees

3.1 General

3.1.1. As required by 5 CFR part 731, Executive Order 10450, HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors," all Federal employees are subject to a personnel security background investigation as set forth in this chapter to assist NASA in determining their suitability for Government employment.

3.1.2. The investigation provides NASA management necessary information to determine if an individual's judgment, trustworthiness, and suitability promote the efficiency of the Government and NASA's mission, and is consistent with the safety and security of the Agency and individual Center.

3.1.3. No personnel actions associated with recruitment, hiring, or position change shall take place without the appropriate prior designation of position risk and sensitivity levels by Center OHR.

3.1.4. No one shall be issued a permanent NASA employee photo-ID, granted access to NASA Centers or facilities, granted access to NASA IT systems, or sensitive information without, at a minimum, immediate completion of a NAC and subsequent completion of a NACI within 6 months. The NAC must be accomplished prior to or NLT than 10 working days after receipt of the written offer of appointment .

a. Temporary photo-ID or visitor badges, issued to new employees, who have not submitted the appropriate investigative forms, will expire at the 10 working days time period.

b. Further delays in forms submittal will require the individuals' supervisor to sponsor one-day visit requests up to an additional 5 working days. The supervisor will also be required to escort the individual.

c. Upon expiration of the additional 5 working days, all issued temporary badges/passes and approved accesses will be terminated pending submittal of forms.

d. Centers shall establish the necessary procedures to ensure abuse of the visitor/temporary photo-ID system does not occur.

3.2 Applicability

3.2.1. This chapter prescribes the requirements and process for the proper conduct of personnel suitability investigations for all NASA civil service personnel, under part-time or full-time employment. A t a minimum, NASA shall conduct the appropriate investigation required by position risk designation, but no less than a National Agency Check with Inquiries (NACI), and shall make an employment suitability determination on all NASA employees. Their assignment, employment, or

retention must be clearly consistent with National-level suitability guidelines, regulations, and employee safety considerations.

3.2.2. 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 by their respective Agency. The CCS shall coordinate with the Center HRO to validate investigative and suitability results for detailees. Upon validation, no further investigation is required relative to issuance of the NASA photo-ID and access to NASA facilities unless specifically required by Center policy or for cause. All subsequent suitability issues associated with personnel identified in this paragraph shall be coordinated with the Center HRO or respective detailee's official Agency personnel office for resolution.

3.3 Responsibilities

3.3.1. The AA/OSPP is responsible for establishing and maintaining a viable and consistent personnel security program in accordance with current personnel security and suitability policies as established by the Office of Personnel Management (OPM).

3.3.2. Center Directors are responsible for ensuring full Center compliance with the provisions set forth in this chapter.

3.3.3. The CCS shall:

3.3.3.1. 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 under this chapter.

3.3.3.2. Assist and support Center HRO personnel in the identification of the type of personnel investigation required for each position, including updating or upgrading requirements, as appropriate.

3.3.3.3. Refer all employment suitability cases to the appropriate HRO.

3.3.3.4. Assist the Center HRO by conducting local records checks, when necessary, to clarify, expand, or mitigate information that has been forwarded to HRO.

3.3.4. The Director of Human Resources at each Center shall:

3.3.4.1. Following the procedures contained in Appendix M, " D esignation of Public Trust Positions and Investigation Requirements," and applying the process flow established in Appendix N " Determining Position Risk and Sensitivity Levels, Process Flow Chart" , ensure management and supervisory personnel use NASA Form 1722 located at Appendix M, Figure 1, "NASA Position Designation Record," to determine and annotate the appropriate risk designation and sensitivity levels for all Civil Service personnel positions per 5 CFR parts 731 and 732 and EO 10450, respectively.

3.3.4.2. Ensure the appropriate investigative forms, as indicated in section 3.7, are completed by the incumbent or prospective employee in a timely manner and forwarded to the CCS for submittal to OPM for investigative action. Use of web-based e-QIP forms (e.g., SF 85 and SF 85P) will be made mandatory when they become available on-line.

3.3.4.3. Verify applicant birth and citizenship status in accordance with Federal Investigations Notice 03-01, dated October 30, 2002, or subsequently issued directive or notice.

3.3.4.4. Ensure the continued familiarity of HRO personnel regarding position risk designation and sensitivity level requirements and procedures, and suitability adjudication standards, criteria, and processes as established by OPM.

3.3.4.5. Refer medical related data in investigative files to the NASA medical authority for review and evaluation, as appropriate.

3.3.4.6. 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 application of this chapter.

3.3.5. Program, Line Managers, and Supervisors shall:

3.3.5.1. As a critical element of their supervisory and management duties, ensure appropriate and accurate position risk designation and sensitivity levels are assigned for all positions under their purview per 5 CFR Parts 731, 732, and EO 10450, as implemented by Appendix M.

3.3.5.2. Assist HRO during the suitability determination process, as appropriate.

3.3.6. The NASA General Counsel or the Chief Counsel of each Center, as appropriate, shall provide legal counsel with regard to implementation of this chapter.

3.4 Submitting Requests for Suitability Investigations

Upon selection for employment in Government service or as a result of a change in position risk and sensitivity level designation the Center HRO shall ensure the completed forms are forwarded to the CCS for review and submittal to OPM.

3.5 Position Types and Risk Levels

3.5.1. Designation of Public Trust Positions **.** Each position shall be designated at the High, Moderate, or Low risk level depending on the position's potential for adverse impact to the integrity and efficiency of the service (5 CFR 731.106). Positions at the High and Moderate risk levels are referred to as "Public Trust" positions

3.5.1.2. PUBLIC TRUST POSITIONS - The criteria for Public Trust Positions are defined in 5 CFR, Section 731.106 The designations of positions indicate the potential for action or inaction by the incumbent of the position to affect the integrity, efficiency, and effectiveness of Government operations. Public trust risk designations are used in conjunction with security clearance requirements to determine the investigative requirements for the position. Positions involving high degrees of public trust, e.g., those with broad policy making authority or fiduciary responsibilities, trigger a more thorough investigation than do positions requiring only the finding that an applicant or an incumbent has the requisite stability of character to hold Federal employment. The three public trust risk designation levels are high, moderate, and low.

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

(1) Policy development and implementation;

(2) Higher level management assignments;

(3) Independent spokespersons or non-management positions with authority for independent action;

(4) Significant involvement in life-critical or mission critical systems; or

(5) Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization of disbursement from systems of dollar amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system.

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

b. MODERATE RISK: A position that has the potential for moderate to serious impact involving duties of considerable importance to the Agency or a program mission of the Agency with significant program responsibilities and delivery of customer services to the public such as:

(1) Assistants to policy development and implementation;

(2) Mid-level management assignments;

(3) Non-management positions with authority for independent or semiindependent action;

(4) Delivery of service positions that demand public confidence or trust; or

(5) Positions with responsibility for the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the high risk level to ensure the integrity of the system. Such positions may include but are not limited to:

(a) Access to and/or processing of proprietary data, information protected by the Privacy Act of 1974, and government-developed privileged information involving the award of contracts;

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

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

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

3.5.1.3. Position risk level determinations are inclusive of many factors, IT positions and/or access being the most prevalent. Provided below are categories of IT positions and/or specific duties that may influence the risk level designation for each individual position.

a. In accordance with the Federal Information Systems Management Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, and NPR 2810.1, NASA has established requirements and procedures to assure an adequate level of protection for NASA IT systems, which includes the appropriate security screening of all individuals having access to NASA IT systems:

(1). High Risk or 6C positions include positions in which the incumbent is responsible for planning, directing, and implementing a computer security program; has major responsibility for directing, planning, and designing an IT system, including the hardware and software; or, can access a system with relatively high risk for causing grave damage or realizing a significant personal gain. High risk IT positions may include positions, which involve the following:

(a) Development or administration of Agency IT Security Programs, directing or controlling IT risk analysis and threat assessments, or conducting investigations.

(b) Significant involvement in life-critical or mission-critical systems; (See section 3.5.6. for further requirements).

(c) Privileged access to NASA IT Systems designated as High Risk systems.

(d) Access to data or systems whose misuse can cause very serious adverse impact or result in significant personal gain.

(e) Assignments involving accounting, disbursement, or authorization of $10 million or more per year.

(2) Moderate Risk or 5C positions include positions where the incumbent is responsible for directing, planning, designing, operating, or maintaining IT systems and whose work is technically reviewed by a higher authority (at the high risk level) to ensure the integrity of the system: Moderate risk IT positions may involve:

(a) Systems design, operation, testing maintenance or monitoring which is under technical review of IT-1 and includes:

(1) Those that contain the primary copy of data whose cost to replace exceeds $1 million dollars.

(2) Those that control systems which affect personal safety and/or physical security, fire, or Hazmat warning safety systems.

(3) Privileged information on contract awards in excess of $10 million dollars.

(4) Accounting disbursement or authorization of more than $1 million dollars but less than $10 million dollars per year.

(b) Access to data or systems whose misuse can cause serious adverse impact or result in personal gain, which includes but is not limited to:

(1) Proprietary data;

(2) Privacy Act protected information;

(3) Export Control Regulation (EAR), International Traffic in Arms Regulations (ITAR), and the Militarily Critical Technologies List (MCTL) information.

(c) Limited privileged access to NASA IT Systems designated as Moderate Risk systems.

(3) Low Risk or 1C positions are all IT system positions that do not fall in the categories above and includes 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:

(a) General word processing;

(b) Systems containing no IT-I or IT-II level information or IT-1 or IT-2 level information that is protected from unauthorized access

b. Specific requirements and criteria for designating Computer/ADP risk levels are contained in Appendix M.

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

3.5.3. Risk Levels. The four suitability position risklevels are defined and explained in the table below.

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

3.5.4. Risk Designation System. NASA's procedure for designating public trust positions is provided at Appendix M. NASA Centers shall follow this procedure for designating public trust to ensure uniformity and consistency.

3.5.5. Relationship of Suitability Risk and National Security Sensitivity to Investigation Type. Basic suitability screening is required for all positions. The first determination NASA must make is whether the person has the character traits and past conduct expected of someone who is to carry out

the duties and responsibilities of a Federal job in order to protect the integrity and promote the efficiency of the service.

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

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

3.5.7. Such screening must occur before the individual is authorized access and periodically thereafter. See chapter 2 for requirements for security clearances to access CNSI.

3.6 Suitability and the Investigative Process

3.6.1. Suitability. Eligibility for employment with NASA (Federal Employment) is based on suitability as measured from past and present conduct, which determines whether or not an employee can perform his or her duties with efficiency and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

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

a. Promoted;

b. Demoted;

c. Reassigned;

d. Converted from career-conditional to career tenure;

e. Appointed (or converted to an appointment) when that employee has been serving with that agency for at least one year in one or more positions under an appointment subject to investigation; or,

f. Transferred, provided the individual has served continuously for at least one year in a position subject to investigation.

3.6.3. Reemployments.

3.6.3.1. Reemployments are not one of the general exceptions to the subject to investigation rule. When individuals are reemployed in Federal service, they must complete a new Declaration for

Federal Employment (OF 306). They must also complete new investigative questionnaires (or update their prior form if the public trust or sensitivity level of their new position is the same as the old one). If suitability issues are admitted on the OF 306 or investigative questionnaire, or if they are otherwise developed, they must be investigated and adjudicated.

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

3.6.4. Investigative Requirements. Pursuant to the authority delegated by the President of the United States under 5 U.S.C. sections 1104 and 3301, and Executive Order 10577, OPM requires individuals seeking admission to the civil service to undergo a background investigation to establish their suitability for employment. OPM has determined that varying levels of investigation are appropriate, depending on the responsibilities of the position. The minimum level of investigation required for entry into the Federal service is the National Agency Check and Inquiry (NACI) investigation. The type of investigation to conducted is a product of the risk level designation of a position and, if appropriate, National Security requirements. OPM has established the following minimum levels of required investigation for positions at the Low, Moderate, and High Risk levels:

RISK LEVEL	MINIMUM REQUIRED INVESTIGATION
LOW Risk	NACI - National Agency Check and Inquiries
MODERATE Risk	MBI - Minimum Background Investigation
HIGH Risk	BI - Background Investigation
PRP	NACI (See subparagraphs 3.5.2.3 and 3.8)

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

3.6.5. Timing of Investigations. Investigations shall be initiated before appointment or, at most, within 10 working days of placement in the position. If, at any time, it is determined that a required investigation has never been conducted for the initial appointment, the appropriate required investigation must be conducted even if there have been subsequent personnel actions that would not be subject to investigation (such as transfers, promotions, or , reassignments).

3.6.6. Change in Position Risk Level. All employees moving to a new position at a higher risk level than the risk level of the position they left must meet the investigative requirements of the risk level designation of the new position. It is a good practice to complete the required investigation before the individual moves to the new position. Any required higher level investigation must be initiated within 10 working days of the date the new position is occupied. If the risk level of an incumbent's position is increased due to a change in duties and responsibilities, the incumbent may remain in the position, but the investigation required by the higher risk level shall be initiated within 10 working days of the effective date of the new position designation. This requirement applies to details as well as permanent reassignments.

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

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

3.6.7.1. Centers shall establish the appropriate checks and balances to ensure abuse of the aforementioned exception does not occure and that the exception is not granted to individuals falling under higher risk levels.

3.6.7.2. Personnel granted access under this provision will be issued a Center-specific temporary photo-ID granting access only to their respective center.

3.7 Coding of Position Risk Level on Personnel Documents

The code for the position risk level is required on Optional Form 8. HR Offices shall place the code for the position risk level in the *Remarks* section of the Standard Forms 50 and 52.

The codes are:

RISK LEVEL	CODE
High	6
Moderate	5
Low	1

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

3.8 Forms Required to Initiate Suitability Investigations for NASA Employees Requiring No Access to CNSI

ACTION	LOW RISK POSITION	MODERATE RISK POSITION	HIGH RISK POSITION	PRP POSITION
NEW FEDERAL APPOINTMENT	NACI/No Access SF 85 - original	MBI /No Access SF 85P - original	BI/No Access SF 85P - original	NACI/No Access SF 85P-original

	SF 87 OF 306* NASA Form 1684 (Authorization and Release of Credit Reports)	OF 306* SF 87 NASA Form 1684 (Authorization and Release of Credit Reports)	OF 306 SF 87 NASA Form 1684 (Authorization and Release of Credit Reports)	OF 306, SF 87, OFI Form 79B, NASA Form 1734, NASA Form 1684 (Authorization and Release of Credit Reports)
REINVESTIGATION	NACC SF85 - Original SF 87 NASA Form 1684 (Authorization and Release of Credit Reports)	PRI/No Access SF 85 - original SF 87 NASA Form 1684 (Authorization and Release of Credit Reports)	PRI/No Access SF 85P - original SF 87 NASA Form 1684 (Authorization and Release of Credit Reports)	NACI/No Access SF 85P-original OF 306, SF 87, OFI Form 79B, NASA Form 1734, NASA Form 1684 (Authorization and Release of Credit Reports)
UPDATE AND UPGRADE INVESTIGATION (For change of position to higher level)	See Moderate or High Risk Position Investigative Requirements as appropriate.	See High Risk Position Investigative Requirements.	See Chapter 2 Investigative requirements for access to CNSI.	None if retained in the PRP Program. See Chapter 2 Investigative requirements for access to CNSI.

*When only the September 1994 version of the OF 306 is available, the subject of the investigation shall complete items 1, 2, 7 through 12, 15, and 16a. When more recent versions of the form are used, the subject of the investigation shall complete items 1, 2, 8 through 13, 16, and 17a. If the form is not available, the specific questions shall be duplicated on a separate attachment and completed by the Subject.

3.9 Suitability Determination Procedures for NASA Federal Employees

3.9.1. The Office of Personnel Management (OPM) establishes the regulations, guidelines, procedures, and criteria governing this program and conducts all suitability investigations.

3.9.2. As required by 5 CFR, Part 731, EO 10450, and FIPS 201, each prospective Federal employee must undergo an initial entry on duty (EOD) personnel security investigation to determine suitability for employment with the Federal Government. This investigation shall take place before appointment

to a Government position or no later than 14 days after appointment.

3.9.3. Determining suitability for Government employment involves a review of completed personnel security investigations for issues of trust, criminal activity, etc., that could impact the employees' ability to perform their job, or in some instances, make them ineligible for Government employment.

3.9.4. The suitability determination process does not stop at submittal, completion of the initial investigation, and the requisite suitability determination. It is a continuous evaluation process whereby the employee must maintain eligibility throughout the employment cycle. Subsequent receipt of reports of a derogatory or objectionable nature (e.g., DUI, illegal drugs, or criminal activity) shall also be evaluated for suitability concerns.

3.9.5. Established below are the processes and procedures required to ensure that the suitability requirement is appropriately managed for each NASA employee. These processes and procedures address two primary aspects of suitability determinations:

a. Entry On Duty (EOD) personnel security investigation and subsequent favorable adjudication for high, moderate, and low risk positions.

b. Report of derogatory or objectionable information subsequent to a favorable suitability determination or during required periodic reinvestigations for high, moderate or low risk positions.

3.9.6. Pre-appointment Checks for High Risk Positions.

3.9.6.1. Civil service positions that have been designated as High Risk as identified in subparagraph 3.5.2.1.a have major impacts on the success of NASA missions. Personnel placed in these positions must meet the highest standards of personal behavior. Upon selection, but prior to official appointment, the Center HRO shall direct the individual to complete the appropriate investigative forms per section 3.8 and return them to the Center HRO. The Center HRO shall review the forms for completeness and then forward them to the CCS for appropriate action. [NOTE: Required forms shall be made available via U.S. Mail or via an online forms management system (e.g., e-QIP)].

3.9.6.2. Upon review of information in the submitted forms the CCS may:

a. Interview the selectee to attempt to resolve any issues of concern;

b. Submit to the OPM for investigation and await final results; or

c. Approve interim favorable facility and/or IT access pending completion of final investigation and subsequent final suitability determination conducted by HRO.

3.9.7. Receipt of EOD Personnel Security Report of Investigation (ROI) from OPM.

3.9.7.1. Upon receipt of the Personnel Security ROI from OPM-FIPS or other investigative documents containing potential derogatory information, the CCS shall review the file.

3.9.7.2. If any suitability issues exist, the CCS shall verify that the coding of the issue(s) is consistent with OPM suitability criteria and that the file is complete. Inconsistent or incomplete cases shall be brought to the attention of OPM-FIPS, as appropriate.

3.9.7.3. The suitability issues shall then be referred to and adjudicated by the Center Human Resources Office per OPM and NASA policies and procedures.

3.9.8. Receipt of Derogatory or Objectionable Information Subsequent to a Favorable Employment Suitability Determination.

Follow the requirements outlined in subparagraph 3.9.7.2.

3.9.9. When a security clearance is being denied, revoked, or suspended as a result of a security determination, the CCS shall initiate the procedure set forth in chapter 2 of this handbook.

3.10 Adverse Information

3.10.1. When adverse information is developed or received in the course of any personnel security investigation, or subsequent to such investigation and initial favorable determination, the scope of inquiry will normally be expanded to the extent necessary to obtain sufficient information to make a sound determination that the employee may or may not be (or continue to be) employed by the Government.

3.10.1.1. 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 Government at NASA's request.

3.10.1.2. 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.

3.10.1.3. Appropriate signed releases from the subject shall be obtained when required to pursue some of these additional leads, e.g., medical records and credit checks.

3.10.2. 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 Security and Program Protection.

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

3.10.3.1. 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 Government at NASA's request.

3.11 Reinvestigation Requirements

3.11.1. Under the continuous evaluation program concept, the CCS shall establish processes and procedures for conducting timely reinvestigations of NASA employees to ensure maintenance of employment suitability. At a minimum, all Public Trust positions at the High Risk level shall be reinvestigated every five years or sooner for cause.

3.11.2. Personnel in Positions at the Moderate Risk level shall be reinvestigated every ten years or sooner for cause.

3.11.3. Positions at the Low Risk Level are subject to reinvestigation every ten years or sooner for cause, or at the discretion of the individual Center.

3.11.4. Re-investigations shall also be conducted upon position assignment change when the change involves moving to a higher risk level position. See subparagraph 3.5.2.3.

3.12 Recordkeeping

3.12.1. Records and information related to this chapter shall be managed per procedures established in chapter 2, section 2.18 of this NPR.

Chapter 4: NASA Personnel Security Program: Risk Designation Process, Background Investigations, and Access Determinations for NASA Contractor Employees

4.1 General

4.1.1. It is an inherent Government function under the "housekeeping" principles authorized by the U.S. Congress for a Government agency to protect its facilities and their occupants from harm and its information and technology from improper disclosure.

4.1.2. HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors, " requires appropriate investigation and adjudication for reliability prior to the issuance of permanent NASA photo-ID.

4.1.3. This chapter establishes position risk designation process, security investigative requirements, and reliability determinations for NASA contractors, Intergovernmental Personnel Act (IPA) personnel, grantees, research associates, co-op students, associated foreign nationals, lawful permanent resident(PARs), volunteers, (hereinafter known as contract employees), located on or within a NASA Center, component facility, or accessing NASA information systems remotely.

4.1.4. NASA contractor employees who are granted continuing and official unescorted access to Government facilities, buildings, information, and IT resources are subject to specific investigative requirements similar to the suitability determination requirements imposed by statute upon NASA Federal employees in chapter 3. This investigation provides NASA management necessary information to determine if an individual's fitness or eligibility to promote the efficiency of NASA's mission, initial access or continued presence on the installation, and access to unclassified IT resources is consistent with the safety and security of the U.S. Government, NASA, and the individual Center.

4.1.5. No NASA contractor employee shall be issued a permanent NASA photo-ID, granted access to NASA Centers or facilities, granted access to NASA IT systems, or sensitive information without, at a minimum, the completion of a NAC and submission of required investigative paperwork required to complete the" Inquiries" portion of the NACI, and interim favorable access determination by NASA Security Officials. (The NAC must be accomplished prior to or NLT than 10 working days after start of employment.)

a. Temporary photo ID or visitor badges, issued to contractor employees, who have not submitted the appropriate investigations forms, will expire at the 10 working day time period.

b. Further delays in forms submittal will require the individuals' supervisor to sponsor one-day visit requests up to an additional 5 working days. The supervisor will also be required to escort the individual.

c. Upon expiration of the additional 5 working days, all issued temporary badges/passes and

approved accesses will be terminated pending submittal of completed forms. Centers must establish the necessary procedures to ensure abuse of the visitor/temporary badging system does not occur.

4.2 Applicability

4.2.1. This chapter is applicable to NASA contracts, grants, cooperative agreements, and other binding agreements (MOA, MOU, etc.) that meet one or all of the following criteria:

4.2.1.1. For Services (research, operations, support);

4.2.1.2. Performed on or within Government facilities, and/or;

4.2.1.3. Require remote access to unclassified NASA IT Systems.

4.2.2. Unlike many Federal agencies, NASA's user community is a very diverse group which includes U.S. citizens, non-U.S. Citizens (lawful permanent resident (LPR's)) and Foreign Nationals) employed by NASA component facilities, contractor organizations, international partners working under the terms of an intergovernmental agreement, university partners working under a grant, individual personnel volunteering their services, private consultants, or other organizations providing support to NASA via memorandums of agreement (MOA) or memorandums of understanding (MOU).

4.2.3. The requirements of this chapter are designed to be equitable with the employment suitability criteria for NASA Civil Service employees, outlined in chapter 3, and shall be uniformly and consistently applied to ensure maximum protection of NASA assets.

4.2.4. Non-federal employees and contractor personnel of tenant organizations shall maintain Center access eligibility in accordance with this chapter and any Center specific processes and procedures established.

4.3 Responsibilities

4.3.1. The AA/OSPP is responsible for establishing and maintaining a viable and consistent personnel security program in accordance with current personnel security and suitability policies, procedural requirements, and guidelines, as established by the Office of Personnel Management (OPM).

4.3.2. Each Center Director is responsible for ensuring full Center compliance with the provisions set forth in this chapter.

4.3.3. All directors, program managers, line managers, and supervisors, using contractor services as described in paragraph 4.2 above, are responsible for ensuring the successful implementation of this chapter within the area of their authority.

4.3.4. The CCS shall assist, as necessary, in the individual contract and contract position risk designation process and shall establish written procedures for the following:

a. Maintaining and distributing forms, including instructions for the completion of all forms and documentation required for the personnel security reliability investigative process.

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

c. Exercising appropriate risk management authority when investigative results have not been

received in a timely fashion (normally within 90 - 120 days) requiring the need to make a decision to deny access, or grant interim or final access, as appropriate.

d. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation, as applicable.

e. Conducting local records checks (LRC) when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS.

f. Making appropriate notifications for:

(1) Confirmation of the results of a favorable access determination.

(2) Actions as a result of a non-favorable access determination.

g. Maintaining, in accordance with the Privacy Act and existing NASA system of records, individual personnel security files on all investigated personnel and reviewing 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 all investigative results,

(2) Any adverse information reports on affected contractor employees,

(3) Copies of documents pertaining to FN permanent residence or naturalization status.

4.3.5. The NASA General Counsel or the Chief Counsel of each Center, as appropriate, shall provide legal counsel with regard to implementation of this chapter.

4.3.6. Contract Management Officials (e.g., Contractor Management, COTR, Project Managers) shall ensure full compliance with this chapter.

4.4 Designation of Security Risk Levels

4.4.1. All contracts, grants, cooperative agreements, or other binding agreements (MOA or MOU) that meet the criteria in section 4.2 above, shall be categorized by security risk level. Each document shall include a security risk level designation of one of the following:

- High Risk;
- Moderate Risk; or
- Low Risk

4.4.2. The contract security risk level designations shall be made by the NASA Center program office representative (typically the designated Civil Service project manager (sponsor) or COTR), in coordination with the CCS, appropriate IT Security Manager(s), and contractor HR Offices. The parties shall review the work to be performed and, following the process flow established in Appendix N " Determining Position Risk and Sensitivity Levels, Process Flow Chart" and assign the highest security risk designation in accordance with the criteria established in Appendix M, "Designation of Public Trust Positions and Investigative Requirements."

4.4.3. The security risk level is determined by evaluating the sensitivity and risk of the work being performed and accesses required by the contractor and the potential for damage to NASA's mission and operations if performed inefficiently, ineffectively, or in an unsafe or unethical manner. Included in this 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. Section 4.6.2 and 4.6.5.1 is applicable.

4.4.4. The risk level, in turn, determines the investigative requirements for the contractor personnel who shall perform the work.

4.4.5. The sponsoring program or project office shall ensure the contractor meets the requirements of this chapter.

4.5 NASA Contractor Employee Position Risk/Sensitivity Level Criteria and Designation Process

4.5.1. Security risk levels for contracts, grants, cooperative agreements, and MOA or MOU shall be established by program or project management and contractor management who, in coordination with the CCS, the IT System Line Manager, and IT System Security Administrator, shall review the work to be performed under the contract or grant and assign to the entire contract, grant, cooperative agreement, MOA, or MOU the highest security risk designation in accordance with the criteria established in this section.

4.5.2. Accordingly, each individual NASA contractor employee shall undergo security screening processing according to the contract, grant, MOA, MOU, and individual position risk designation levels as determined using the criteria in this section and the process flow established in Appendix N " Determining Position Risk and Sensitivity Levels, Process Flow Chart" and Appendix M, this NPR.

4.5.3. In instances where there is a wide variance in the security risk level of the work to be performed under a contract, grant, MOA, MOU, or other binding agreement, individual contractor employees must be processed at the risk designation commensurate with 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.

4.5.4. The contractor shall identify the employees to be processed at each risk designation and shall specify the duties of the positions. 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 security area designation that requires a higher degree of trust.

4.5.4.1. 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.

4.5.4.2. 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.

4.5.5. 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 (e.g., IT-6C = 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.

4.5.6. Position risk level determinations are inclusive of many factors. Generally, they are

represented in the categories below:

a. **High Risk** positions involve duties that are especially critical to the Agency and its programs and operations, with a broad scope of policy or program authority such as policy development and implementation; higher level management assignments; and/or non-management positions with authority for independent action. High Risk positions may also include national security positions as described Chapter 6.

b. **Moderate Risk** positions involve duties of considerable importance to the Agency and its programs and operations with significant program and/or operational responsibilities such as: assistants for policy development and implementation; mid-level management assignments; non-management positions with authority for independent or semi-independent action; or positions that demand public confidence or trust. Moderate Risk positions may also include national security positions as described in Chapter 6.

c. **Low Risk** positions involve duties with limited relations to the Agency and its programs and operations and which have little affect on the efficiency of the Agency's programs and operations. Low Risk positions may also include national security positions as described in Chapter 6.

d. Provided below are categories of positions and/or specific duties that are unique to NASA and therefore, may influence the risk level designation for each individual position.

(1). Information Technology (IT) Resources Positions.

(a). In accordance with the Federal Information Systems Management Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, and NPR 2810.1, NASA has established personnel security requirements and procedures to assure an adequate level of protection for NASA IT systems, which includes the appropriate screening of all individuals having access to NASA IT systems.

(b). The level of reliability checks or investigations range from a NACI to a full-field background investigation, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual.

(1) **High Risk or 6C** positions include positions in which the incumbent is responsible for planning, directing, and implementing a computer security program; has major responsibility for directing, planning, and designing an IT system, including development activity associated with hardware and software; or, can access a system with relatively high risk for causing grave damage or realizing a significant personal gain. High Risk IT positions may include positions that involve:

(a) Developing or administration of Agency IT Security Programs, directing or controlling IT risk analysis and threat assessments, or conducting investigations.

(b) Significant involvement in life-critical or mission-critical systems (see paragraph 4.6.;

(c) Privileged access to Mission Essential IT Systems (See section 4.7. for further requirements).

(d) Access to data or systems whose misuse can cause very serious adverse impact or result in significant personal gain.

(e) Assignments involving accounting, disbursement, or authorization of $10 million dollars or more per year.

(f) Privileged access to IT systems whose misuse can cause "significant adverse impact" to NASA missions. These systems include those that interconnect with a NASA network in such a way as to enable the user to bypass firewalls or systems operated by a NASA contractor whose function and

data has substantial value, even if these systems are not interconnected to a NASA network. (NOTE: Foreign Nationals (FN) are not authorized to have "Privileged" access to NASA IT Systems. The only exception is an FN who is involved in an international program or project under an International Space Act Agreement (ISAA). IT System Line Managers contemplating the granting of such access shall consult with their Center Export Administrator and Center International Visit Coordinator (IVC) to ensure that an ISAA is in place, that the ISAA includes such a requirement, and that the international program or project involved certifies the need for such access.)

(2) **Moderate Risk or 5C** positions include positions where the incumbent is responsible for directing, planning, designing, operating, or maintaining IT systems and whose work is technically reviewed by a higher authority (at the high risk level) to insure the integrity of the system: Moderate risk IT positions may involve:

(a) Systems design, operation, testing, maintenance, or monitoring which is under technical review of IT-1 and includes:

(1) Those that contain the primary copy of data whose cost to replace exceeds $1 million.

(2) Those that control systems which affect personal safety and/or physical security, fire, or Hazmat warning safety systems.

(3) Privileged information on contract awards in excess of $10 million.

(4) Accounting disbursement or authorization of more than $1 million, but less than $10 million per year.

(b) Access to data or systems whose misuse can cause serious adverse impact or result in personal gain.

(1) Proprietary data:

(2) Privacy Act protected information:

(3) Export Control Regulations (EAR), International Traffic in Arms Regulations (ITAR), and the Militarily Critical Technologies List (MCTL) information.

(c) "Limited privileged" access to IT systems whose misuse can cause "adverse impact" to NASA missions. [NOTE: Foreign Nationals (FN) are not authorized to have "Limited Privileged" access to NASA IT Systems. The only exception is an FN who is involved in an international program or project under an ISAA. IT System Line Managers, contemplating the granting of such access shall consult with their Center Export Administrator and Center International Visit Coordinator (IVC) to ensure that an ISAA is in place, and that the ISAA includes such a requirement, and that the international program or project involved certifies the need for such access.]

(3) **Low Risk or 1C** positions are all IT system positions that do not fall in the categories above and includes 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:

(a) General word processing;

(b) Systems containing no IT-I or IT-II level information or IT-1 or IT-2 level information that is protected from unauthorized access.

(c) Positions that provide for no privileged or limited privileged access or do not afford IT-1 or IT-2 access. Includes: Systems that contain Sensitive But Unclassified (SBU) as described in chapter 5,

section 5.24. These requirements do not apply to NASA web-pages established for general public access. These web-pages are prohibited from containing classified information or NASA Sensitive But Unclassified (SBU), or providing unprotected links to NASA "Private" domains.

(4) Specific requirements and criteria for designating Computer/ADP risk levels are contained in Appendix M.

(2) CHILDCARE WORKER EMPLOYEE RELIABILITY INVESTIGATIONS (42 U.S.C. 13041) - Reliability investigations are to be completed on all childcare providers prior to working in NASA-sponsored childcare facilities.

(a) Personnel shall work under regular and continuous observation by a favorably investigated employee pending completion of the investigation.

(b) 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.

(c) Per OPM Federal Investigations Notice #98-06, Subject: "Child Care Provider Investigations," Centers shall use the services of OPM to conduct these investigations.

4.5.7. When a NASA contractor employee's duties require any overlap into a higher or lower risk level, the position sensitivity designation must then be set at the highest risk level anticipated.

4.5.8. Personnel investigated and favorably adjudicated within the previous 3 to 5 years under the provisions of Chapter 6 of this NPR may be considered fully qualified to occupy any position established under this chapter.

4.6 Contractor Coordinated Background Investigations for U.S. Citizen Employees

4.6.1. With the exception of the NASA Child Care Center program, obtaining background investigations for each contractor employee (U.S. Citizen only) at the **Low** and **Moderate Risk** Levels are to be the responsibility of the contractor at some time in the near future when the Federal Acquisition Regulations (FAR) are updated to reflect this new mandate. Therefore, this section will apply only after the FAR is updated and implemented.

a. Pending update and implementation of the FAR, section 4.7. is applicable.

b. Investigations may only be conducted by the Office of Personnel (OPM) or Defense Security Service (DSS) at the request of the contractor. The investigations conducted by OPM or DSS follow the requirements of all pertinent Federal statutes, regulations, executive order, and presidential directives and fully meet the requirements of this chapter. Refer to Chapter 10 for definitions of the various types of investigations required. Results of investigations will be made available to the CCS through the DSS.

4.6.2. NASA shall conduct the appropriate security screening for all foreign national contractor employees regardless of the position risk level designation and access requirements.

4.6.3. Position Risk Designation Management for Non-U.S. Citizens (Foreign Nationals and Permanent Resident Aliens) **(See Section 4.10 for overall guidance on Foreign National contractor employee security screening.)**

a. Non-U.S. citizens (including lawful permanent residents (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/OSPP 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/OSPP via the CCS. The request shall:

(1) Specify why it is impractical or unreasonable to use U.S. Citizens to perform the required work or function.

(2) Define the individual's special expertise.

(3) Define the compelling reasons for the request.

b. The CCS shall review the request for accuracy, endorse or non-endorse it, and forward it to the AA/OSPP.

c. The AA/OSPP shall coordinate with the Office of External Affairs for concurrence (Export Compliance), and if approved, shall return it to the requestor. A copy shall be retained in the OSPP and CCS files.

4.6.3.1. A completed background investigation and favorable adjudication are required before the position may be occupied and access granted. Foreign National personnel must:

a. Be entered into the NASA Foreign National Management System (FNMS) by the sponsoring organization and processed by the Center International Visits Coordinator (IVC) to ensure they:

b. Have legal visa status with the U.S. Citizenship and Immigration Services (USCIS) and U.S.-VISIT Program.

c. Have advance sponsorship and concurrence from Program Management, Center International Visits Coordinator (IVC), CCS, Center Export Administrator (CEA), appropriate System Administrator, and IT Security Manager(s).

d. Undergo a review of Central Intelligence Agency (CIA), U.S. Department of State, and Bureau of Immigration and Customs Enforcement (BICE) databases as necessary and available.

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

4.6.4. The AA for Security and Program Protection may waive some, or all, investigative requirements for representatives of foreign Governments who request, in writing, access to NASA IT systems pursuant to an intergovernmental agreement. Access shall be limited to that which is necessary to execute the agreement.

4.6.4.1. Foreign national personnel with approved placement in **High Risk** positions shall be closely monitored. All personnel shall be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

4.6.4.2. Any requests for FN access to sensitive information owned by another agency must be coordinated with and approved by that agency.

4.6.5. Subsequent reinvestigative requirements established in section 4.16 remain in effect.

4.7 Contractor Personnel Security Background Investigations Conducted by NASA

4.7.1. Per FIPS 201 NASA is responsible for ensuring appropriate investigations are conducted and access suitability determined for all contractor personnel.

a. When the contractor has not accomplished the required background investigations the Center CCS must ensure the appropriate investigation is conducted, in the following manner:

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

(2). The COTR shall notify the CCS who shall make the necessary blank investigative forms, identified in section 4.8, available to the contractor. Forms shall be made available using the web-based e-QIP system).

4.7.2. The NASA contractor employee shall complete and submit the forms, with appropriate written releases of the Government from liability, to the CCS through the use of electronic web-based investigative forms as stated in paragraph 4.8.

4.7.3. The timing of security form submittal and the established risk level may dictate whether a proposed NASA contractor employee can begin work prior to a final access determination. Based on the specifics of the situation and a preliminary review of the submitted forms, the CCS shall advise the COTR whether the individual can commence working prior to the receipt of the completed investigation and final access determination.

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

4.7.4.1. Upon selection, but prior to assignment, the Contracting or Grants Officer shall direct the NASA contract employee or company to complete the required security investigative forms for the High Risk position (refer to section 4.8) and return them to the CCS for review and investigative action.

.7.4.2. Upon review of information in the completed forms, the CCS may:

a. Interview the prospective NASA contractor employee to resolve any issues; or,

b. Request investigation through NASA channels and await final results; or,

c. Conduct further screening, as appropriate to resolve any issues; or,

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

e. Deny access and take the necessary actions per section 4.11.

4.8 Forms Required to Request an Investigation

ACTION	LOW RISK POSITION	MODERATE RISK POSITION	HIGH RISK POSITION
NON-NASA PERSONNEL	NACI/No Access SF 85 - e-QIP OFI Form 79B, FC 258	NACI/No Access SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization	BI SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization and Release of

		and Release of Credit Reports)	Credit Reports)

4.9 Adjudication Process for Access

4.9.1. When the results of the completed personnel security investigation has been made available, the CCS shall determine if the individual is eligible for the type of accesses required for the work.

4.9.1.1. In cases that contain significant adverse information, the personnel security investigation is not complete until a subject interview described in section 4.11.3 has been conducted.

4.9.1.2. The CCS, or designee, shall make the final determination based on the results of the DSS investigation

4.9.2. All personnel involved in the adjudication process shall be trained in adjudication methods and shall keep their training current. NASA shall follow established OPM suitability adjudicative guidelines in order to determine a contractor's suitability status. The process shall examine the facts in the investigation and result in a determination that an individual is or is not eligible for access, or continued access, to NASA facilities, information, or IT systems.

4.9.3. When adverse information becomes known about a NASA contractor employee who already has access to NASA facilities or IT systems and the initial Entry on Duty (EOD) required personnel security reliability investigation has been completed and favorability adjudicated, the adjudicator shall consider whether the individual:

- Voluntarily reported the information;
- Was cooperative, truthful, and complete during the investigation;
- Sought assistance and followed professional guidance;
- Resolved or appears likely to favorably resolve the concern;
- Has demonstrated positive changes in behavior and employment.

4.9.4. The CCS may approve conditional access based on mitigating factors. The CCS may also require written agreements with the NASA contractor employee certifying that any future adverse actions would be grounds for immediate revocation of access.

4.9.5. If the CCS decides to deny or revoke access, the CCS shall notify the individual, formally and in writing, of NASA's decision and include the reasons that were used to make the determination. The individual shall also be informed of the provisions of the Privacy Act and the Freedom of Information Act and how to obtain official copies of any pertinent investigation.

4.9.6. If a final decision to deny or revoke access is made, the CCS shall notify the contractor through the COTR and the CO that the individual is not eligible for the needed access.

4.9.6.1. The CO shall inform the NASA contractor of NASA's decision and provide a statement that NASA's decision is not intended to imply that the individual's employment elsewhere in the company should be affected.

4.9.6.2. Adverse information shall not be disclosed to the individual's employer since it could affect the individual's employment and possibly subject NASA to legal liability.

4.9.7. NASA Security Offices, in consultation with responsible program officials and IT Security Managers, may grant interim access to NASA facilities and IT systems, if the submitted forms do not contain adverse or questionable information.

4.9.8. NASA reserves the right to immediately and unilaterally revoke or suspend such interim access in the event that adverse information is developed.

4.10 Escort Requirements in Lieu of Completed Favorable Background Investigations

4.10.1. While the most desirable procedure for the utmost safety and security of NASA personnel and facilities would be total escort of non-affiliated personnel (visitors, unscreened contractors, delivery personnel, Foreign Nationals, U.S. Representatives of Foreign entities, etc.), this NPR recognizes the limitations and potential cost associated with such a policy.

4.10.2. U.S. Citizens: Each Center shall develop and implement procedures for the proper escort of non-affiliated U.S. citizen visitors and NASA contractor employees when the completion and receipt of an appropriate personnel security reliability investigation is not readily available and the visit is under 30 days or is intermittent that would warrant the submission of, at a minimum, a NAC investigation. Decisions not to escort shall be made by the CCS, supported by appropriate consideration of the risk involved, the areas and information to be accessed, availability of certification by the individual's employer that the appropriate reliability investigation has been conducted, and the implementation of compensatory security measures, as appropriate, to prohibit unauthorized access.

4.10.3. Foreign Nationals (FN): FN visitors, representatives, or contractor employees (including permanent resident aliens) requiring access to a NASA Center for a period exceeding 30 days shall be managed in accordance with the following requirements:

a. Due to the strict investigative requirements for positions designated at the High Risk level, foreign nationals will not normally be eligible to assume duties designated at High Risk. Sponsors desiring to place a foreign national in a high risk position must follow the procedures established in section 4.6.3 of this NPR.

b. All foreign nationals from designated and non-designated countries shall be escorted at all times pending the completion of the requisite personnel security reliability investigation and favorable determination.

c. Upon a favorable determination, individual compensatory security measures (e.g., information/data access, on-Center movement restrictions) in the form of a written agreement titled, "Security/Technology Control Plan," shall be developed, agreed upon, and signed by the individual FN visitor, visit sponsor, Center Export Administrator, International Visits Coordinator, and CCS.

(1) FN visitors, representatives, or FN contractor employees (including PRA's) from a non-designated country shall not be granted unescorted access privileges to NASA Centers after normal working hours unless specifically justified and included in the Security/Technology Control Plan. See Appendix K for a Security/Technology Control Plan Template.

(2) FN visitors, representatives, or FN contractor employees (to include PRA's) from designated countries shall not be granted unescorted access privileges to NASA Centers after normal working hours unless the employee can be effectively monitored and appropriate controls implemented that establishes strict accountability during the access period. Establishment of movement and access controls must be document in a Security/Technology Control Plan. See Appendix K for a Security/Technology Control Plan Template.

(3) Compliance with the FN access plan must be validated by the Center security office through periodic random visits by security personnel.

(4) Violations of established FN visit protocols will be properly investigated by Center CI agents, and action taken, including termination of visit or access, when warranted. All violations of FN visit protocols will be reported to the Director, Safeguards Division.

(5) Security/Technology Control Plans shall be reviewed for continued applicability upon changes in visitor status (e.g., visit extension/renewal, new project parameters, etc.).

4.10.4. Foreign National visitors, representatives, or contractor employees who are visiting 30 days or less, and for which the cost and time of conducting a satisfactory security reliability check may not be warranted, shall be escorted at all times unless a previous satisfactory investigation has been conducted within the last 3 years. Escorts must be permanently NASA photo-ID'd Civil Service employee or Contractor Employees possessing U.S. Citizenship.

4.10.5. Foreign national visitors of less than 30 days, working under an implemented International Space Act Agreement (ISAA) as defined in NPD 1050.1G, "Authority to Enter Into Space Act Agreements," NPD 1360.2A, "Initiation and Development of International Cooperation in Space and Aeronautics Programs," and NPR 1050.1, "Space Act Agreements," must be escorted by a permanently assigned NASA photo-ID'd U.S. citizen or a NASA permanently assigned NASA photo-ID'd foreign national currently working under an ISAA (e.g., FN Astronauts, ISS, etc.) . E scorts by a Foreign National or U.S. person (LPR) under this paragraph is permitted only in those areas authorized by the ISAA .

4.11 Adverse Information

4.11.1. When adverse information is 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 determination that the contractor shall or shall not be (or continue to be) granted access to NASA facilities or IT systems.

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

4.11.1.2. Investigative expansion may consist of many different lines of inquiry, including but not limited to, interviews of the subject, supervisors, co-workers, neighbors, physicians, records checks with various local agencies, and credit checks.

4.11.1.3. Releases from the subject shall be obtained when required to pursue additional leads (e.g., medical records and credit checks).

4.11.2. 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 Security and Program Protection.

4.11.3. A NASA contractor employee on whom significant unfavorable or derogatory information has been developed or received during the personnel security reliability process must be confronted with the information and offered an opportunity to refute, explain, clarify, or mitigate the information in question prior to final access determination.

4.12 Tenant Organization Employee and Contractor Reliability

4.12.1. NASA Centers hosting tenant organizations necessitating access to tenant facilities located in Center controlled areas shall establish appropriate processes and procedures to ensure full compliance with this chapter.

4.12.2. Approval for accessing tenant facilities does not constitute authority for accessing NASA facilities unless authorized by local center policy.

4.13 Reinvestigation Requirements

4.13.1. At a minimum, reinvestigations conducted under this chapter shall be conducted every 5 to 7 years, or sooner for cause, for all High and Moderate Risk contractor, grantee, MOA, or MOU positions to ensure maintenance of eligibility under the Continuous Evaluation Program (CEP) for access to NASA Centers , facilities, and information.

4.13.2. Positions at the Low Risk Level are be subject to reinvestigation every 10 years, at any time for cause, or at the discretion of the individual Center.

4.13.3. Re-investigations shall also be conducted upon position assignment change when the change involves moving to a higher risk level position.

4.13.4. All reinvestigations, except those conducted as a result of moving to a higher risk level position, will be comprised of a National Agency Check with Inquiries (NACI), local records check, as necessary, and personal interview by a qualified investigator, as necessary.

4.14 Recordkeeping

Records and information related to this chapter shall be managed per procedures established in chapter 2, section 2.18 of this NPR.

Chapter 5 was cancelled by NPR 1600.2 on October 11, 2011

Chapter 5. Classified National Security and Sensitive but Unclassified (SBU) Information Management

5.1 General

5.1.1. NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified/nonsensitive nature with few restrictions on its use and dissemination.

5.1.2. NASA also generates, receives, stores, disseminates, and maintains classified national security information (CNSI) under a variety of Agency programs, projects, and through partnerships and collaboration with other federal agencies, academia, and private enterprises.

5.1.3. In accordance with EO 12958, "Classified National Security Information," as amended, this chapter establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA.

5.1.4. Nothing in this chapter or the applicable EO limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act of 1974, and the National Security Act of 1947.

5.1.5. This chapter also establishes a uniform process whereby sensitive but unclassified (SBU) NASA information, known as "Administratively Controlled Information (ACI)," is identified and properly managed to ensure disclosure to unauthorized persons is effectively prohibited.

5.1.6. Further, this chapter defines the security review requirements for programs and projects, pursuant to NPR 7120.5 series, and establishes procedures for the creation of Security Classification Guides (SCG), as well as requirements for reviewing permanent historical documents, pursuant to NPR 1441.1 series, for continued classification before retirement into Federal Records Centers (FRC) or the National Archives and Records Administration (NARA).

5.2 Responsibilities

5.2.1. Per ISOO Directive 1, Section 2001.61(b)(6)(iii)(E), the Administrator will ensure that individual performance plans will include management of classified information as a critical element for "cleared" personnel whose duties "significantly involve the creation or handling of classified information." In this context, "significant involvement" means at least 50% of duty time is involved in activity related to accessing, creating, or handling CNSI.

5.2.2. The AA/OSPP is responsible for providing direction and oversight for an Agency-wide administrative security program and implementation of EO 12958 for the protection of CNSI and SBU in NASA's custody. He/she shall:

5.2.2.1. Establish Agency-wide procedures pertaining to the management of CNSI and material, and

ACI generated by or in the custody of NASA.

5.2.2.2. Periodically review Center procedures and systems to ensure CNSI and ACI are properly protected against unauthorized disclosure or access.

5.2.3. Center Directors are responsible, through the CCS, for ensuring proper planning and implementation of EO 12958, and managing classified information and material and ACI under the jurisdiction and custody of their respective Centers. This responsibility includes component activities geographically separated from the parent Center.

5.2.4. The CCS shall ensure an information security program for CNSI is developed, implemented, and maintained at a level sufficient to meet the requirements of this chapter and national level requirements. This includes:

5.2.4.1. Developing and implementing appropriate processes and procedures for classifying NASA information per EO 12958 and other national level requirements.

5.2.4.2. Developing and implementing appropriate processes and procedures for automatic declassification per EO 12958.

5.2.4.3. Developing and implementing procedures for the appropriate safeguarding of CNSI and ACI.

5.2.4.4. Conducting periodic reviews of NASA organizational units involved in classified work and storage of classified material to ensure compliance with EO 12958, this NPR, and any applicable local procedures. Reviews shall be conducted in a manner that meets the intent of ISOO Directive No.1, Subpart C, and shall be reported in Block 9 of Standard Form 311, Agency Security Classification Management Program.

5.2.4.5. Promptly and fully determining the circumstances surrounding any loss or possible compromise of classified information or material and initiating appropriate investigative action.

5.2.4.6. Establishing more stringent standards, specifications, procedures, or guidelines when special conditions or circumstances arise that indicate increased safeguards are necessary in the interest of national security.

5.2.5. NASA supervisors at all levels shall ensure that all personnel entrusted with classified information or material are fully knowledgeable of and comply with the provisions set forth in this NPR and established National level policies governing accessing, protecting, accounting for, and safeguarding classified information and material, and that management of classified information be included in individual performance plans as a critical element .

5.2.6. Employees entrusted with CNSI shall immediately report the following to the CCS:

5.2.6.1. Loss or suspected compromise of classified information or material.

5.2.6.2. Known or suspected practice or condition that compromises the proper safeguarding and handling of classified information or material.

5.2.6.3. Attempts by uncleared personnel, or personnel with no need-to-know, to gain access to CNSI.

5.2.6.4. Initial classification, downgrading, or declassification actions associated with NASA generated information or material.

5.2.7. All personnel entrusted with CNSI are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. This will be accomplished

by:

a. Submit in writing, to the CCS, the justification for the challenge.

b. Ensure the written challenge carries the same classification level as the original. Control as classified information.

c. The CCS will review and, where necessary, consult the original classification authority, to assist in determining the merits of the challenge, and:

(1). Grant the challenge and adjust the classification level as appropriate, or;

(2). Deny the challenge, provide rational for the denial, as appropriate, or;

(3). Refer the challenge the challenge to the NASA Information Security Program Committee who will make the final Agency determination, or;

(4). The NASA Information Security Program Committee may refer the challenge to the Information Security Oversight Office (ISOO) for final determination.

5.3 Agency Information Security Program Data Report, SF-311

Annual SF-311 reports are required at the end of each fiscal year. The reporting period is from October 1 to September 30. The CCS shall submit an unclassified report to the Director, NASA Security Management Office, no later than October 15 following the reporting period.

5.4 Classifying, Marking, and Declassifying CNSI

5.4.1. Classification. Information is classified pursuant to EO 12958 by an Original Classification Authority and is designated and marked as Top Secret, Secret, or Confidential. Except as provided by statute, no other terms may be used to identify classified information.

5.4.1.1. Classification challenges. Authorized holders of classified information wishing to challenge the classification status of information shall present such challenges, per subparagraph 5.2.7, to the Director, Security Management Division (DSMD), Office of Security and Program Protection (OSPP). Once the challenge is received, a determination will be made to submit the challenge to an original classification authority with jurisdiction over the information. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level. An attempt shall be made to keep all challenges, appeals and responses unclassified. However, if it's necessary to include classified information into a challenge, please contact your local Security Office to assist you with preparing the classified challenge. The following procedures will be followed when processing a challenge:

a. The DSMD shall provide an initial written response to a challenge within 60 days.

b. If the DSMD is unable to respond in 60 days, the challenge will be acknowledge in writing and the letter will include a response date.

c. The challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision.

d. The challenger may also forward the challenge to the ISCAP if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal.

e. If a challenge is denied, the challenger will be made aware of their appeal rights to ISCAP.

5.4.2. Original Classification Authority (OCA). Agency personnel with OCA designation are identified in 14 CFR, Section 1203.800, Delegation of Authority to Make Determinations in Original Classification Matters. The following NASA personnel possess OCA designation:

5.4.2.1. NASA Administrator - Up to and including Top Secret.

5.4.2.2. Deputy Administrator - Up to and including Top Secret.

5.4.2.3. Associate Deputy Administrator - Up to and including Top Secret

5.4.2.4. Associate Deputy Administrator for Technical Programs - up to and including Top Secret.

5.4.2.5. Assistant Administrator for Security and Program Protection (AA/OSPP) - up to and including Top Secret.

5.4.2.6. Director, Security Management Division (DSMD) - up to and including Top Secret.

5.4.2.7. NASA Inspector General (Non-delegable) when so designated in writing - up to Secret.

5.4.2.8. Center Chiefs of Security when so designated, in writing, by the AA/OSPP - up to Secret.

5.4.2.9. Other personnel, with sufficient justification, as designated in writing by the AA/OSPP - up to Secret.

5.4.3. Marking for Original Classification.

5.4.3.1. Personnel shall not designate information as classified (Confidential, Secret, or Top Secret) unless specifically approved by the CCS or an individual having OCA.

a. Physically marking classified information with the appropriate classification markings clearly warns and informs people of their responsibility to protect it.
b. Other notations facilitate downgrading, declassification, and aid in derivative classification actions.

5.4.3.2. Overall markings along with page, component, portion markings, and use of cover sheets shall conform to guidelines established by the CCS in accordance with EO 12958 and promulgated in Chapter 8, "Classified Correspondence," NPR 1450.10C, "NASA Correspondence Management and Communications Standards and Style."

5.4.3.3. Documents classified under any previous EO need not be remarked to comply with current marking requirements.

5.4.4. Marking for Derivative Classification.

5.4.4.1. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a classification guide issued by an original classification authority. Persons who apply derivative classification markings shall observe and respect original classification decisions, carry forward to any newly created documents the pertinent classification and declassification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward, the date or event for declassification that corresponds to the longest period of classification among the sources and a listing of the sources on or attached to the official file or record copy. Users can also use classification guides for derivative classifying. Center

Security Office will be prepared to provide assistance as requested. The CCS will ensure they have access to the ISOO Marking Classified National Security Information Pamphlet www.archives.gov/isoo/ and other guidance.

5.4.4.2. Markings other than "Top Secret", "Secret", and "Confidential," such as "For Official Use Only," "Sensitive But Unclassified," ":Limited Official Use," or "Sensitive Security Information," shall not be used to identify Classified National Security Information (CNSI). Foreign Government documents shall contain the country of origin or FGI. If the identity of the specific government must be concealed, the document shall be marked, "This Document Contains Foreign Government Information," and pertinent information marked "FGI", together with classification level, e.g., "(FGI-C)."

5.4.4.3. As required, the CCS shall develop and issue appropriate requirements on derivative classification actions and procedures.

5.4.4.4. Mark documents containing Foreign Government Information with: "This document contains (country of origin) Information." Mark the portions that contain the foreign government information to indicate the country of origin and the classification level. Substitute the words "Foreign Government Information" or "FGI" in instance in which the identity of the specific government must be concealed. Note: If the fact that information is foreign government information must be concealed, the markings described here shall not be used and the document shall be marked as if it were wholly of U.S. origin. Your Center Security Office can provide you with information and pamphlets on how to properly mark all classified information.

5.4.5. Special Access Program (SAP) Markings. NASA employs SAP markings that are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG) concerning national security information for limiting access to cleared personnel having a need-to-know in the performance of their official duties.

5.4.6. Sensitive Compartmented Information (SCI). The NASA Special Security Office (SSO) must review for appropriate classification and marking any document for interagency use (MOU/MOA, Memorandum, or general correspondence) involving SCI or suspected SCI produced without the benefit of a specific classification guide.

5.4.7. Declassification and Downgrading.

5.4.7.1. In accordance with E.O. 12958, as amended, all Classified National Security Information (CNSI) records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under Title 44, United States Code, shall be automatically declassified on December 31, 2006, whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification unless the information falls under one of the (9) exemption categories in E.O. 12958, as amended. If that is the case, a decision will be made to continue classification of the information. Pursuant to the Atomic Energy Act of 1954 as amended and 50 USC 435, all NASA Declassification Authorities (DCA) must successfully complete the Department of Energy (DoE) training on the recognition of restricted data and formerly restricted data (RD/FRD). Upon nomination to the AA/OSPP by an AA, or Center Director/Chief of Security, and completion of the required DoE training, individuals may be granted DCA.

5.4.7.2. The DSMD has developed the NASA Declassification Management Plan which provides the framework for NASA compliance with Section 3.3 through 3.7 of E.O. 12958, as amended. The NASA Declassification Plan will cover the following: Purpose, Legal Basis and Authority, 25 year Automatic Declassification, Systematic Declassification Review, Mandatory Declassification Review, Declassification Review Technique, RD/FRD review, Special Media Records, TS, TS/SCI,

SAP Material review, Classification and Declassification Guides, Foreign Government Information, Declassification vs. Release, NASA Records Retention Schedule, NASA Handbook for Preparing Security Classification Guides, NASA Security Classification Guides, NASA Original Classification Authority, NASA Declassification Authority, Major Subject Matter/Equity Headings, Classification/Declassification Glossary, 25 year Automatic Declassification Exemptions, NASA Declassification Review and Referral Handbook, Review and Referral procedures, Declassification Authorities and NASA Staff contacts. NASA DCAs may only declassify NASA-originated classified national security information (CNSI).

5.4.7.3 An agency head may exempt from automatic declassification classified national security information, a group or file series "EXEMPT FILE SERIES" (A "file series" is also described in Information Security Oversight (ISOO) guidance as an "integral file block.") of records if the release of a substantial portion of the records within the file series would be expected to remain exempt based on the provisions of E.O. 12958, as amended, Section 3.3. (b) and (c). E.O. 12958, as amended, Section 3.3. (d) states: At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) E.O. 12958, as amended, Section 3.3., that the agency proposes to exempt from automatic declassification. File series exemptions were approved by ISOO in 1996 pursuant to the E.O.12958, signed in April 1995, and did not have to be re-approved under E.O. 12958, as amended, signed in March 2003. File series exemption criteria include the following:

a. a description of the information, either by reference to information in specific records or in the form of a declassification guide

b. an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time

c. except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of E.O. 12958, as amended, Section 3.3., a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

5.4.7.4. The following Agency personnel have declassification and downgrading authority.

5.4.7.4.1. As OCAs for the Agency, individuals listed in 5.4.2.1. through 5.4.2.6. are also authorized to declassify NASA-originated CNSI.

5.4.7.4.2. Other individuals who hold a signed letter of designation as a DCA for their directorate, office, or Center. All letters of designation must be signed by the AA/OSPP.

5.4.8. When conducting yearly reviews of classified holdings for automatic declassification as required under EO 12958, the CCS shall ensure declassification authority is assigned, per subparagraph 1.1.7.11, to qualified federal employee personnel subject matter experts and shall assist them in declassification efforts, as appropriate.

5.5 Access to CNSI

5.5.1. At a minimum, NASA personnel and other individuals associated by contract or other agreement shall meet the following criteria for accessing CNSI:

5.5.1.1. Possess a personnel security clearance commensurate with the required access. (Reference chapter 2 and chapter 6 of this NPR).

5.5.1.2. Have a justified need-to-know.

5.5.1.3. Must have signed an official nondisclosure statement (SF 312) witnessed by a NASA security official.

5.6 Accountability and Control of CNSI

5.6.1. Accountability of classified information is essential to maintaining a history of what you have, where it is, and who has it. Through effective accounting procedures it must be possible to trace the movement and detect the loss of classified information in a timely manner.

5.6.1.1. All CNSI information shall be strictly accounted for and covered by a continuous chain of signature receipts. However, this chapter represents the MINIMUM requirements for accountability and control. Centers are encouraged to implement additional controls they deem appropriate.

5.6.1.2. Each Center shall have an information management system and set of written procedures to control the classified information in its possession. The system or procedures shall contain specific requirements for accounting and safeguarding CNSI. The system shall be sufficient to reasonably preclude the possibility of its loss or compromise.

5.6.2. A trained Top Secret Control Officer (TSCO) and Alternate shall be designated, in writing, by the Center Director or CCS. The TSCO shall ensure that all Center TS material is accounted for, protected, and transmitted under a chain of receipts using NASA Form 387, "Classified Material Receipt," identifying each individual with custody of the material.

5.6.3. A trained Classified Material Control Officer (CMCO) and Alternate shall be designated in writing by the Center Director or CCS. The CMCO shall ensure that all Center CNSI material is accounted for, protected, and transmitted under a chain of receipts using NASA Form 387, "Classified Material Receipt," for each individual with custody of the material. Upon written designation by the Center Director or CCS, the CMCO, as well as his/her alternate, may also serve as the TSCO.

5.6.3.1. The CMCO is responsible to the CCS for the Center Security Control Point (SCP) and oversight of the Document Control Stations (DCS) within the Center and/or facilities.

5.6.3.2. Establishment of Security Control Point (SCP). One SCP, operated by the CMCO, shall be established within each Center or facility that has a requirement to handle classified information. The SCP shall be designated in writing within the local security Procedural Requirements. All incoming and outgoing classified information shall be processed through the SCP with the following exceptions: Sensitive Compartmented Information (SCI) material, CMS material, and classified messages that are handled, processed, and stored within secure telecommunications spaces.

5.6.3.3. Document Control Station (DCS). At a Center with a significant volume of classified material and where the SCP serves many organizations, each organization which has or shall have custody of classified material shall establish a DCS run by a Document Control Station Officer (DCSO). Organizationally, this station may be established at the office, division, staff or lower level depending upon the circumstances. Creation of such stations shall be coordinated with the CMCO, and approved in writing by the CCS.

5.6.4. Accountability records.

5.6.4.1. All CNSI must be accounted for throughout its lifecycle. Records shall be maintained for all CNSI and retained for five years after final disposition. These records shall be maintained at the SCP for any accountable information which is received, generated, reproduced, transmitted, downgraded, or destroyed. A Classified Document Control Log shall be used for this purpose.

5.6.4.2. The Document Control Log maintained at the SCP shall at a minimum reflect the following:

a. Date of receipt and date of origination.
b. Agency/installation from which received or by which originated.
c. Classification level of the material.
d. A brief unclassified title or description of the material.
e. The date of declassification or downgrading.
f. Control number assigned. Each copy of a classified document or item shall have its own control number. Copy numbers shall not be used as part of the control number.
g. Information indicating the location or local holder of the material. (Local holders/custodians shall have some form of signature receipt on file acknowledging that they have custody of the material).
h. Disposition and date for all material destroyed, downgraded, declassified, or dispatched outside the installation.

5.6.4.3. The Document Control Log maintained at the DCS shall at a minimum reflect the following:

1. (1) Classification level of the material.
2. (2) Control number assigned.
3. (3) Disposition and date for all material destroyed, downgraded, declassified or dispatched outside of the DCS.

5.6.4.4. Accountability records shall also contain signed receipts and destruction reports. Signed receipts and destruction reports shall be retained for four years after final disposition.

5.6.5. Top Secret disclosure records.

5.6.5.1. A disclosure record of all persons who are afforded access (visual, oral, record copies, etc.) to Top Secret information (except safe combinations) shall be maintained. This record shall show the names of all individuals given access and the date of such access. To comply with this requirement, a Top Secret Cover Sheet (Form SF 703) shall be attached to all Top Secret information in document form. For access given orally, a log listing the required information shall be maintained. At a minimum, the Disclosure Record Sheet shall provide:

a. Information reflecting the document being disclosed;
b. Individual to whom the information is being disclosed;
c. Organization and Telephone Number; and
d. Date the information is disclosed.

5.6.5.2. Records shall be retained for five years from the date of final disposition.

5.6.6. Exceptions from accountability.

5.6.6.1. Electronic Processing: Installations that electronically process Confidential and Secret information, including e-mail, within a designated restricted area that meets the security requirements of a classified space in accordance with this manual are authorized an exception from the requirement to account for that information under the following conditions:

a. They shall account for IT storage media.
b. They shall account for all Confidential and Secret material that is transferred or distributed outside the classified space.
c. When a classified IT system is used, print only that material that is operationally required to be "hard copy." Conspicuously mark the "hard copy" to indicate the installation and office printing the copy.
d. They shall limit the number of personnel authorized to print classified material from a classified IT system.
e. They shall ensure that all Confidential and Secret material is destroyed by an approved method.
f. They ensure quarterly refresher security briefs are conducted and documented for all personnel working in the classified space. The intent is to increase security awareness to compensate for these relaxed security requirements.
g. They shall establish written procedures approved by the CCS to ensure compliance with the above requirements. These procedures may be included in the unit's information security plan discussed in this manual.

5.6.6.2. This exception does not apply to any other accountable Confidential and Secret material stored within the classified space.

5.6.7. Receipt of classified material.

5.6.7.1. The CCS shall provide written procedures for the handling of incoming classified material. When a Center/facility receives incoming mail, bulk shipments, and items delivered by messenger, the following controls shall be implemented:

1. All classified material shall be delivered promptly to the SCP or properly safeguarded in accordance with this manual until delivery to the SCP can be effected.
2. All Registered, USPS Express mail, and contract (FEDEX, etc.) overnight delivery packages shall be delivered unopened to the SCP and protected as Secret material until determined otherwise.
3. All personnel who open official mail of any sort shall be directed to immediately deliver any classified material to the SCP. Outer wrappers along with the UNOPENED inner wrapper shall be delivered to the SCP. If an individual opens mail which is not correctly packaged, causing exposure to uncleared or unauthorized individuals, the material shall be delivered to the SCP, and the CCS shall be notified. The CCS shall investigate and submit a report of incidents involving classified material outlined in paragraph 5.19 of this chapter.
4. All incoming packages containing classified material shall be inspected for tampering. If tampering is discovered, it shall be reported to the CCS who shall conduct such inquires as are necessary. The contents of the package shall be checked against the enclosed receipt.
5. Incoming classified information that does not fall under the CMC system shall be processed in accordance with the procedures established for that type of material (e.g., COMSEC, NATO).

5.6.8. Record of destruction.

5.6.8.1. An accurate record of destruction of classified material is as important as its destruction. Proper accounting procedures, together with accurate records of destruction, provide evidence of the proper disposition of classified material. Records of destruction shall be retained for 4 years.

5.6.8.2. A record of destruction is required for all CNSI material. The destruction record shall indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness.

Both individuals must have personal knowledge of the actual material destroyed. If applicable, the official authorizing the destruction shall also sign the record. Either the control log or a separate destruction report may be used for this purpose.

5.6.9. Inventory requirements.

5.6.9.1. Two appropriately cleared individuals shall conduct inventories. One of the individuals may be the control officer for the material. However, the other individual must be an appropriately cleared, disinterested party not involved in the operation of the account.

5.6.9.2. An inventory is a visual sighting of each item of accountable material. All documents held shall be checked to ensure that they are entered into accountability, and all documents entered into accountability shall be sighted, including those items signed out on local custody. If no disposition can be determined, an incident involving classified material shall be submitted in accordance with paragraph of this chapter.

5.6.9.3. All Top Secret holdings shall be inventoried upon change of custodian or semiannually. Semiannual inventories may be combined with change of custodian inventories. Accountability records shall also be reviewed for accuracy and continuity. See section 5.7 for a complete listing of required page checks.

5.6.9.4. All Secret and Confidential holdings shall be inventoried upon change of custodian or annually. Annual inventories may be combined with change of custodian inventories. In those instances where exceptionally large holdings (more than 500 control numbers) make conducting an annual inventory difficult, Centers may complete the inventory of material over a 3-month period. An inventory is not required for material authorized for an exception to the accountability requirements listed in section 5.6.4. Top Secret material must be inventoried semi-annually. One inventory may be conducted in conjunction with the scheduled annual inventory of Secret and Confidential material.

5.6.9.5. The Center shall retain a record of all inventories for a period of at least five years. An inventory and a report of the results, including any discrepancies discovered, shall be forwarded annually to the cognizant CCS. Although an inventory of Top Secret holdings is required on a semi-annual basis, a written report to the CCS is only required annually unless discrepancies are discovered. Although the Top Secret inventory is only reported annually, local documentation of all inventories must be maintained at the installation as described above.

5.6.9.6. Upon change of custodian, all classified material shall be transferred to the new custodian. A joint inventory shall be conducted, accounting for each item. Both parties shall sign the report.

5.6.10. Changes and corrections

The custodian, under the direction of the CMCO, shall be responsible for the entry of all changes and corrections to the material in their custody. A Publication Change Checklist must be used for all changes entered. Completed checklists shall be retained until the publication is destroyed or superseded.

5.7 Page Checks

5.7.1. A page check shall be conducted on all Top Secret (TS) material. Page checks involve visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the correct change. In the absence of a list of effective pages, the document shall be examined for continuity. After each page check, the individual shall sign the page check record (except for page checks prior to destruction). If one does not exist, a

page check record shall be produced locally and kept with the publication. The record shall identify the publication, the name of the individual conducting the page check, discrepancies noted, and the date of the check.

5.7.2. Page checks on TS material shall be conducted on the following occasions:

Initial receipt	Yes
Page change	Yes
Change residue	Yes
Change of custodian	Yes
Inventory	Yes
Destruction	Yes

5.7.3. Page checks on Secret material shall be conducted on the following occasions:

Initial receipt	Yes
Page change	Yes
Change residue	Yes
Change of custodian	Yes
Inventory	No
Destruction	Yes

5.7.4. No page checks are required for Confidential material.

5.8 Working Papers

5.8.1. Working papers are documents, including drafts, notes, photographs, computer media, etc., accumulated, created, or received electronically to assist in the formulation and preparation of a finished document. Classifying as "working papers" is not intended as a way around the original classification procedure or temporary classification. Working papers, which contain classified information produced by a unit shall be:

5.8.1.1. Dated when created.

5.8.1.2. Marked with the highest classification of information contained in the document.

5.8.1.3. Protected in accordance with the classification assigned.

5.8.1.4. After 180 days, material classified as working papers must be destroyed or correctly classified by an original classification authority.

5.8.2. The accounting, control, and marking requirements prescribed for a finished document shall be followed when working papers contain Top Secret information or are:

5.8.2.1. Released by the originator outside the NASA facility or transmitted electronically.

5.8.2.2. Retained more than 90 days from the date of origin, and

5.8.2.3. Filed permanently.

5.9 Storage of CNSI, NATO and Classified Foreign Government Material.

5.9.1. All classified documents and material under the jurisdiction of NASA shall be stored in a "General Services Administration Approved" Security Container with an approved combination lock or approved facility/room with sufficient physical and procedural security measures to preclude unauthorized access. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System. See section 5.21 for requirements on security container management. The CCS shall ensure that adequate storage is available for CNSI in accordance with applicable NASA and federal regulations.

5.9.2. Each Center shall apply the following:

5.9.2.1. Mandatory use of Standard Form (SF) 702-101, "Security Container Sheet."

5.9.2.2. Combinations shall be changed when first placed in service and then as needed whenever a person knowing the combination is transferred or terminated from employment or for some other reason is no longer authorized access to the classified material stored in the equipment or area; whenever it is possible that the combination may have been subjected to compromise; or whenever the security storage equipment or security area has been found unsecured and unattended.

5.9.2.3. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I-69 and I-70. Foreign Government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. Safeguarding standards may be modified if required or permitted by treaties or agreements, or for other obligations, with prior written consent of the National Security Authority of the originating government, hereafter "originating government. Please see ISOO Directive No.1 for more detail on how to protect foreign government information.

5.9.2.4. Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding and destruction of classified information during certain emergency situations. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose

b. Limit the number of individuals who receive it

c.Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in subpart C of ISOO Directive No.1, or other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement

f. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

1. A description of the disclosed information

2. Who authorized the disclosure

3. .To whom the information was disclosed

4. How the information was disclosed and transmitted

5. Reason for the emergency release

6. How the information is being safeguarded

7. A description of the briefing provided and a copy of the nondisclosure agreements signed.

5.10 Reproduction of CNSI

5.10.1. Reproduction of classified information and material must be kept to a minimum. Only equipment designated by the CCS is authorized to reproduce classified information. Each Center CCS shall develop and implement written procedures to ensure that the following requirements, as a minimum, are met:

5.10.1.1. Protect classified information during reproduction.

5.10.1.2. Adequately clear equipment after reproduction.

5.10.1.3. Ensure reproduced copies are incorporated into the Center CNSI accountability system.

5.10.1.4. Safeguard overruns, waste, and blank copies generated during the clearing of reproduction equipment as classified material and destroy accordingly.

5.10.1.5. Ensure security procedures are provided for reproducing classified information by other technical means.

5.11 Hand Carrying and Receipting of Classified Material

5.11.1. CNSI shall be transmitted in a manner that ensures protection of the material. A receipt shall be required whenever CNSI material is transmitted using an internal mail routing system, entered in the U.S. Postal System or via authorized contract courier, transmitted off the Center by any means, transmitted to a non-NASA activity, or when the transmitting custodian wishes to verify change of custody.

5.11.2. Methods of Transportation within a Center.

5.11.2.1. The TSCO, custodian, or other employee having a Top Secret clearance and designated by either TSCO or the CCS, shall personally hand-carry Top Secret information within a Center. A Top Secret Cover Sheet (Form SF 703) shall be attached to all Top Secret information in document form.

5.11.2.2. When traveling within a building or between buildings on a Center, classified material shall be hand carried covered with the appropriate coversheet and enclosed in a single envelope or other suitable package marked with the highest classification or carried in a briefcase or other

container. When hand carrying classified material, the individual shall proceed directly to the intended destination. Restroom breaks, coffee breaks, etc., are not permitted when hand carrying classified material.

5.11.2.3. Between buildings of a Center that are widely dispersed or between buildings occupied by NASA and located in metropolitan areas, Top Secret information shall be transmitted within double-wrapped, appropriately marked, and addressed envelopes as prescribed in paragraph 5.11.3 below or in a manner approved by the CCS.

5.11.2.4. Additional measures may be established by the CCS to control access to any CNSI by an unauthorized person during transmission.

5.11.2.5. Such material shall be transmitted inside a Center by hand-delivery from an employee possessing a clearance at least as high as the category of classification of the material involved.

5.11.3. Hand Carrying Outside a Center.

5.11.3.1. The DSMD or the CCS shall appoint a NASA employee or contractor to be a designated courier of CNSI when it is essential for that NASA employee or contractor to hand carry such information outside HQ or a Center.

5.11.3.2. Couriers may also be required for symposiums where transport, control, and access to CNSI may be necessary, for "cleared" conference or symposium attendees, including other agency personnel, or NASA contractors holding NASA security clearances under a NASA DD Form 254.

5.11.3.3. Designated couriers shall be briefed that classified material must be in their physical possession at all times (i.e., not in checked baggage, left unattended in hotel room or vehicles, safeguarded in hotel safety boxes, or taken to bars, dining, or places of entertainment) and protected from opening, examination, or inspection. Furthermore, designated couriers must acknowledge that their authorization to courier CNSI is only valid within the United States of America and its territories.

5.11.3.4. Authorization shall be provided to the designated courier on letterhead NASA stationery, marked "Valid only in the United States of America," and shall include a specific expiration date and the names and home telephone numbers of two NASA Security Specialists who may be contacted if the designated courier is challenged to open the materials by non-NASA personnel (e.g., police, other Government officials, or airline personnel).

5.11.3.5. Personnel shall be briefed on Advisory Circular, "Federal Aviation Administration, Subject: Screening of Persons carrying U.S. Classified Material, AC 108-3."

5.11.3.6. CNSI transmitted outside a Center shall be enclosed in an envelope with opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents.

5.11.3.7. A receipt shall be attached to or enclosed in the inner cover. It shall identify the sender, the addressee, and a description of the materials being transmitted. It shall be signed by the recipient, returned to the sender, and retained for two years.

5.11.3.8. A suspense system shall be established to track transmitted documents until a signed copy of the receipt is returned. If signed receipts are not received within 30 days of transmission of the material, the DCSO or CMCO shall report the non-receipt to the CCS.

5.11.3.9. When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary

protection while the material is in transit.

5.12 Transmission of Classified Material

5.12.1. The term "transmission" refers to any movement of classified material or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation is not significant.

5.12.1.1. Classified material shall be transmitted either in the custody of an appropriately cleared individual, by an approved system or courier, or otherwise in accordance with the provisions of this chapter.

5.12.1.2. The carrying of classified material across national borders is not permitted unless arrangements have been made that shall preclude customs, postal, or other inspections. In addition, foreign carriers may not be used unless the U. S. escort has physical control of the classified material.

5.12.2. Top Secret transmission. Neither the normal mail or messenger system of an Installation nor postal and commercial delivery services are authorized for the transmission of Top Secret material. Top Secret material shall only be transmitted by:

5.12.2.1. Defense Courier Service (DCS).

5.12.2.2. Department of State Courier System.

5.12.2.3. Appropriately cleared NASA civilian personnel specifically designated as a courier.

5.12.2.4. Telecommunications systems specifically approved for transmission of Top Secret material.

5.12.3. Secret transmission. Transmission of Secret material may be effected by:

5.12.3.1. Any of the means approved for the transmission of Top Secret, except that Secret material, other than that containing cryptological information, may be introduced into the DCS only when the control of such material cannot otherwise be maintained in U. S. custody. This restriction on use of the DCS does not apply to Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) material. When the Department of State Courier System is to be used for transmission of Secret material, the Secret material shall be sent by registered mail to the State Department Pouch Room.

5.12.3.3. U. S. Postal Service (USPS) registered mail within and between the 50 United States and its Territories.

5.12.3.4. USPS Express Mail Service may be used between NASA units and contractors within and between the 50 United States and its Territories. USPS Express Mail is authorized only when it is the most cost effective method or when time/mission constraints require it. The package shall be properly prepared for mailing. The USPS Express Mail envelope shall not serve as the outer wrapper. Under no circumstances shall the sender execute the "WAIVER OF SIGNATURE AND INDEMNITY" section of the USPS Express Mail Label for classified material. This action can result in drop-off of a package without the receiver's signature and possible loss of control.

5.12.3.5. When an urgent requirement exists for overnight delivery within the 50 United States and its Territories, the Center Director may authorize the CCS to use Federal Express (FedEX) for overnight delivery of material for the Executive Branch. The sender is responsible for ensuring that an authorized person shall be available to receive the delivery. The package may only be addressed

to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO, and foreign government information (FGI) shall not be transmitted in this manner.

5.12.3.6. Outside the area described in subparagraph 5.12.3.5 above, Secret material may be moved by USPS registered mail through Army, Navy or Air Force Postal Service facilities provided that the material does not pass through a foreign postal system or any foreign inspection, or via foreign airlines. The material must remain under U. S. control. Special care shall be taken when sending classified material to U. S. activities overseas. If the material is introduced into a foreign postal system, it has been subjected to compromise.

5.12.3.7. Within U. S. boundaries only, qualified carriers authorized to transport Secret material via a Protective Security Service (PSS) under the National Industrial Security Program. This method is authorized only when the size, bulk, weight, nature of the shipment or escort considerations make the use of other means impractical.

5.12.3.8. Other carriers under escort of appropriately cleared personnel. Carriers included are Government and Government contract vehicles, aircraft, ships of the U.S. Navy, Federal employee-manned U.S. Naval Ships, and ships of U. S. registry. Appropriately cleared operators of vehicles, officers of ships, or pilots of aircraft who are U. S. citizens may be designated as escorts provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period if stored in an aircraft or shipped in connection with , flight or se , a transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons aboard or loaded in specialized shipping containers, including closed cargo containers.

5.12.3.9. Telecommunications systems specifically approved for the transmission of Secret material.

5.12.4. Confidential transmission. Transmission of Confidential material may be effected by:

5.12.4.1. Any of the means approved for the transmission of Secret material.

5.12.4.2. USPS registered mail for:

a. Confidential COMSEC, NATO, and other special category material.
b. Other Confidential material to and from Fleet Post Office (FPO) or Army Post Office (APO) addressees located outside the U. S. and its Territories.
c. Other addressees when the originator is uncertain that their location is within the U. S. boundaries. Use of return postal receipts is not authorized. If considered desirable, a document receipt may be used.
d. When the sender deems it necessary to ensure adequate protection of the classified material.

5.12.4.3. USPS First Class mail between NASA and other U.S. Government agency locations anywhere in the U. S. and its territories. However, the outer envelope/wrappers of such Confidential material shall be marked "FIRST CLASS," and endorsed "RETURN SERVICE REQUESTED."

5.12.4.4. Certified or, if appropriate, registered mail shall be used for material directed to contractors and to agencies of the Executive Branch.

5.12.4.5. Within U. S. boundaries, commercial carriers that provide a Signature Security Service (SSS). This method is authorized only when the size, bulk, weight, nature of shipment, or escort considerations make the use of other methods impractical.

5.12.4.6. In the custody of commanders or masters of ships of U. S. registry who are U. S. citizens. Confidential material shipped on ships of U. S. registry may not pass from U.S. Government control. The commanders or masters must give and receive classified material receipts and agree to:

a. Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection shall not be unloaded; and
b. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

5.13 Release of Classified Information to Foreign Governments

5.13.1. Subsequent to a determination by the DSMD that classified material may be released to a foreign government; the material shall be transferred between authorized representatives of each government in compliance with the provisions of this chapter. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the DSMD prior to release of the material. Classified material shall be transmitted only:

a. To an embassy or other official agency of the recipient government which has extraterritorial status; or
b. For on-loading aboard a ship, aircraft, or other carrier designated by the recipient government at the point of departure from the U. S. or its territories or possessions, provided that at the time of delivery a duly authorized representative of the recipient government is present at the point of departure to accept delivery, ensure immediate loading, and to assume security responsibility for the classified material.

5.13.2. Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee. This written designation shall contain assurances that such person has a security clearance at the appropriate level and that the person shall assume full security responsibility for the material on behalf of the foreign government. The recipient shall be required to execute a receipt for the material, regardless of the level of classification.

5.13.3. Each contract, agreement, or arrangement, which contemplates transfer of U. S. classified material to a foreign government within the U. S. or its territories, shall designate a point of delivery in accordance with subparagraph 5.13.1.a. or 5.13.1.b. If delivery is to be made at a point described in subparagraph 5.13.1.a., the contract, agreement, or arrangement shall provide for U. S. Government storage or storage by a cleared contractor at or near the delivery point so that the U. S. classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading. Any storage facility used or designated for this purpose must afford the U. S. classified material the protection required by this manual.

5.13.4. If U. S. classified material is to be delivered to a foreign government within the recipient country, it shall be transmitted in accordance with this chapter. Unless a designated or approved courier or escort accompanies the material, it shall, upon arrival in the recipient country, be delivered to a U. S. Government representative who shall arrange for transfer to a duly authorized representative of the recipient foreign government.

5.14 Receipt System

5.14.1. Top Secret material shall be transmitted under a continuous chain of signed receipts.

5.14.2. Secret and Confidential material shall be covered by a receipt between installations and other authorized addressees and between custodians within the same Center/facility.

5.14.3. Receipts shall be provided by the transferring installation, and the forms shall be attached or enclosed in the inner envelope or cover. Domestic Return Receipt form, PS Form 3811, or NASA Form 287 (Classified Material Receipt) or a facsimile shall be used for this purpose.

5.14.4. Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

5.14.5. A duplicate copy of the receipt shall be retained in a suspense file until the signed original is returned. If a signed receipt is not received within 45 days, follow-up action shall be initiated and the cognizant CCS shall be informed.

5.14.6. Copies of signed receipts shall be retained for a period of 4 years.

5.15 Managing and Handling COMSEC Material

Pending issuance of separate specific NASA COMSEC Policy and Procedures, users of COMSEC material shall follow the requirements in managing and handling COMSEC material established in the NASA Central Office of Record Standard Operating Procedures (CSOP) and the National Security Telecommunications Systems Security Instruction (NSTSSI) 4005. The Center COMSEC Officer shall serve as the focal point for all COMSEC issues.

5.16 Defense Courier Service Reimbursement Program

Upon request of the AA/OSPP, the CCS shall provide information on the Center's use of the reimbursable service of the Defense Courier Service (DCS) for transmitting CNSI outside the Center.

5.17 Disposition or Destruction of Classified Material

5.17.1 Inactive CNSI shall be disposed of in accordance with NPR 1441.1, NASA Records Retention Schedules. Each Center shall employ security procedures and methods for destruction, witnessing, certification, and retention of CNSI in accordance with this chapter.

5.17.2 Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information.

5.17.3. Installations shall continuously review their classified holdings. Classified information shall be destroyed when determined to be no longer required for operational or administrative purposes. The Center CCS shall establish annual Centerwide classified material destruction events to ensure classified holdings are properly reviewed and unneeded CNSI disposed of in accordance with NPR 1441.1, NASA Records Retention Schedules. Custodians of classified material deemed no longer viable shall be required to destroy it or transfer to a Center technical library. Collecting or hoarding CNSI is prohibited.

5.17.4. Additional policy must be followed when destroying Communications Security (COMSEC) material as contained in approved CSOPs and NSTSSI 4005.

5.17.5. NASA ACI or For Official Use Only (FOUO) that cannot be decontrolled or that which is no longer needed shall be deleted from IT systems and shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure.

5.17.6. Unclassified material, including formerly classified material that has been declassified, unclassified messages, and ACI material, does not require the same assurances of complete destruction. To avoid overloading an installation's classified material destruction system, unclassified material shall be introduced only when the CCS or higher authority determines it to be required because of unusual security considerations or efficiency.

5.17.7. Approved destruction methods. Destruction devices must be approved by NSA, as listed in NTISSI 4004 Annex B, NSA Evaluated Destruction Devices. Pulpers, pulverizers, or shredders may be used for the destruction of paper products and some forms of computer media. Only paper-based products may be destroyed by pulping. Classified material in microform, that is, microfilm, microfiche, or similar high data density material, may be destroyed by burning or chemical decomposition or other methods as approved by the cognizant CCS. Equipment approved for the destruction of classified material shall be operated properly and provided with regular maintenance, as suggested by the manufacturer. The following are the approved methods for the destruction of classified material:

5.17.7.1. Burning. When burning is used for destruction of classified information, steps shall be taken to ensure that the wind or draft does not carry portions of burned material away and that the resulting ash is broken up sufficiently to preclude reconstruction.

5.17.7.2. Shredding. Any crosscut shredder whose residue particle size is equal to or smaller than 1/32 of an inch in width by 1/2 inch in length (1/32 x 1/2 is approved for the destruction of all classified paper material, magnetic tape, and cards. Shredders shall not be used to destroy classified microfilm, microfiche or similar high information density human readable material. THIS DOES NOT INCLUDE COMSEC ITEMS WHICH MUST BE DESTROYED IN ACCORDANCE WITH ESTABLISHED NATIONAL SECURITY AGENCY (NSA) REQUIREMENTS CONTAINED IN COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS) POLICY NO. 16, DATED OCTOBER 2002. (NOTE: THESE NSA REQUIREMENTS WILL BE MAINTAINED AT CENTER SECURITY OFFICES.)

5.17.7.3. Pulping (Wet Process). Wet process pulpers with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material. Since pulpers only destroy paper products, staples, paper clips, and other fasteners shall be removed to prevent clogging the security screens.

5.17.7.4. Pulverizing (Dry Process). Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use, unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators may be used to destroy photographs, film, typewriter ribbons, magnetic tape, flexible diskette (floppy disk), glass slides, and offset printing plates. Pulverizers and disintegrators shall have a 3/32-inch or smaller security screen.

5.17.7.5. Chemical. Classified microfilm or microfiche may be destroyed by chemical process (e.g., put in an acetone bath).

5.17.7.6. Destruction of Classified Equipment. All components of classified equipment shall be destroyed by any method that destroys them beyond recognition.

5.17.7.7. Eradication of Magnetic Media. Destruction of classified Automated Information System (AIS) magnetic media shall be in accordance with established NASA requirements. A record of destruction records must be executed upon eradication of the classified information.

5.18 Destruction Procedures

5.18.1. Classified material shall only be destroyed by authorized means by individuals cleared to the level of the material being destroyed. A minimum of two individuals shall be responsible for destroying CNSI material, one of whom is a witness to the destruction. These individuals must have personal knowledge of the actual material destroyed (e.g., must positively identify the data which is to be destroyed).

5.18.2. The personnel tasked with the destruction or preparation for destruction of classified material shall be thoroughly familiar with the requirements and procedures for safeguarding classified information. They shall be thoroughly briefed on the following:

5.18.2.1. Safeguarding all classified material entrusted to them for destruction.

5.18.2.2. Conducting a thorough page check before destruction is accomplished.

5.18.2.3. Observing all documents destroyed or being prepared for destruction and checking the residue of locally destroyed material to ensure that destruction is complete and reconstruction is impossible.

5.18.2.4. Taking precautions to prevent classified material or burning portions of classified material from being carried away by wind or draft.

5.18.2.5. Completing and signing all appropriate records of destruction.

5.18.3. Classified waste. Classified waste shall be destroyed as soon as practicable. Containers used for the accumulation of Secret classified waste shall be dated when the first item of classified waste is deposited. If, after 30 days, the classified waste has not been destroyed, it shall be entered into the accountability records of the SCP. It is not necessary to identify the individual items of classified waste when entering the waste into accountability. It is sufficient to identify simply as one container, for example, "box and bag etc., Secret classified waste." When destruction is completed, a record of destruction shall be prepared.

5.18.4. The CCS and AA/OSPP shall review or direct a review, at least annually, of Center classified material holdings expressly for the purpose of reducing to an absolute minimum the quantity on hand. A specific period shall be designated each year for classified material review and destruction. Custodians of CNSI shall be encouraged to dispose of classified holdings that are no longer relevant to ongoing research. Holding non-essential and outdated material poses storage and accountability problems that lead to loss and/or compromises as the owner soon loses track of the material. The CCS shall provide information on annual CNSI reduction efforts in accordance with paragraph 5.3 this chapter.

5.19 Security Violations and Compromise of CNSI

5.19.1. The CCS shall ensure that written procedures exist for the following:

5.19.1.1. Emergency action and reporting requirements for the loss of CNSI.

5.19.1.2. Action to be taken by the CCS in the event of the loss of control over CNSI.

5.19.1.3. Action required in the event that the lost CNSI was not compromised.

5.19.1.4. Action required in the event of possible compromise of CNSI.

5.19.1.5. Action required in the event of unauthorized disclosure of CNSI by NASA or contractor personnel.

5.19.1.6. Notification to the DSMD and the CAF when classified information is presumed compromised.

5.19.2. A written incident report shall be made to the DSMD on all issues as described in 5.19.1.

5.19.2.1. An initial report of incident involving classified material requires an immediate notification and presentation of the facts for the purpose of limiting and assessing the damage to the national security. The initial report shall be made to the DSMD within two working days. The intent is to notify all cognizant officials as soon as possible to limit further damage, assess weaknesses and correct a discrepancy, if appropriate. If a formal report cannot be accomplished in two days, the DSMD shall be provided with electronic mail that briefly describes the incident, immediate actions taken, and those planned.

5.19.2.2. Reports of incidents involving classified information shall contain the following information:

1. Type of report:

a. Compromise; or
b. Possible Compromise; or
c. Administrative Discrepancy.

2. Type of incident:

a. Compromise or Possible compromise;

1. Improper Destruction; or
2. Unauthorized access; or
3. Improper transmission (transmission via non-secure means or use of unauthorized equipment); or
4. Improper storage; or
5. Loss of material; or
6. Found material (material not in accountability system or previously
7. reported as lost) not subjected to possible compromise; or
8. Other (explain).

b. Administrative Discrepancy;

1. Mailed via non-registered/certified mail; or
2. Sent in single container; or
3. Markings on outer container divulged classification of contents; or
4. Classification not marked on inner container; or
5. No return receipt; or
6. Inadequate wrapping: not securely wrapped or protected; or
7. Received in poor condition: compromise improbable; or
8. Addressed improperly; or
9. Classified by unauthorized original classifier; or
10. Markings incorrect; or
11. Classified by, reason for classification, or declassify on, incorrect or missing (originally classified documents); or
12. Derived from or declassify on line incorrect or missing (derivatively classified documents); or

13. Other (explain).

3. Complete identification of all material involved including;

a. Unclassified title
b. Classification
c. Originator

4. Identity of all personnel involved including;

a. Full name
b. SSN
c. Security Clearance
d. Basis of Security Clearance

5. A statement of actions taken upon discovery of incident and description of events.
6. Weakness leading to the incident.
7. Corrective actions taken and actions taken to preclude recurrence.
8. Disciplinary action taken, if any.
9. Unit incident number, to include.

a. Fiscal year
b. Sequential number

5.19.2.3. The CCS shall submit a final incident report within 30 days of the incident. The report shall include:

a. Likelihood CNSI was compromised (provide details supporting determination).
b. Make general comments (may include authority to remove material from accountability or request further information).
c. Incident closure or further investigation required.
d. Center incident number (to include fiscal year and sequential number).

5.20 CNSI Meetings and Symposia

5.20.1. General

Any meeting (conference, seminar, exhibit) or symposium sponsored by NASA or held at a Center or NASA Headquarters where classified information is disclosed must meet the minimum-security standards established in paragraph 5.20.3. Meetings held by an association, society, or other group whose membership consists of primarily cleared contractors may be sponsored by NASA, provided an appropriately cleared contractor is designated and accepts responsibility for furnishing all symposium security measures.

5.20.2. Responsibilities

5.20.2.1. Key officials of the Office of the Administrator, Officials-In-Charge of Headquarters Offices, and Center Directors, as appropriate, are responsible for ensuring that AA/OSPP approval is obtained for a NASA-sponsored conference or symposium involving CNSI discussion and presentations. Security approval shall be coordinated with the Office of External Relations regarding the attendance of any foreign nationals or representatives at a CNSI symposium or meeting.

5.20.2.2. The CCS is responsible for ensuring that all minimum-security standards are met.

5.20.3. Minimum Standards

5.20.3.1. A CNSI meeting or symposium shall be restricted to appropriate areas at Government facilities approved for CNSI discussions or appropriate cleared contractor facilities.

5.20.3.2. Supervisors and meeting hosts shall ensure that all attendees possess the appropriate personnel security clearances and a **need-to-know** .

5.20.3.3. A request for security approval for a CNSI symposium shall be forwarded through the CCS to the DSMD and shall include the following items: date(s) and specific location for the proposed meeting (Government or cleared contractor facility), identification of CNSI subject matter and highest classification level involved, and the identification and status of any non-U.S. citizen (Foreign National or resident alien) and foreign representative invited to attend during any classified or unclassified session.

5.20.3.4. If any non-U.S. citizen, foreign national (to include resident aliens), or foreign representative shall be in attendance, the following information must be submitted to the DSMD: complete name, date, and place of birth; current citizenship status; type of personnel security clearance, if any; identification of each foreign Government, firm, and/or entity represented; date(s) of attendance; nature of participation, and the reason why attendance is considered to be in the U.S. national interest.

5.20.3.5. Foreign nationals or representatives shall not be extended an invitation to attend or be permitted to attend any CNSI or unclassified session unless advance approval has been obtained from the DSMD. Refer to NPR 1371.2A, Procedural Requirements for Processing Requests for Access to NASA Installations or U.S. Citizens who are Representatives of Foreign Entities, for more detailed requirements on facilitating Foreign National visits.

5.21 Security Container, Vault, and Strong Room Management

5.21.1. Deployment, use, and maintenance of security containers, vaults, or strong rooms designed for storage of CNSI shall be centrally managed by the CCS to ensure their use is consistent with Agency and Center policies and procedures for storage and accountability of CNSI. The CCS shall:

5.21.1.1. Ensure only GSA-approved security containers, designed specifically for storage of CNSI, are used. (NOTE: File containers with lock-bar are not authorized for the storage of TOP Secret material. Lock-bar containers must be completely eliminated from the Center inventory of authorized CNSI storage media NLT December 31, 2005.)

5.21.1.2. Maintain a current database of all Centerwide security containers, vaults, and strong rooms to include, at a minimum:

a. Assigned Center-specific security container, vault, or strong room number (e.g., ARC 000465).

b. Location of container, vault, or strong room (building/room#).

c. Custodian/Alternate custodian.

d. Highest classification level of information stored.

5.21.1.3. Ensure approved containers, vaults, and strong rooms are used only for storage of CNSI and necessary unclassified reference materials. Storage of unclassified materials must be kept to the absolute minimum.

5.21.1.4. Ensure high value items that are targets of theft such as funds, weapons, and precious metal

are not to be stored in the same drawer as classified materials.

5.21.1.5. Ensure approved security containers, vaults, and strong rooms are appropriately decertified and properly tagged "Not for Storage of Classified Material" by the CCS prior for use in storage of non-classified material.

5.21.1.6. Establish procedures to remove unneeded security containers are removed from service and retain for future use or properly disposed.

5.21.1.7. Ensure locking mechanisms are properly outfitted with or upgraded to appropriate federally mandated 'X' series locks under the following circumstances:

a. When the security container, vault, or strong room is newly procured or reentered into service.

(NOTE: For storage of classified material: containers, vaults and strong rooms must be inspected, reconditioned as necessary, recertified, and designated in writing by the Center Locksmith and acknowledged by the CCS prior to being reentered into service.)

b. When the locking system requires replacement.

c. When, at the discretion of the CCS, funding is available to retrofit existing container or vault inventory, or

d. When the contain , er, vault or strong r , oom is used to store Top Secret, COMSEC, Special Access Required, or SCI information and material.

5.22 Classified Material is NOT Personal Property

5.22.1. Classified information is always official U.S. Government information and never personal property . Confusion sometimes arises about classified notes from a training course or conference. As classified material, it is official information that must be safeguarded, transmitted, and destroyed in accordance with this NPR. Classified notes cannot be removed from a NASA installation without the approval of the Center Director or CCS. Classified notes shall not be considered as working papers but as official information for which the Center/facility is responsible. It must be transmitted by one of the means authorized for transmittal of classified material and eventually destroyed by authorized means. When an individual leaves one NASA installation and transfers to another, the installation may officially transfer his/her notes classified material to the new NASA installation where the material shall again be available for his/her use. If the individual desires to have the material transferred to another U.S. Government agency, the CCS, as approved by the Center Director, may facilitate such transfers.

5.22.2. CNSI and SBU are always the property of the United States Government. Individuals who remove SBU or CNSI may be subject to disciplinary action up to and including prosecution under Title 18 and Title 50 USC and other applicable laws.

5.23 Security Classification Reviews for NASA Programs and Projects

5.23.1. Pursuant to NPR 7120.5B, 1.4.3.a.(b); 2.1.g.(3); 2.1.1.2; 2.1.1.3.k; et al., programs and projects must conduct formal security reviews that, in addition to personnel, physical, and information technology security, shall include reviews for traditional information classification security needs. Security reviews shall be undertaken to determine if information used or produced as part of a program or project, meets the requirements for designation as CNSI and/or Sensitive But

Unclassified (SBU) controlled information. Project managers will:

a. Refer to Appendix O, "Mandatory Review Process for Determining Classification and/or Sensitivity Level of Information and Technology Process" Flow Chart for guidance in conducting the review, and;

b. Complete NASA Form 1733 **, "** Information and Technology Classification and/or Sensitivity Level Determination Checklist."

c. Include the Form 1733 as permanent program documentation and in any procurement related documentation.

5.23.2. Upon the conclusion of the security review, if the information surrounding or concerning the program of project, or portions thereof, meet one or more of the categories of information presented in the executive order, a Subject Matter Expert (SME) must develop an appropriate Security Classification Guide (SCG). The SME and project officials shall consider the level of classification needed for specific information. NOTE: See chapter 10 for a definition of an SME. There are three levels of classified national security information: Top Secret, Secret, and Confidential. Chapter 10 provides a definition of each. Subject matter experts (SME) must be able to specifically identify what particular information is under consideration for classification. The SME, weighing the information being protected against the definitions in chapter 10, shall provide a recommendation to the Office of Security and Program Protection (OSPP) as to what level the information must be classified (Top Secret, Secret or Confidential) and how long the information must be kept classified. Duration of classification shall be considered within the following guidelines:

a. The SME shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity and shall assign such date or event as the declassification instruction.

b. If unable to determine a date or event of less than 10 years, the SME shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

c. If unable to determine a date or event of 10 years, the SME shall assign the declassification date not to exceed 25 years from the date of the original classification decision.

5.23.2.1. All SCGs must be approved by the OSPP. The DSMD shall assist program and project managers in the development of SCGs.

5.23.2.2. The OSPP will establish and maintain a central repository for all NASA originated SCGs and declassification guides, and shall provide a sequential numbering schema for all SCGs and declassification guides both classified and unclassified. The OSPP will also obtain and maintain SCGs and declassification guides from other agency programs in which NASA is working or supporting.

5.23.2.3. The SCG must be reviewed for updating every 5 years.

5.23.2.4. Upon completion, termination, or cancellation of a program or project, a declassification guide must be produced to provide the necessary requirements for declassifying the project information. The declassification guide must be approved by the OSPP.

5.23.2.5. The " *NASA Handbook for Writing Security Classification Guides* " provides requirements and guidance for the creation of a SCG.

5.23.3. If information surrounding or concerning the program or project is considered to be unclassified, a letter of transmittal shall be produced that reflects this determination. The original letter shall be maintained by the Project Office, with copies sent to the Mission Directorate Office

having responsibility for the project or Center and to the DSMD.

5.23.4. If information surrounding or concerning the program or project is considered to be SBU, the information shall be managed as prescribed in section 5.24 of this NPR.

5.23.5. All CNSI and SBU information should be reviewed by a Record Manager, the responsible Program Manager or head of the office and a Declassification Authority (DCA), if the information is classified, to determine the disposition of the records before they are sent to the Federal Records Center (FRC) or the National Archives and Record Administration (NARA) for temporary or permanent storage.

5.24 Sensitive But Unclassified (SBU) Controlled Information

The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

5.24.1. With the exception of certain types of information protected by statute, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency. Therefore, NASA has determined that official information and material of a sensitive but unclassified (SBU) nature that does not contain national security information (and therefore cannot be classified) shall be protected against inappropriate disclosure by designating and handling such information as SBU in accordance with the procedures set forth in this NPR. See also the definition ofSensitive Information/Material in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

5.24.1.1. Information, regardless of its form (digital, hard-copy, magnetic tape, etc.), the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests is designated as SBU to control or restrict its access. Information designated as SBU shall be afforded appropriate protection sufficient to safeguard it from unauthorized disclosure.

5.24.1.2. Within NASA and the Federal Government, such information had previously been designated "FOR OFFICIAL USE ONLY." This designation was changed at NASA to "Administratively Controlled Information" for clarity and to more accurately describe the status of information to be protected. However, recent efforts to apply consistent terminology across multiple federal agencies have prompted NASA to change the designation to "Sensitive but Unclassified." Therefore the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)" will be used to identify sensitive but unclassified information within the NASA community when that information is not otherwise specifically described and governed by statute or regulation. The use of caveats other than SBU will be governed by the statutes and regulations issued for the applicable category of information.

5.24.1.3. The SBU designation and procedures set forth herein do not apply to the information, reports, or analysis by members of other agencies or departments who are members of the National Intelligence Board (NIB), who are on loan to NASA, and whose authorities are derived from other sources. However, SBU designation and procedures shall be applied when such information, or portions thereof, is copied for dissemination within NASA.

5.24.2. Identification of SBU Information. The failure to sufficiently identify information that

requires protection from disclosure may result in increased risk to life or mission essential assets, damage to official relationships, monetary or other loss to individuals or firms, or embarrassment to NASA.

5.24.2.1. The originator of information, or the official approving its dissemination, must review the information for possible designation as SBU prior to its use. In general, information to be designated as SBU falls into one of the 3 categories described below. The criteria of at least one of the following subparagraphs must be met to designate the information as SBU:

a. Information originated within or furnished to NASA that falls under one or more of the exemption criteria of the Freedom of Information Act (5 U.S.C. º552). However, designating information as SBU does not represent that the information has been determined to be exempt from disclosure under FOIA. Requests under FOIA, for information designated as SBU, will be reviewed and processed in the same manner as any other FOIA request.

b. Information exempt or restricted from disclosure by statute, regulation, contract, or agreement. The following are examples of such information.

(1) Information subject to export control under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR)

(2) Information disclosing a new invention in which the Federal Government owns or may own a right, title, or interest.

(3) Proprietary information of others provided to NASA under a nondisclosure or confidentiality agreement.

(4) Source selection and bid and proposal information.

(5) Small Business Innovative Research Data, Limited Rights Data, and Restricted Computer Software received in performance of NASA contracts.

(6) Information developed by NASA under a Space Act agreement and subject to section 303(b) of the Space Act (42 U.S.C. 2454(b)).

(7) Information concerning or relating to private entity trade secrets or confidential commercial or financial information received by a NASA employee in the course of government employment or official duties.

(8) Information subject to the Privacy Act of 1974 (5 U.S.C. º552a)

c. Information that is determined by a designated NASA official to be unusually sensitive (refer to paragraph 5.22.5. for decontrol provisions). The following are examples of such information.

(1) Predecisional materials such as national space policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries

(2) Geological and geophysical information and data, including maps, concerning wells.

(3) Center maps and/or plain text documents describing locations/directions (e.g., latitude, longitude, depth, etc.) of underground utility conduits (e.g., sewers, gas, data, communications, etc.).

(4) Drawings and specifications that identify existing or proposed security measures for mission essential infrastructure designated assets or other key resources

(5) Mission specific security plans that identify protective measures and procedures for assets that are sensitive in nature but are not classified. (Example: Payloads that utilize special nuclear

materials, payloads that contain certain animal experiments, and STS missions, as determined by the CCS, etc.)

(6) Emergency contingency or continuity of operations plans that provide detailed information regarding emergency response processes and procedures that, if publicized, could give a potential adversary vital information with which to thwart or compromise emergency response efforts.

(7) Sensitive scientific and technical information (STI) (See NPD 2200.1 and NPR 2200.2 for requirements for documentation, approval, and dissemination of NASA STI).

(8) Information that could result in physical risk to personnel.

(9) NASA information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models.

(10) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.

(11) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(12) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

(13) Developing or current technology, the release of which could hinder the objectives of NASA, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

5.24.2.2. Information identified in paragraphs a. and b. below that has designation and protection criteria established by other statutes, regulations, NASA directives, etc., shall be protected and marked in accordance with those applicable directives.

a. Information or material that may already have individual, officially designated identification, protection, or management requirements (e.g., FAR, FOUO, Export Control, FOIA, STI), and/or established markings on the sheet(s) will be controlled in accordance with their respective requirements. However, for the purpose of uniformity and consistency, physical protection and disclosure requirements established for the broader spectrum of SBU will still apply.

b. Information exempted from disclosure by treaty, statute (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulation (ITAR), and Section 303(b) of the Space Act), or other agreements.

5.24.2.3. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to SBU. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for SBU as provided in this document. Should the additional guidance be less restrictive than in this document, the information will be safeguarded in accordance with this NPR.

5.24.2.4. Information shall not be marked or designated as SBU if it does not meet the criteria in paragraph 5.24.2.1.

5.24.2.5. New material derived from documents marked SBU shall carry forward the control marking, if any, from the source documents.

5.24.3. Marking for SBU

Information designated as SBU will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of SBU markings on information known by the holder to be SBU does not relieve the holder from safeguarding responsibilities. Where the SBU marking is not present on information known by the holder to be SBU, the holder of the information will protect it as SBU. Information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with such guidance need not be additionally marked SBU. If there is no specific guidance or marking requirements, information designated SBU will be marked as follows:

a. Prominently mark the top and bottom of the front cover, first page, title page, back cover and each individual page containing SBU information with the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)."

b. Materials containing specific types of SBU information may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It is to be controlled, stored, handled, transmitted, distributed, and disposed* of *in accordance with NASA policy relating to SBU information. This information shall not be distributed beyond the original addressees without p without prior authorization* of *the originator.*

c. SBU information being transmitted to recipients outside of NASA, for example, other federal agencies, state or local officials, NASA contractors, etc., shall include the following additional notice:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It contains information that may be exempt from public release under the Freedom of Information Act* (5 *U.S.C.* 552) or other applicable laws or restricted from disclosure based on NASA policy. *It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have* a *valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).*

d. Computer storage media, i.e., disks, tapes, removable drives, memory sticks, etc. containing SBU information will be marked "SENSITIVE BUT UNCLASSIFIED."

e. Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only SBU information will be marked with the abbreviation (SBU).

f. Individual portion markings on a document that contains no other designation are not required.

5.24.4. Responsibilities.

5.24.4.1 Officers and employees designating information or materials as SBU and those receiving materials so marked shall be responsible for properly safeguarding the information contained therein. These individuals will:

a. Comply with the safeguarding requirements for SBU information as outlined in this document.

b. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding SBU and other sensitive information and the penalties that could result in unauthorized disclosure of SBU information.

c. Keep the number of copies of SBU information to a minimum.

d. Require that all individuals performing work for NASA (contractors, consultants and other persons not employed directly by NASA) execute a NASA Form (TBD), "Sensitive But Unclassified Information Non- Disclosure Agreement (NDA)," as a condition of access to SBU information. Other individuals not assigned to, employed by or performing work for NASA, but to whom access to SBU information will be granted, may be required to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

5.24.4.2. Supervisors and managers will:

a. Ensure that an adequate level of education and awareness is established and maintained to emphasize safeguarding and preventing unauthorized disclosure of SBU information.

b. Ensure that an adequate level of education and awareness is established and maintained to emphasize that disclosing SBU information without proper authority could result in administrative or disciplinary action, fines and/or imprisonment.

c. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when unauthorized disclosures of SBU information occur.

5.24.5. Decontrol Provisions. Officers and employees designating information or materials as SBU shall be held responsible for their continued review and the prompt removal of such designations and restrictive markings when the necessity no longer exists. Authority to decontrol such material and any copies is limited to the official who initially designated the material as SBU, a successor or superior, or an official of an office having primary interest in the material. The following procedures apply:

5.24.5.1. The control status of any information or material designated as SBUshall be reviewed upon request by an individual or individuals to whom disclosure has been restricted. Such material shall be decontrolled and disclosed unless the office of origin or the office of primary interest determines, within a reasonable period of time after the request and after consultation with legal counsel, that the information must remain protected against disclosure. The existence of an SBU marking does not necessarily make information exempt from disclosure. A determination that information is exempt from disclosure must be based on the applicability of some legal authority. Consultation with the Office of the General Counsel at Headquarters or Center Office of Chief Counsel is required.

5.24.5.2. The restrictive marking on information designated as SBU in accordance with paragraph 5.24.2.1. shall be immediately removed when the need for protection no longer exists, (e.g., imminent public release, transfer to records archives, implementation of organization plan, or conclusion of sensitive travel).

5.24.6. Storage, Access, Disclosure, Protection, Transmittal, and Destruction of SBU. The minimum requirements for storage, access, protection, transmittal, and destruction of SBU information is provided in section 5.24.6.1 through 5.24.6.5, respectively. However, some types of SBU information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this NPR. For example, certain types of

information may be considered extremely sensitive based on the consequences of an unauthorized release. Such consequences could be increased risk to life or mission essential assets, damage to official relationships, or embarrassment to NASA. Additional control requirements may be added as necessary to afford appropriate protection to such information. NASA employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

5.24.6.1. Storage. Employees who handle information or material designated SBU shall ensure the proper safeguarding of such information by limiting its access to authorized persons only and by storing it in cabinets, desks, or other containers, or securing it within an individual office area when not in use. Access to SBU information is on a "need to Know" basis in accordance with section 5.24.6.2.

a. When unattended, SBU information will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. SBU information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

b. SBU information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When SBU information is stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

c. IT systems that store SBU information will be certified and accredited for operation in accordance with federal and NASA standards. Consult the NPR 2810.1, Security Information Technology, for more detailed information.

d. Laptop computers and other media containing SBU information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with NPR 2810.1.

5.24.6.2. Access and Disclosure. SBU information of which NASA or a NASA contractor is the originator may disclosed to any Federal Government employee or contractor who has a demonstrated "need-to-know" in connection with official duties. When NASA is not the originating agency, SBU information may be disclosed only with authorization from the originating or designated action agency. Whenever SBU information is disclosed, the recipient must be made aware of the following restrictions on access and disclosure:

a. In no case shall SBU information be disclosed - orally, visually, or electronically - unless the disclosure is clearly in accordance with existing law and Agency regulations or policy directives and is in the best interest of NASA.

b. Access to SBU information is based on "need-to-know" as determined by the holder of the information. When discussing with or transferring SBU information to another individual(s), the holder of the information must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, or from observing or otherwise obtaining the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his/her next-level supervisor or the information's originator.

c. A security clearance is not required for access to SBU information.

d. SBU information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where SBU information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable NASA program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The NASA program office shall then determine if it is appropriate to release the information to the other a , gency official. (See section 5.24.3 for marking requirements)

e. When NASA is not the originating agency, further dissemination of SBU information by the holder of the information may be made only with authorization from the originating or designated action agency. When information requested or to be discussed originated with another agency, the holder of the information must comply with that originating agency's policy concerning third party discussion and dissemination.

,

f. The holder of the SBU information will comply with any access and dissemination restrictions cited on the material, provided with the material, or verbally communicated by the originator. Sensitive information protected by statute or regulation, i.e., Privacy Act, Critical Infrastructure Information, etc., will be controlled and disseminated in accordance with applicable guidance for that type of information. Where no guidance is provided, handle SBU information in accordance with the requirements of this NPR

g. NASA IT Systems containing SBU shall be appropriately protected from unauthorized access. Access shall be granted only after the requisite security investigation, as outlined in chapters 3 or 4 of this NPR, has been accomplished. In addition, access provisions for FIPS 199 Security Category Moderate shall apply.

h. When discussing SBU information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

5.24.6.3. Protection. When materials marked SBU are prepared for dissemination or forwarded to any locations/persons (within or outside a NASA Center), they must be protected using NASA Form 1686, "SENSITIVE BUT UNCLASSIFIED" (SBU) cover sheet. Users shall check appropriate boxes on the form to signify what type of SBU information is contained in the document.

a. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal SBU information to unauthorized persons, a SBU cover sheet (NASA Form 1686) will be used to prevent unauthorized or inadvertent disclosure.

b. When disclosing, disseminating, or transmitting SBU information, a SBU cover sheet, (NASA Form 1686), should be placed on top of the transmittal letter, memorandum, or material.

c. When receiving SBU equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this NPR.

5.24.6.4. Transmittal. Transmission of SBU information may be made via first class mail, courier, encrypted e-mail, encrypted FTP, encrypted HTTP, or secure fax to known recipients. All transmissions of SBU information require a SBU cover sheet (NASA Form 1686) be transmitted with the information. Additionally, the holder of the SBU information will comply with any access,

dissemination, and transmittal restrictions cited on the material, provided with the material, or verbally communicated by the originator.

a. Transmission of hard copy SBU information within the U.S. and its Territories:

(1) Material containing SBU information will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(2) Material containing SBU information may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(3) Material containing SBU information may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

b. Transmission of hard copy SBU information to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, SBU may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the SBU information will be sent through the Department of State, Diplomatic Courier.

c. Electronic Transmission.

(1) Transmittal via fax. The use of a secure fax machine is highly encouraged. However, unless otherwise restricted by the originator, SBU information may be sent via nonsecure fax. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the SBU information faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

(2) Transmittal via E-Mail, FTP, and HTTP (Web)

(i) SBU information transmitted via email, FTP, web, etc., should be protected by encryption or transmitted within secure communications systems. If it is not possible to transmit SBU via appropriately encrypted channels, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of SBU information will comply with any email or other electronic transmission restrictions imposed by the originator.

(ii) Due to inherent vulnerabilities, SBU information shall not be sent to personal email accounts.

(3) NASA Internet/Intranet

(i) SBU information will not be posted on a public NASA website or any other public website.

(ii) SBU information may be posted on the NASA Intranet or other government controlled or sponsored protected encrypted data networks. However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular Intranet site. The official must determine the nature of the information is such that need-to-know applies to all such personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as SENSITIVE BUT UNCLASSIFIED; and information posted does not violate any provisions of the Privacy Act or other applicable laws.

5.24.6.5. Destruction. SBU information or material that cannot be decontrolled per paragraph 5.24.5 or which is no longer needed shall be removed from IT systems, shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure. Destruction may be accomplished by:

a. "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing, or non-recoverable encrypted deletion. Contact local IT security personnel for additional guidance.

c. Paper products containing SBU information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

5.24.6.6. Disposal of IT Systems Containing SBU. Refer to NPR 2810.1 for procedural requirements regarding clearing of hard drives, blackberries, personal digital assistant (PDA's), and other storage mediums, prior to disposal or recycling.

5.24.7. Incident Reporting. The loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will be reported. Incidents involving SBU in NASA IT systems will be reported to the center IT Security Manager in accordance with IT incident reporting requirements in NPR 2810.1.

5.24.7.1. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the NASA Center Chief of Security.

5.24.7.2. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will report it immediately, but not later than the next duty day, to the originator and the Center Chief of Security.

5.24.7.3. Additional notifications to appropriate NASA management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5.24.7.4. At the request of the originator, an inquiry will be conducted by the center security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender

5.24.8. Administrative Violations and Sanctions.

5.24.8.1. All NASA employees, as well as non-employees, who have access to SBU are responsible individually for complying with the provisions of this NPR and may be subject to administrative sanctions if they disclose information designated SBU without proper authorization.

5.24.8.2. Sanctions include, but are not limited to warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, and/or discharge.

5.24.8.3. Such sanctions may be imposed, as appropriate, upon any person determined to be responsible for a violation of disclosure restrictions in accordance with applicable law and regulations, regardless of office or level of employment.

5.25 Use, Protection, and Accountability of Department of Energy (DoE) Unclassified Controlled Nuclear Information (UCNI)

5.25.1. Use.

5.25.1.1. UCNI is sensitive unclassified Government information concerning nuclear material,

weapons, and components, whose dissemination is controlled under section 148 of the Atomic Energy Act.

5.25.1.2. It is to be accessed only by personnel with a need-to-know.

5.25.1.3. Foreign Nationals are not authorized access without approval of DoE.

5.25.2. Protection.

5.25.2.1. UNCI must be stored to prevent unauthorized disclosure. Securing in a locked room, file cabinet, or desk drawer is the minimum requirement.

5.25.2.2. UCNI may be reproduced.

5.25.2.3. Use of encryption is mandatory for electronic transmission.

5.25.2.4. Use of a Secure Telephone Unit (STU III) or Secure Telephone Equipment (STE) is mandatory whenever conversations involving UCNI are necessary.

5.25.3. Accountability.

5.25.3.1. Organizations using UCNI shall designate in writing a Reviewing Official responsible for reviewing created NASA correspondence, reports, and related materials for the presence of UCNI and ensuring the appropriate marking per DoE policy.

5.25.3.2. All copies of UCNI must be periodically inventoried to ensure appropriate accountability.

5.25.3.3. Unneeded copies shall be destroyed by burning or shredding.

Chapter 6. Industrial Security

6.1 General

6.1.1. This chapter provides procedural requirements for implementation of industrial security requirements in accordance with the National Industrial Security Program Operating Manual (NISPOM) and the NISPOM Supplement.

6.1.2. It pertains to, but is not limited to, the requirement to review all programs/projects in accordance with Chapter 5, subparagraph 5.25.1, classified contract administration and the processing and control of classified visits for cleared Government and contractor employees.

6.1.3. The processing and control of classified and unclassified visits to a Center in relation to classified contracts is the responsibility of the CCS and shall be covered in written local security procedures tailored to that Center.

6.2 Department of Defense (DoD) Support

6.2.1. Currently, the DoD, through the Defense Security Service (DSS), acts on behalf of NASA in providing industrial security services for most NASA classified contracts.

6.2.2. The standard security provisions of NASA classified contracts require the contractor to obtain a facility security clearance and be assigned a Cage Code, execute a DoD Security Agreement (DD Form 254), and complete other applicable industrial security forms that require the contractor to comply with the NISPOM for industrial security matters.

6.2.3. NASA exercises the right to inspect contractor operations located on NASA property that are involved in access to and safeguarding classified information.

6.3 Scope

This chapter pertains to contracts, grants, cooperative agreements, and other binding transactions in which performance shall require access to CNSI by the contractor, supplier, grantee, or its employees. It does not apply to agreements with other Federal agencies.

6.4 Responsibilities

6.4.1. NASA program or project management personnel contemplating offers or quotations for a classified contract, negotiating or awarding a classified contract, or bearing responsibility for the performance of a classified contract will:

6.4.1.1. Ensure the CCS is fully engaged in supporting the development of security requirements for the contract.

6.4.1.2. Ensure adequate resources are provided to the CCS for program security oversight, as required.

6.4.1.3. Per the NISPOM, ensure the contractor provides a "Classified Visit Request" to the CCS and updates the list, as appropriate.

6.4.2. The Director of Procurement of each Center is responsible for the following:

6.4.2.1. Ensuring that the request for proposals or offers includes a statement that the contractor or prospective contractor shall or shall not require access to classified information and shall or shall not generate classified information in the performance of such contract. If the contract shall involve access to classified information or cause the generation of classified information, a letter as discussed in paragraph 2305.1 of the NISPOM shall be attached to the material submitted to the individual negotiating the contract.

6.4.2.2. Ensuring that each classified contract contains the standard security clauses prescribed by Section 4.404(a) of the Federal Acquisition Regulation, and NASA Supplement 1804.404-70.

6.4.2.3. Ensuring that any proposed deviation in this standard security provision (e.g., elimination, addition, or substitution) is forwarded to the Office of Procurement for approval by the Assistant Administrator for Procurement, with concurrence by the AA/OSPP and the OGC.

6.4.3. The CCS shall ensure that NASA recommendations affecting the contractor's security program are made primarily through the cognizant security office (Defense Security Service) for the contractor concerned, since that office is primarily responsible for ensuring that the contractor complies with all security recommendations. When it becomes apparent that full and satisfactory action on a specific NASA recommendation has not been taken by the cognizant security office or by the contractor, a detailed report of the circumstances shall be forwarded to the AA/OSPP for appropriate action with a copy to the contracting officer (CO).

6.4.4. All changes to a contractor's security program that may affect the cost, performance, or delivery of the contract must go through the contracting officer (CO) for the processing of a contract modification.

6.4.5. Through coordination with the CO and Contracting Officer's Technical Representative (COTR), the CCS shall develop local written security procedures to ensure that the following requirements are met:

6.4.5.1. All DD Form 254s, Contract Security Classification Specification, shall be completed by the procurement officer with the assistance of the security office. The completed form shall then be signed by the CCS or designated security representative. Additionally, the following is applicable to a DD Form 254 for NASA contracts:

6.4.5.2. In item 12 of the DD Form 254, delete the words: "To the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review in accordance with the Industrial Security Manual," and insert the words: "To the Office of Public Affairs, National Aeronautics and Space Administration, Washington, DC 20546, for review."

6.4.5.3. In the case of prime contracts, the Public Information Office of the NASA contracting Center shall also be specified in item 12 to indicate that proposed publicity releases shall be submitted through that office to the Office of Public Affairs, NASA, Washington, DC 20546.

6.4.5.4. In the case of subcontracts, the publicity office of the prime contractor shall be specified, in addition to the Public Information Office of the NASA Contracting Center, to indicate that proposed publicity releases shall be submitted through those two offices to the Office of Public Affairs, NASA, Washington, DC 20546.

6.4.5.5. The Chief, Headquarters Security Office shall perform these responsibilities for Headquarters contracts.

6.4.5.6. A signed copy of each DD Form 254 shall be forwarded to the DSMD.

6.4.6. The CCS shall ensure contractors operating under a DD Form 254 provide the appropriate "Classified Visit" documentation, per the NISPOM, on all "cleared" contractor personnel working under the DD Form 254 and ensure updates are provided on an as need basis. Classified Visit Requests are mandatory for all NASA Classified Contracts.

6.5 Suspension, Revocation, and Denial of Access to Classified Information

6.5.1. Occasionally, Center security offices may find it necessary to take action to suspend, revoke, or deny a NASA contract employee access to CNSI or to suspend operation of the entire contract. To ensure uniformity and consistency, the following shall apply:

6.5.2.. Only the AA/OSPP or designee may deny or revoke a cleared contractor's access to classified information.

6.5.3. The AA/OSPP, DSMD, or CCS may grant interim and final access or suspend access for cleared contractor personnel, as necessary.

6.5.4. The AA/OSPP, Center Director, CCS, or the DSMD shall suspend a contractor's access for cause.

6.5.4.1. Each action shall be fully documented. Information developed during the security inquiry shall not be shared with the Contracting Officer or contractor management while the inquiry is ongoing. The DSMD or CCS 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 may otherwise be ineligible for continued access to classified information.

6.5.4.2. Center security officials shall ensure coordination is effected with the local or regional Industrial Security investigative organization (OPM, DSS, DIS) to obtain direction and to ensure information is provided to enable them to properly adjudicate for continued clearance eligibility.

6.5.4.3. During the investigative and adjudicative process, all reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

6.5.5. The CCS shall propose denials and revocations of contractor access to the AA/OSPP. The AA/OSPP shall make final denial or revocation determinations after consultation with the NASA CAF and the OGC.

6.5.6. Subjects of adjudication must be allowed to review and refute any information developed during the investigation process which shall make him or her ineligible for access to NASA CNSI, unless release of that information jeopardizes national security.

6.6 Periodic Review of DD Form 254

6.6.1. Each approved DD Form 254, Contract Security Classification Specification, or other written notification, issued in lieu thereof, shall be reviewed at least annually by CCS with the assistance of the procurement office.

6.6.2. The individual(s) responsible for this review shall be identified by the CCS in local written security procedures.

6.6.3. When a change is made in a security classification specification pertaining to a prime contract, that change shall be reflected in all applicable Form DD 254s, or other classification documents pertaining to subcontractors.

Chapter 7: Physical Security Program

7.1 Security Control at NASA Centers

7.1.1. Each Center shall apply and maintain appropriate physical security measures necessary to provide for protection of persons and property.

7.1.2. Positive entry controls shall be implemented at all entry points to the Center and individually designated security areas and facilities, as deemed necessary, to preclude unauthorized access to critical areas, information, or personnel.

7.1.3. Procedures shall be established to ensure only authorized personnel are admitted to NASA Headquarters and field Centers.

7.2 NASA Photo-Identification (Photo-ID) Badge Program

7.2.1. NASA currently employs an Agency-specific employee photo-ID badge or Center-specific visitor pass to ensure only properly authorized personnel are granted access to NASA Centers, facilities, and other resources.

7.2.2. The CCS shall develop and monitor local procedures pertaining to the issuance, utilization, control, and accountability of the NASA Photo-ID badge and any Center-specific visitor passes.

7.2.2. NASA photo-ID badges are color-coded to designate the following categories of personnel, as specified in Appendix I, NASA Photo-Identification Standards. These photo-ID badges are required as official identification for entry to NASA facilities:

7.2.2.1. NASA civil service

7.2.2.2. NASA non-appropriated fund employees

7.2.2.3. Consultants/contractors

7.2.2.4. Other Federal agency employees and military personnel detailed to NASA

7.2.2.5. COOP students, summer students

7.2.2.6. Appropriately accredited members of the press

7.2.2.7. Foreign national visitors and contractor employees from designated and non-designated countries. Includes permanent resident aliens (PRA).

7.2.3. Security clearance status shall not be designated by any device, color, or code on any NASA photo-ID.

7.2.4. The NASA photo-ID issued to NASA civil service employees and other Federal agency and military detailees shall be honored for access to NASA Headquarters and all NASA Centers.

7.2.5. NASA photo-ID badge system databases shall be designated "sensitive unclassified information" and protected as ACI.

7.2.6. At a minimum, a favorable review; conducted by center security personnel, of submitted investigative documentation (e.g., SF 85, SF 85P, SF 86, NASA Form 531, etc.) is required for

issuance of the NASA photo-ID to authorized NASA civil service, NASA contractor, and tenant organization personnel. See chapters 2, 3 & 4 for specific investigative requirements.

7.2.7. Issued NASA photo-ID badges or visitor passes shall be properly displayed and worn at all times while bearer is on a NASA Center or Component Facility. They shall be worn:

7.2.7.1. Above the waist on the outermost garment.

7.2.7.2. Photo-side visible.

7.2.8. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, etc.) on the NASA photo-ID (or any alteration or modification thereof) is not authorized.

7.2.9. The NASA photo-ID is not personal property. It is the property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued NASA photo-ID's; immediately reporting the loss or false use of a NASA photo-ID; challenging unbadged personnel; notifying the CCS of a name change; properly displaying the badge when on Center; and surrendering the NASA photo-ID upon resignation or retirement, or upon the direction of the issuing authority.

7.2.10. NASA Retiree ID Card. The Center HR Office shall initiate the request for the NASA Retiree ID Card only for those NASA Civil Service employees who have retired under favorable conditions (e.g., instances other than retired in lieu of termination for cause, etc.). The issuance and use of the NASA Retiree Card is a privilege that may be denied or revoked at any time for cause.

7.2.10.1. The NASA Retiree photo-ID Card is valid at any NASA Center and when presented along with another appropriate form of photo-identification shall be used to obtain a visitor pass to enter the Center.

7.2.10.2. Access shall normally be restricted to business hours only, unless after hours access is "sponsored" and monitored by a Center employee.

7.2.10.3. All Center procedures and controls for visitor pass and visitor access, to include escorting, shall be observed as appropriate.

7.2.11. Forging, falsifying, or allowing misuse of a NASA Photo-ID or other forms of NASA identification in order to gain unauthorized access to NASA facilities is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than 1 year, or both, and may further result in termination of employment and access to NASA facilities.

7.2.12. To deter duplication, falsification, and misuse, the NASA photo-ID shall be redesigned and reissued, at a minimum, every 6 years.

7.3 NASA Photo-ID Issuance Criteria

7.3.1. NASA Civil Service personnel photo-ID: NASA civil service personnel are issued Agency-unique color-coded photo-identification that clearly identifies the individual as a NASA employee. The NASA Photo-ID design, color, and other characteristics are established in Appendix J, NASA Photo Identification Card Standards.

7.3.1.1. Issuance of the NASA civil service personnel NASA photo-ID is restricted to U.S. Citizens only, with the following exception:

7.3.1.2. The NASA civil service personnel photo-ID may be issued to Foreign Nationals, including foreign members of the Astronaut Corps, employed under an IPA when:

a. a. Such issuance is deemed to be in the best interest of the Agency.
b. b. The FN is nominated by a Center Director, in writing with sufficient justification for consideration and approval by the AA/OSPP.

7.3.1.3. The CCS shall ensure that these non-civil service personnel nominated for issuance of the NASA civil service personnel photo-ID are appropriately screened and restrictions imposed where appropriate to preclude inadvertent access to areas and information (e.g., export controlled information, other forms of ACI, etc.) not authorized through the implementing hiring agreement.

7.3.1.4. As a reminder, when issued, the NASA photo-ID provides an individual with official NASA civil service personnel identification; therefore, care must be taken to ensure appropriate awareness and due consideration of the risk involved.

7.3.2. Non-NASA Employee NASA Photo-ID. Contractor employees, consultant, military or other Government agency detailees, students, interns, and accredited press shall be issued a unique color-coded NASA photo-ID, per design specifications established in Appendix I. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3. Foreign National (FN) NASA Photo-ID. All Foreign Nationals, except Astronauts, visiting or assigned to work at NASA Installations shall be issued a unique color-coded NASA photo-ID unless the exception established in subparagraph 7.3.1.2 above is granted. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3.1. Specific and prominent lettering on the front of all FN NASA photo-ID will be placed identifying the bearer as a Foreign National and whether the FN is from a non-designated or designated country. This shall be accomplished with the placement of the letters "FN" for non-designated and "FND" for designated countries on the front of the NASA photo-ID.

7.3.3.2. An expiration date that is the earlier of the expiration of the individual's foreign passport, the expiration of the U.S. visa, or such earlier date as determined through review and approval pursuant to NPR 1371.2A, "Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. citizens who are Representatives of Foreign Entities."

7.3.3.3. If the Foreign National is deemed to require an escort per chapter 4, section 4.13, the issued photo-ID shall be so labeled with the words "Escort Required" on the face of the badge, and procedures shall be developed to ensure the escort requirement is appropriately implemented and monitored to ensure compliance.

7.3.3.4. Access and movement restrictions, if any, shall be placed on the back of the FN NASA photo-ID and recorded on a Security/Technology Control plan as required in chapter 4, paragraph 4.13.9.

7.4 NASA Photo-ID Color-Coding

7.4.1. Gold NASA Photo-ID - NASA civil service personnel, and all active members of the NASA Astronaut Corps. Accepted for access to all NASA Centers, as appropriate.

7.4.1.1. Foreign National members of the Astronaut Corps shall have a representation of their National Flag superimposed on the badge for further designation as a FN.

7.4.2. Blue NASA Photo-ID - NASA consultants and contract employees (U.S. Citizen) who require access to a NASA Center or controlled facility.

7.4.3. Green NASA Photo-ID - Military and other U.S. Government agency detailees. Accepted for access to all NASA Centers, as appropriate.

7.4.4. Violet NASA Photo-ID - Any intern/student (U.S. citizen) who requires access to a NASA Center to perform their duties.

7.4.5. Orange NASA Photo-ID - Any foreign national (FN) contractor personnel from non-designated countries who require access to a NASA Center, or NASA controlled facility to perform their work.

7.4.6. Red NASA Photo-ID - Any Foreign National (FND) contractor personnel from designated countries who require access to NASA IT systems or shall have a need to work at a NASA controlled facility to perform their work.

7.4.7. Brown NASA Photo-ID - Any accredited member of the media (U.S. only) who may require access to "public" areas only of a NASA Center.

7.4.8. Silver NASA Photo-ID - Employees of the Jet Propulsion Laboratory (JPL).

7.4.9. If an individual does not require access to controlled Center assets, a local Center specific photo-ID may be issued in lieu of the NASA photo-ID.

7.4.10. Foreign national visitors shall be issued a visitor's pass, specifically identifying them as a foreign national, and escorted at all times.

7.5 Inspection of Persons and Property

7.5.1. General.

7.5.1.1. In the interest of national security and general employee safety, NASA shall provide appropriate and adequate protection or security for personnel, property, installations (including NASA Headquarters, Center, and Component Facilities), and information in its possession or custody.

7.5.1.2. In furtherance of this policy, NASA reserves the right to conduct an inspection of any person and property in their possession as a condition of admission to, or continued presences on, or upon exit from, any NASA Installation. Requirements, policy, and procedures for all aspects of this program are contained in 14 CFR part 1204, subpart 10.

7.5.1.3. All NASA entities must adhere to these requirements in the implementation of this program.

7.5.2. Requirements.

7.5.2.1. Per 14 CFR, Section 1204.1003 all entrances to Centers shall be conspicuously posted with the following notices:

1. " CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from, this installation is contingent upon your consent to inspection of person and property.
2. UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS

PROHIBITED: Unless specifically authorized by NASA, you shall not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

7.5.2.2. Only properly trained members of the Center's security organization shall conduct inspections pursuant to this NPR and the CFR. Personnel may be supplemented with detection devices (mirrors, x-ray, other sensing devices) and/or canines as the situation dictates.

7.5.2.3. Training shall include:

a. Appropriate search techniques for the type of vehicle being searched.
b. Key locations where devices or other contraband may be secreted.
c. Procedures for confiscating illegal or dangerous items, detaining of individuals and referring incidents to appropriate external law enforcement.

7.5.2.4. Such inspections shall be conducted in accordance with the following guidelines:

a. Consent to inspection notices covering NASA employees, contractors, and visitors to NASA Centers shall be issued in accordance with the authority contained under Section 304(a) of the National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. 2455(a), and 14 CFR section 1204.1003.
b. A consent to the inspection must be obtained from the person to be inspected giving permission for a general exploratory inspection while that person is about to enter or is on the grounds of, or is about to depart from a NASA Center. The person may change their mind at any time, and inspection shall not be pursued further. If an individual does not consent to an inspection, it shall not be carried out, and the individual shall be denied admission to, or be escorted from, the Center.
c. Inspecting personnel must exercise good judgment at all times prior to or while conducting an inspection. They must avoid exceeding their authority or exercising their authority with undue severity.
d. Security personnel shall present appropriate NASA credentials to the subject of the inspection.
e. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., weapons, drugs, explosives), the items may be confiscated, the individual shall be denied admission to, or be escorted from, the Center; or detained at the scene while the appropriate investigation is conducted by NASA investigators. The NASA Office of Inspector General or appropriate law enforcement authorities shall be notified to assume jurisdiction over the matter.
f. The Office of the General Counsel shall approve Agency procedures based upon the requirements of this section.

7.6 Security Areas

7.6.1. Types of Security Areas.

7.6.1.1. Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource shall be "Restricted" areas (as a minimum designation).

7.6.1.2. Limited Area. An area in which security measures are taken to safeguard classified material

or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors shall be escorted or other internal restrictions implemented, as determined by the CCS.

7.6.1.3. Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

7.6.1.4. Temporary Secure Work Area (TSWA). An area in which security measures are needed for 30 days or less. Shall be of a "restricted," "limited," or "closed" nature. A TSWA shall also be established if approval as a permanent security area is pending.

7.6.2. Establishment, Maintenance, and Revocation.

7.6.2.1. Establishment. Center Directors; Director, Headquarters Operations; the AA/OSPP; and the CCS shall establish, maintain, and protect such areas designated as restricted, limited, or closed depending on the rationale for the establishment of the area and the area's vulnerability to unauthorized access.

7.6.2.2. Maintenance. Security measures shall vary according to individual situations; however, the following minimum-security measures shall be taken in all security areas:

a. Post appropriate signs at entrances and at intervals along the perimeter of the designated area, as appropriate for the facility, to provide reasonable notice to persons that the area is a security area.
b. Signs must read as shown in Appendix G; however, the AA/OSPP may approve existing signs now used pursuant to a State statute.
c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

7.6.2.3. Revocation. Once the need for a security area no longer exists, the area must return to normal procedures as soon as practical.

7.6.3. Access. Only those NASA employees, contractors, and visitors who need access and who meet the following criteria shall enter a security area unescorted. All other individuals must be escorted. Escorts must be authorized NASA employees or NASA contractors (U.S. Citizens).

7.6.3.1. To enter a Restricted Area unescorted, individuals must undergo the appropriate investigation required for that area as established by the individual Center; the investigation shall be, at a minimum, a NACI for civil service employees and a NAC for non-NASA personnel.

7.6.3.2. To enter a Limited Area, individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a NACI for unclassified but sensitive information and material.

7.6.3.3. To enter a Closed Area, individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

7.6.3.4. Center Directors and the AA/OSPP shall rescind previously granted authorizations to enter security areas when an individual's clearance and need-to-know is no longer justified, their presence threatens the security or safety of the property, or when access is no longer required for official purposes.

7.6.4. Cellular phones and other devices with digital camera capability. When introduced into security areas and/or areas of a sensitive nature, these items pose an unacceptable security risk to NASA. This risk encompasses numerous facets of the NASA security program. These risks include,

but are not limited to: the protection of information (both classified and unclassified but sensitive (SBU) such as ACI and ITAR information); contract proceedings and information; investigative information; and employee right to privacy. The Center CCS will implement and enforce the following:

a. No cell phones or other devices with photographic capabilities may be introduced into a NASA area housing the processing, display, or open storage of classified information.
b. Each Center Security Office shall conduct a continuing review of their facilities to ascertain the locations of other sensitive functions requiring protection from an overt or inadvertent compromise utilizing such devices.
c. Centers must have written security plans to accomplish the protection of those areas. Copies of those plans shall be maintained in the Center Security Office, and a copy must be available within the protected area at all times. Plans must include, as a minimum, the following items:

1. The method used to alert and educate affected employees.
2. Details on how the policy shall be enforced, including how the devices shall be physically denied entry or otherwise controlled.
3. Spot-check procedures.

7.6.5. Two-way pagers and other communications devices capable of recording and sending text messaging are also not authorized in security risk areas.

7.7 Facility Security

7.7.1. NASA Buildings and Facilities.

7.7.1.1. NASA buildings and facilities come in varying types and sizes, are used for varying purposes, and require implementation of varying levels of security to ensure adequate protection of NASA personnel and assets.

7.7.1.2. Facilities and buildings shall be provided the level of security commensurate with the level of risk as determined by conducting a vulnerability risk assessment:

a. Physical security enhancements for existing facilities shall be established based on an assessment of the type of vulnerability(ies) identified during a security vulnerability risk assessment, development of strategies to address identified vulnerabilities, and implementation of selected security measures, both physical and procedural.
b. Minimum physical security requirements shall be incorporated into construction of facilities projects in accordance with the requirements established by the CCS, Facility Engineering, and the Interagency Security Committee (IASC).
c. Procedural security measures shall be developed, implemented, and properly disseminated to ensure awareness, adherence, and compatibility with implemented physical security measures.

7.7.2. Security Fencing.

7.7.2.1. When used properly and in conjunction with other physical and procedural security measures, fencing provides for a cost-effective method of delineating U.S. Government property boundaries, establishing clearly visible protected borders, and serving as a deterrent to most would-be intruders.

7.7.2.2. Selection and placement of security fencing shall be in accordance with the requirements established in Chapter 6, NPR 1620.3, Physical Security Requirements for NASA Facilities and

Property.

7.7.3. Keys, Locks, Locking Devices (hasps and chains), and Protective Seals.

7.7.3.1. Despite the growth and sophistication of IT-based access control systems, traditional keys, locks, and seals continue to play a significant role in the implementation and management of facility and asset protection.

7.7.3.2. Center Security Officials shall establish key and lock control policies and procedures in accordance with Chapter 5, NPR 1620.3, Physical Security Standards for NASA Facilities and Property.

7.7.4. Minimum Protection Considerations for MEI Facilities or areas housing MEI assets.

7.7.4.1. A Facility Security Manager (FSM) shall be designated for each facility. The FSM shall ensure that security training is provided to employees with access to the MEI asset and that program management implements and enforces the security requirements developed for the asset.

7.7.4.2. An access control system shall be employed at all times.

7.7.4.3. Intrusion Detection Systems (IDS) and other surveillance systems (e.g., video surveillance), when required, shall be appropriately monitored and shall receive appropriate response by armed mobile security personnel capable of responding within locally established time limits, but shall not exceed 5 minutes. Unannounced response tests shall be performed at a minimum of twice in a calendar year.

7.7.4.4. Security fencing shall be installed when the need is identified during the conduct of security vulnerability risk assessments.

7.7.4.5. Security lighting shall be installed at key areas around the facility to facilitate, to the extent possible, detection of intruders.

7.7.4.6. All personnel requiring unescorted access to the MEI shall have been investigated per chapters 3 or 4. All personnel not meeting investigative requirements shall be escorted.

7.7.4.7. Personnel shall properly display issued photo-ID.

7.7.4.8. NASA MEI shall be designated and properly posted as a NASA "Restricted" area, at a minimum. See Section 7.6 for criteria regarding designation of NASA Security Areas.

7.7.4.9. After completion of an initial security vulnerability risk assessment upon designation as an MEI asset, reassessments shall be conducted every 2 years at a minimum, or more frequently as circumstances warrant.

7.7.5. Childcare Centers

7.7.5.1. Childcare centers established under the auspices of NASA sponsorship shall, with coordination and approval of the CCS:

a. Establish positive measures to ensure the proper identification of authorized personnel, to include parents and others, authorized to pick up children.
b. Establish physical and procedural security measures necessary to separate and control child areas from visitor reception areas.
c. Install duress system buttons at key locations per Security Office specifications.
d. Install video surveillance capability in key locations per Security Office specifications.
e. Ensure adequate mechanisms are in place for emergency notification and response.
f. Ensure appropriate security lighting is installed at key areas around the facility to enable

detection of would-be intruders.

7.7.5.2. Minimum physical security and antiterrorism construction standards for new NASA Childcare Centers shall be incorporated into construction of facilities projects in accordance with the requirements established in NPR 8820.2E, NASA Facility Project Implementation Guide, and the Interagency Security Committee (IASC).

7.7.6. Visitor Centers and Outdoor Displays

7.7.6.1. NASA Visitor Center and outdoor displays traditionally house one-of-a-kind, irreplaceable items of historical significance.

7.7.6.2. Such items are generally considered invaluable because they are irreplaceable and must be considered sensitive property. They must be reasonably protected.

7.7.6.3. The degree of protection necessary must be determined locally and in partnership between the Visitor Center curator, CCS, and supporting facility engineers.

7.7.6.3. Visitor Center buildings and apertures providing access to the building must be modified or constructed so as to delay a determined intruder long enough for a security force to respond.

7.7.6.4. Interior and exterior security lighting shall be provided in all Visitor Center buildings in which sensitive property is located.

7.7.6.5. Viewing surfaces of exhibit or display cases shall be constructed of materials resistant to breakage and must be securely fastened into frames or into the container.

7.7.6.6. Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.

7.7.6.7. Pilferable component parts shall be secured to the display or removed at the close of each business day.

7.7.7. Minimum Strongroom Physical Security Standards.

7.7.7.1. While generally considered sufficient for their intended purpose, the use of strongrooms to protect CNSI must be kept to the absolute minimum.

7.7.7.2. Any room designated for use as a strongroom must be modified in accordance with the following:

a. Doors shall be solid core metal clad and installed with the appropriate "X" Series tumbler lock.
b. Doors frames shall be steel.
c. Construction shall be a minimum of true floor to ceiling wood stud framing covered by 3/4" plywood and 1/2" wallboard. If necessary, plywood and new wallboard shall be installed directly over existing framing and wallboard.
d. Use of Intrusion Detection Systems (IDS) shall be determined by the CCS on a case-by-case basis and shall be evaluated on the basis of existing threats, overall building security program, and establishment of periodic security checks of facility.

7.7.8. IDS, Video Surveillance, and Electronic Access Control System Minimum Standards and Integration.

7.7.8.1. Security systems intended to protect people, property, or information are the responsibility of the CCS.

7.7.8.2. IDS, Video Surveillance, and Electronic Access Systems provide an effective means to enhance any organization's physical security program. If employed correctly and managed appropriately, these systems offer a wide range of coverage options.

7.7.8.3. The CCS shall:

a. Determine, in coordination with facilities engineering personnel with the appropriate expertise in security systems design, integration, and operation overall performance requirements for IDS, video surveillance, and Electronic Access Control Systems.
b. Establish and operate a 24-hour monitoring site where emergency response can be dispatched upon need.

7.7.8.4. Individual, stand alone systems offering no centralized monitoring oversight and alarm response capability (including internally-monitored systems) are not authorized.

7.7.9. For those facilities protected under the National Preservation Act of 1966, implementation of security measures shall be those measures allowable under the Act, to the extent necessary and practical.

7.8 Airfield and Aircraft Security

7.8.1. The cost and criticality of aircraft assets require protection at the home port, at intermediate landing locations, and at destinations. The CCS, in concert with Center Airfield Operations Management personnel, shall:

7.8.1.1. Ensure that a physical security survey and security vulnerability risk assessment are conducted on resident aircraft, hangars, ramps, and airfields.

a. The security vulnerability risk assessment shall help to determine the level of criticality and vulnerability of NASA flight assets to theft, sabotage, terrorism, vandalism, and air piracy.

b. The survey shall be used to establish a requisite level of protection that is reasonable and sustainable.

7.8.1.2. Ensure that specific physical and procedural security measures for the protection of NASA aircraft, are implemented, as appropriate.

7.8.1.3. At a minimum, designate and post airfield and associated support facilities as "Restricted Areas," and establish appropriate access control measures.

7.8.1.4. With the assistance of aircraft commanders, develop physical security requirements tailored to the configuration of specific aircraft to be included in the Pilot's Aircraft Checklist.

7.8.1.5. Develop a procedure for reporting and responding to the unauthorized movement or taxiing of aircraft.

7.8.1.6. Develop an alerting system that promptly advises the tower, fire department, security force, and other appropriate authorities of unauthorized activity.

7.8.1.7. Develop a response procedure in the event of the unauthorized movement of an aircraft.

7.8.2. Aircraft Commanders shall:

7.8.1.1. Ensure security of their aircraft at transient domestic and international locations.

7.8.1.2. Prohibit unauthorized access to aircraft under NASA control.

7.8.1.3. Ensure that passengers are properly identified and that baggage and packages are either associated with passengers or are authorized NASA cargo.

7.8.1.4. Reject unaccompanied or unidentifiable luggage or cargo and release to the custody of Center or other Airfield security forces for appropriate disposition.

7.8.1.5. Conduct appropriate security inspections of any NASA aircraft before placing it in service and after it has been left unattended.

7.9 Control and Issuance of Arms, Ammunition, & Explosives (AA&E)

7.9.1. Authority.

7.9.1.1. The AA/OSPP shall direct or grant approval for the following security officers and employees to carry firearms on official duty:

a. The DSMD and designated HQ security personnel.

b. The CCS of each Center and designated security personnel.

c. NASA employees, contractors, and subcontractors, while engaged in the performance of their official security duties such as couriers, investigators, or protective operations and details. This does not include the OIG, whose authority is derived from other sources.

d. NASA contractors and subcontractors engaged in the protection of property owned by the United States and located on NASA Centers or component facilities.

7.9.2. Responsibilities.

7.9.2.1. NASA certifying officials, described in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms," shall ensure compliance with the requirements of this section.

7.9.2.2. NASA employees and contractors to whom firearms are issued are responsible for strict compliance with all the conditions regarding the carrying and use of firearms as established herein and set forth at 14 CFR part 1203b, Security Programs, Arrest Authority and Use of Force by NASA Security Force Personnel.

7.9.2.3. NASA security personnel and contractors shall not carry firearms outside the 50 States, the District of Columbia , and U.S. territories (Puerto Rico, Guam , U.S. Virgin Islands, American Samoa , et al.) without the advance approval of the AA/OSPP.

7.9.3. Certification to Carry Firearms.

7.9.3.1. The certifying official shall issue a NASA Form 699A or 699B, Certificate of Authority to Carry Firearms. The following items define the forms and their use and procedures for certification:

a. NASA Form 699A is a certification to carry concealed firearms when necessary in the performance of official duties.

b. The form shall be issued to NASA Civil Service employees and select contractor security officers (requires AA/OSPP approval) only. Uniformed contractor personnel shall not carry concealed weapons.

c. The NASA Form 699A is prepared in triplicate and indicates an expiration date (not to exceed 2 years from date of issue).

d. Upon termination of employment or assignment to duties not requiring carrying concealed weapons in the course of official duties, the certificate must be returned to the issuing officer within 15 days.

e. Exceptions to these requirements shall be made (in writing) only by the DSMD.

7.9.3.2. NASA Form 699B is a certification to carry unconcealed firearms that shall be issued only to NASA contractor employees serving as uniformed guards.

a. This form shall be prepared in duplicate and shall indicate the date of expiration (not to exceed the term of any applicable guard service contract; otherwise, not to exceed 5 years).

b. The form shall also identify the specific nature and location of official duties that require the carrying of firearms.

c. The original certificates shall be issued to the employee and shall be retained in the employee's possession while on official duty.

d. One copy of the certificate shall be retained by the NASA certifying official.

e. All losses of certificates shall be reported immediately to the certifying official.

f. Upon termination of employment or assignment to duty no longer needing certification to carry firearms, the original certificate shall be returned to the certifying official.

g. Only the certifying official may make exceptions to these requirements.

7.9.3.3. NASA Forms 699A and 699B are serialized for control and accountability purposes. Certifying officials shall maintain appropriate accountability records, including certification of destruction, for all forms in their custody and ensure that all unused forms are kept in a secure storage container other than the one in which the accountability records are stored.

7.9.3.4. Certifying officials shall not sign their own certificates. The Center Director or the AA/OSPP shall sign certificates authorizing the issue of a weapon to a certifying official.

7.9.4. Conditions Under Which Firearms May be Carried by Center Security Personnel. Including shoulder-fired weapons (e.g., rifles, machine guns, shotguns):

7.9.4.1. Firearms may be carried only when all of the following criteria are met:

a. The individual has successfully completed the appropriate suitability background investigation and has been favorably evaluated by a qualified physician to be physically fit as well as emotionally stable.

b. The individual is in immediate physical possession of a valid NASA certification to carry firearms.

c. The individual has successfully completed a qualification course for the firearm being carried, and the qualification is current. (Refer to Appendix E and paragraph 7.9.8)

d. It is necessary in the performance of official NASA duties and with the knowledge and approval of a certifying official.

e. There is no use of intoxicants (e.g., illegal drugs, alcohol) during duty and prior to 12 hours of reporting to duty.

7.9.4.2. The wide range of circumstances under which it shall be necessary to carry firearms requires consideration of all pertinent factors, augmented by common sense and good judgment.

7.9.5. Conditions Under Which Firearms and Explosives May be Used, Stored, and Maintained by Non-Security Personnel:

7.9.5.1. Researchers and scientists frequently use firearms and explosives during testing and experimentation. The safe operation, storage, and accountability of firearms and explosives used under testing and experimentation are required to ensure the safety and security of Center personnel.

a. NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics, are the governing documents for establishing the safe storage and handling of firearms and explosives.

b. This chapter is the governing document for issue, use, secure storage, and accountability for firearms and explosives.

7.9.5.2. The following procedures are required for the use, storage, and accountability of firearms and explosives by non-security personnel.

a. NASA program and project personnel contemplating the of use firearms or explosives in testing or experimentation programs must submit a written request to the CCS outlining the program or project need for introducing firearms, ammunition, and explosives onto a NASA facility.

b. An inventory of the type of weapons and explosives with serial numbers, type and amount of ammunition, and type and amount of explosives shall be maintained and updated on a quarterly basis. The inventory shall be made available for review by security and safety personnel, as requested.

c. Identify location of stored/secured and names of personnel having access.

d. In coordination with the Center Security and Safety personnel, establish appropriate secure storage for AA&E.

7.9.6. Weapons Aboard Commercial Aircraft.

7.9.6.1. Armed NASA Special Agents (SA) may only carry firearms on commercial aircraft after completion of required Federal Aviation Administration certification in accordance with 14 CFR 108.219, and then only in conjunction with "Official" Government travel requiring the SA to be armed.

a. Refresher Federal Aviation Administration certification training, for carrying firearms on a commercial aircraft, shall be required every 2 years and shall be integrated with required firearms qualification to ensure appropriate awareness.

b. The DSMD or designee shall be notified in advance of all official air travel of armed NASA Civil Service SA. NASA security services contractor personnel are not authorized to fly armed.

7.9.6.2. In addition to the Federal Aviation Administration requirement, the SA must be currently qualified to carry a firearm.

7.9.6.3. The SA must be in possession of a current NASA Form 699A (concealed weapons permit) and NASA badge and credentials.

7.9.6.4. The SA shall not display his/her weapon or make known to passengers that he/she is carrying a weapon.

7.9.6.5. The SA shall always carry the weapon on his/her person and never in carry-on baggage.

7.9.6.6. The SA shall always carry handcuffs.

7.9.6.7. The SA shall never carry Oleoresin Capsicum spray or other chemical intermediate weapon while on-board a commercial flight.

7.9.7. Firearms Instruction.

7.9.7.1. The certifying official shall designate a firearms instructor, who shall inform the certifying official in writing of an individual's knowledge of the rules of firearm safety and the content of this NPR.

7.9.7.2. In cases involving a contractor guard force, the firearms instructor may be appointed from the guard force complement.

7.9.7.3. Minimum standards shall be met before a firearms instructor or certifying official shall consider an individual qualified to carry firearms.

7.9.7.4. Recent firearms training and experience during prior employment, such as the FBI, Secret Service, police, military, or other significant and qualifying experience, shall meet NASA standards if the individual has qualified under all provisions of this chapter within the past 30 days.

7.9.7.5. These qualifications shall be verified by a review of employment and training history either through an interview with previous management or visual inspection of documented training history.

7.9.7.6. Appropriate NASA training, including firearm safety procedures and use of deadly force, followed by obtaining a qualifying score on a recognized course as specified in paragraph 7.9.8 below, shall also be required.

7.9.8. Training.

7.9.8.1. Personnel shall be trained and qualified on professional firearm ranges established and maintained by NASA, or other federal, state, or municipal authorities.

7.9.8.2. Personnel shall be certified for carrying firearms after firing a qualifying score under the NASA certified firearm course. (See Appendix E of this NPR.)

7.9.8.3. The AA/OSPP shall establish firearms course of fire standards for all Center armed security personnel, to include standards for shoulder-fired weapons (e.g., rifles, submachine guns, shotguns).

7.9.8.4. As soon as possible after certification, personnel shall receive testing and training in judgmental shooting (whether to shoot or not to shoot) through NASA's current firearms training simulator or other approved methods of judgmental shooting.

7.9.9. Maintenance of Proficiency.

7.9.9.1. Personnel authorized to carry firearms shall be required to fire a qualifying score on the NASA course of fire at least once every 6 months.

7.9.9.2. All personnel authorized to carry firearms must successfully complete testing and training on the simulator or other approved methods of judgmental shooting annually, if possible, or as often as the system is available at that Center.

7.9.10. Records.

7.9.10.1. The certifying official or firearms instructor shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data.

7.9.10.2. Records shall be maintained for 2 years.

7.9.11. Firearms Standards.

7.9.11.1. CCS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm their Civil Service and contractor security staff.

7.9.11.2. The AFL is approved by the Office of Security and Program Protection (OSPP) and maintained by the NASA Federal Arrest Authority Training Academy (NFAATA) at Kennedy Space Center .

7.9.11.3. The AFL may be waived or modified only by the AA/OSPP.

7.9.11.4. Training, qualifications, and certification for all approved firearms shall be documented per paragraph 7.9.8.

7.9.11.5. Modifications.

a. No modifications to the operating system, firing mechanism, and/or trigger groups shall be made to any NASA approved firearms.

b. Center armorers shall modify grips, sights, and control levers to best suit individual users.

7.9.11.6. Handguns.

a. NASA approved handguns are semi-automatic pistols in calibers 9mm, .40, or .357.

b. Uniformed contractors at each Center must be armed with the same make and model handgun.

c. Emergency response teams/SWAT teams may carry a different make and model.

d. NASA Civil Service personnel shall carry the same make but may vary the model to suit individual users.

e. Handguns must always be worn in standard, commercially available holsters; uniformed officers must use holsters with a retention device.

7.9.11.7. Patrol Rifles.

a. At the discretion of the CCS, contractors shall be armed with semi-automatic or select fire patrol rifles.

b. Only iron or optical sights shall be installed on these weapons.

7.9.11.8. Patrol Shotguns.

a. At the discretion of the CCS, contractors and Civil Service personnel shall be armed with semi-automatic or pump action 12 gauge shotguns.

b. These weapons shall also be used to employ "less-lethal" ammunition.

7.9.11.9. Submachine guns.

At the discretion of the CCS, contractor security force may be armed with submachine guns.

7.9.12. Other approved firearms.

At the discretion of the CCS, and with the consent of the AA/OSPP, other firearms may be utilized to meet Center security requirements.

7.9.13. The user of any NASA approved firearm must meet the training and certification requirements of paragraph 7.9.8.

7.9.14. Personal weapons.

The use or carrying of personal weapons is prohibited.

7.9.15. Ammunition.

7.9.15.1. Only premium, commercially manufactured, "law enforcement only" duty ammunition shall be issued.

7.9.15.2. Duty ammunition shall be expended at training sessions at least once every 18 months to ensure use of fresh duty ammunition.

7.9.15.3. Normal training ammunition shall be commercially manufactured "lead-free" training ammunition designed for range use.

7.9.16. Firearm maintenance.

7.9.16.1. All firearms shall be periodically inspected and kept in good working order by a qualified gunsmith/armorer.

7.9.16.2. Ammunition, holsters, and related equipment shall be periodically inspected for deterioration and kept in good working order.

7.9.17. Accountability of Arms, Ammunition, and Explosives (AA&E).

7.9.17.1. The control and custody of all AA&E within a Center shall be under strict accountability at all times and is the ultimate responsibility of the CCS.

7.9.17.2. The CCS shall appoint a custodian for all AA&E within the Center Security Office, within each contractor guard force, and within each non-security organization using AA&E (e.g., explosives, propellants, etc.) for research or testing purposes.

7.9.17.3. Each custodian shall maintain an ongoing inventory of all AA&E. The inventory shall indicate:

a. The date and method of acquisition of all firearms and ammunition.

b. Full identifying data, e.g., the caliber, make, and serial number of each firearm.

c. Amounts of basic load and training ammunition on-hand.

d. Types and amounts of explosives, (e.g., fragmentary, flash-bang grenades, C/S, pepper spray, etc.).

7.9.17.4. The CCS shall report all Center AA&E data to the AA/OSPP on an annual basis the third week after the end of the fourth quarter of each fiscal year.

7.9.17.5. Current contractor firearm data shall be maintained in the Center Security Office.

7.9.17.6. A receipt system for recording the issuance, transfer, and return of all firearms, ammunition, and explosives, shall be maintained by the custodian. Receipts shall include the following details:

a. Dates of issuance, transfer, or return to custody.

b. Serial numbers of firearms.

c. Numbers and types of assigned explosives.

d. Types and numbers of ammunition on-hand.

e. Signatures of recipients.

f. Signatures of custodians upon return of the firearms and explosives.

(NOTE: Both NASA personnel and contractor receipts shall be retained by each Center for 1 year.)

7.9.18. Lost, stolen, or missing AA&E shall be reported immediately, but no later than 24 hours after discovery, to the DSMD:

a. This preliminary report shall include all available details concerning the event with a complete description of the weapon or other lost AA&E item(s).

b. This preliminary report shall not be delayed pending a complete report of the circumstances.

c. A description of the lost, stolen, or missing AA&E shall also be entered into the National Criminal Information Center (NCIC) database.

7.9.19. Security Services contract personnel issued AA&E may only be armed on NASA property to perform their mission, if approved by the CCS.

7.9.20. Non-security personnel having NASA mission related uses for AA&E items (e.g., researcher, scientists, etc.) shall:

7.9.20.1. Ensure control, storage and accountability of authorized AA&E are in accordance with the provisions in paragraph 7.9.21 of this chapter and the requirements established in the NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics.

7.9.20.2. Maintain appropriate and current inventories of issued and maintained AA&E per paragraph 7.9.17 and provide a copy of the inventories to the CCS as changes occur.

7.9.21. Storage and Exchange of AA&E.

7.9.21.1. Issued firearms for NAS security and law enforcement personnel may be stored loaded or unloaded under secure means, per local policy.

7.9.21.2. When not in use, all issued firearms and ammunition shall be securely stored per local policy.

a. Non-issued firearms and shoulder-fired weapons shall be stored in an arms room or a security container with a built-in 3-position combination lock and issued only as required.

b. Non-issued ammunition shall be stored in either a suitable lockable container or an arms room.

7.9.21.3. Explosives shall be stored in separate secure containers, specifically designed for the purpose of storing explosive materials.

7.9.21.4. Firearms or ammunition shall not be stored in containers with money, drugs, precious materials, evidence, or CNSI. They shall be stored separately.

7.9.21.5. NASA HQ and each Center shall adopt procedures for the maintenance of records with respect to the issuance of AA&E and access to firearms and ammunition storage areas and containers.

7.9.21.6. Weapons shall not be exchanged on a guard post. Any exchange or inspection of firearms shall be done only in an area where a "clearing barrel" is available and under proper supervision.

7.9.21.7. Firearms shall always be considered loaded. Armed NASA security personnel shall not point the firearm at anything that they do not intend to shoot.

7.10 Standards for Secure Conference Rooms

7.10.1. When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities."

7.10.2. The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with DCID 6/9.

7.10.2.1. Meetings shall be limited to collateral Secret or below.

7.10.2.2. Positive access control shall be implemented.

7.10.2.3. A Technical Surveillance Countermeasures (TSCM) Specialist, if available, or Security Officer shall conduct a visual inspection and establish security procedures for the meeting.

7.10.3. Special Cases.

7.10.3.1. The preceding specifications do not apply to conference areas in which the level of security exceeds the collateral Secret level.

7.10.3.2. For these areas, guidance on additional requirements will be provided by the CCS on a case-by-case basis.

7.10.3.3. The DSMD or CCS shall be contacted for any interpretation of these specifications.

7.11 Threat Assessment

7.11.1. Reliability.

7.11.1.1. NASA personnel, facilities, and programs are subject to a wide range of internal and external threats.

7.11.1.2. Such threats may be presented by natural forces, workplace violence, the technological sophistication of NASA Research and Development (R&D) and test facilities and programs, and the inherent risk of component and system failure by both internal and external attempts to disrupt Agency operations or to compromise National security.

7.11.2. Threat Assessments.

7.11.2.1. The DSMD, after consultation and input from various sources, shall publish an annual NASA Postulated Threat Statement.

7.11.2.2. Of significant importance are the Agency's resources identified under the Critical infrastructure and key resources protection program. However, threat assessments must transcend

formally designated critical resources and assets and cover the full realm of NASA personnel and physical resources, assets, and program/project information.

7.11.2.3. The CCS shall use the NASA Threat Statement in developing a localized threat statement for their Center.

7.11.3. Countermeasures.

7.11.3.1. NASA shall employ a sound and comprehensive security program that includes security awareness training and the development and implementation of Center security plans to counter these threats.

7.11.3.2. To ensure an Agencywide standard for reacting to periods of increased security threats, the threat conditions established in section 7.17 below shall be employed as directed by NASA Headquarters or as determined by local events.

7.12 Threat and Incident Reporting

7.12.1. General.

7.12.1.1. All Centers shall implement a threat and incident reporting system as required by NPD 1600.2, NASA Security Policy.

7.12.1.2. The system's purpose is to keep the Administrator and senior management officials advised on a timely basis of serious security-related incidents or threats that may affect the NASA mission.

7.12.1.3. Reports shall be forwarded to the DSMD. Refer to appendix F for a sample of the Serious Incident Report format.

7.12.2. Responsibilities.

7.12.2.1. The CCS ensures that incidents are reported to the DSMD and followed up with a fax that describes the incident.

7.12.2.2. The DSMD shall report information from the CCS (or designated representative) to the AA/OSPP, if available.

7.12.2.3. The AA for Security and Program Protection shall then decide whether it is appropriate to brief either the NASA Administrator, Deputy Administrator, or Chief of Staff.

7.12.2.4. If a principal or designated representative is unavailable at any of the cited levels, the information shall be automatically passed to the next level.

7.13 Reportable Incidents

7.13.1. Any type of incident that might have security implications shall be reported to the AA/OSPP in a timely manner, including the following:

7.13.1.1. All crimes committed at a Center requiring notification of NASA OIG, or, as appropriate, the FBI, DEA, ATF, or local law enforcement.

7.13.1.2. Possible Espionage (Reported through Center CI channels via the NASA Secure Network (NSN)).

7.13.1.3. Possible Sabotage (Reported through Center CI channels via the NSN).

7.13.1.4. Suspected terrorist activity (e.g. surveillance, photography, attempted penetrations, unusual requests for information). (Reported through Center CI channels via the NSN).

7.13.1.5. Bombing incidents, including bomb threats that severely impact Center activities.

7.13.1.6. Actual or planned demonstrations or strikes.

7.13.1.7. Shootings or other violent acts.

7.13.1.8. All incidents which involve the need for professional medical attention or damage to NASA facilities or equipment exceeding $25,000 shall also be reported in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Record Keeping.

7.13.1.9. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on NASA property may also require reporting to and through the NASA Safety Program channels in accordance with NPR 8621.1.)

7.13.1.10. A security-related incident in which the media has become involved and publicity is anticipated.

7.13.1.11. An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incidents shall include unauthorized access, theft, interruption of computer/network services or protective controls, damage, disaster, or discovery of a new vulnerability.

7.13.1.12. Threats against NASA property.

7.13.1.13. Threats that affect NASA missions.

7.13.1.14. Threats against NASA personnel.

7.13.1.15. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.

7.13.1.16. Information concerning individuals who are perceived to be acting irrationally in their efforts to make personal contact with high Government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American and anti-U.S. Government demonstrations in the United States, involving serious bodily injury or destruction of property; or an attempt or credible threat to commit such acts to further political, social, or economic goals through intimidating and coercive tactics.

7.14 NASA Security Office Special Agent Badges and Credentials (B&C)

7.14.1. Control.

B&C's are sequentially numbered and accountable security items. Their issue, use, and accountability shall be monitored by both the AA/OSPP and the CCS.

7.14.2. Issuance, Use, and Return.

7.14.2.1. B&C's identify NASA Special Agents authorized to conduct investigations and inspections and to perform other duties that shall be assigned by virtue of the National Aeronautics and Space

Act of 1958, as amended. [NOTE: This does not include the Office of Inspector General (OIG), whose authority is derived from other legal sources].

7.14.2.2. The AA/OSPP shall create, authenticate, and issue credentials and procure metallic badges at the request of the CCS.

7.14.2.3. The CCS shall nominate civil service personnel to receive B&C's.

7.14.2.4. Security specialists whose official duties do not require routine investigative work and/or frequent liaison with Federal, State, or local authorities shall only be issued credentials appropriate for the position occupied.

7.14.2.5. The CCS shall ensure that B&C's or credentials no longer required for official duties are returned to the AA/OSPP. B&C's shall be surrendered to the CCS when replacements are issued.

7.14.2.6. The CCS shall ensure that B&C's are not misused and shall withdraw them immediately upon any report of misuse, pending investigation of the allegation:

a. A report outlining the circumstances of any withdrawal of B&C's shall be forwarded to the DSMD within 72 hours.

b. A report on the final disposition of the incident, including the results of a Return To Duty (RTD) assessment and recommendation, shall also be furnished to the DSMD for review and final determination.

7.14.2.7. Lost or stolen B&C's must be reported immediately. The appropriate CCS shall forward a report outlining all pertinent facts to the DSMD no later than 2 days after the loss.

7.14.2.8. Security specialists must surrender B&C's when requested by the issuing authority or when relieved of security duties by transfer, termination, or retirement. Upon termination of security duties, requests to keep B&C's shall be addressed as follows:

a. Employee must have been employed by NASA as a Security Official for a minimum of 10 years.

b. Credentials shall be sent, along with a letter requesting retention of "voided" credential, for the individual concerned.

c. Retirement and presentation of the NASA metal badge shall be considered based on the following prerequisites:

(1) Employee must be retiring from Federal service under honorable circumstances.

(2) Employee must have served NASA in an agent capacity for a minimum of 10 years.

(3) Badges must be mounted in a Lucite award block, which shall be funded by the either the individual or requesting office and procured by the OSPP.

(a) Individuals or organizations shall submit to the OSPP a written request containing the individuals name, position, and length of service with NASA, along with a personal check in the amount required at that time, made out to the OSPP selected vendor.

(b) The OSPP shall arrange fabrication of the award. Delivery time shall normally be within 4 weeks from submission of order.

7.14.2.9. B&C's may be returned to the AA/OSPP by NASA Pouch Mail, double wrapped, or they may be hand-carried.

7.14.3. B&C's for Contractors.

a. The CCS shall issue Center-unique B&C's to contractor security personnel as deemed appropriate. The B&C must identify the individual as a NASA Contract employee, authorized under the Space Act to perform specified duties (e.g., investigations, inspections, etc.).

b. All provisions of section 7.14 also apply to NASA contract security services personnel.

7.14.4. Acceptance of B&C's for Access to NASA Centers.

B & C's (Federal, State, or NASA) shall not be accepted for access to NASA Centers unless accompanied by a NASA photo-ID or issued NASA visitors pass.

7.15 Technical Surveillance Countermeasures (TSCM)

7.15.1. TSCM Program.

The AA/OSPP is responsible for the NASA TSCM program. The program shall be consistent with national policy issued by the U.S. Security Policy Board (USSPB). All matters pertaining to the conduct of TSCM activities throughout the Agency shall be directed and coordinated through the DSMD.

7.15.1.1. The AA/OSPP shall ensure that a NASA TSCM capability exists which can:

a. Conduct physical, electronic, and visual search techniques to identify and protect Agency persons, facilities, information, or activities that are vulnerable, through design or circumstance, to hostile technical surveillance activities.

b. Ensure that TSCM operations are conducted in a manner consistent with U.S. Security Policy Board guidelines.

c. Acquire and employ TSCM technologies, techniques, and methods to identify and neutralize hostile technical surveillance activities that are consistent with accepted national TSCM policies.

d. Collect, analyze, and disseminate data regarding the technical surveillance threat to the Agency.

e. Provide support by ensuring that all NASA TSCM personnel are accredited through U.S. Government TSCM training and that individuals receive continuing, advanced training necessary to maintain the level of technical expertise as prescribed by TSCM USSPB Procedural Guides 1 through 3.

f. Develop, with input by the DSMD; Director, Safeguards Division; and Center Security Chiefs, a listing of facilities that require a TSCM service.

g. Coordinate TSCM efforts with Centers that have organic TSCM assets.

7.15.1.2 Conduct of TSCM Services

a. TSCM services shall be conducted in accordance with USSPB TSCM Procedural Guides, following the four distinct phases.

b. TSCM services shall be coordinated through the DSMD for the purpose of tracking TSCM efforts.

7.15.1.3 Facilities Requiring TSCM Support

a. A TSCM service shall be performed for initial accreditation purposes for any Sensitive Compartmented Information Facility (SCIF) within the Agency. Follow-on TSCM support shall be

coordinated through the Agency SSO when threat conditions warrant, when there has been a modification to the SCIF, when uncleared personnel have not been continually escorted while in the SCIF, or when new equipment or furnishing have been introduced to the SCIF.

b. A TSCM service shall be conducted in all offices in which Top Secret discussions routinely occur.

c. A TSCM service shall be conducted in offices or areas that are routinely used to process information or to discuss information that addresses sensitive aspects of controlled U.S. technology or controlled Agency technology.

d. TSCM services shall be conducted in NASA senior executive office spaces.

e. TSCM services shall be conducted in contractor facilities that process and discuss NASA classified national security information as annotated in the DD-254, DOD Contract Security Classification Specification.

f. TSCM in-conference monitoring support shall be scheduled if the conference is conducted in an area not usually associated with classified discussions and the area has not been under continuous control by cleared employees.

7.15.1.4 TSCM Request Procedures

All requests for TSCM support shall be addressed in writing to the DMSO, Security Management Division and classified at the Secret level at a minimum. Advanced coordination may be done telephonically, but only via secure means. When requesting or coordinating a TSCM service, requestors shall not use any communication medium located within the area that is to be the subject of the TSCM service. At a minimum, the request must identify:

a. Complete identification of the area requiring TSCM support, to include: name of area, room number, building number, address, location, and brief mission description of the area/facility.

b. Brief justification why a TSCM service is necessary.

c. Square footage of each space identified.

d. The name of the point of contact and an alternate, with telephone numbers for both secure and nonsecure telephones.

e. Clearance requirements for TSCM personnel.

f. The time frame the service is required.

7.15.1.5 TSCM Reports

1. Upon completion of a TSCM survey, a complete report shall be provided for the requestor. At a minimum the report shall include:

a. Complete identification of the facility receiving the TSCM support.

b. Who requested the survey.

c. When the survey was accomplished and by whom.

d. Description of the support provided.

e. Findings/Observations if security vulnerabilities or hazards were discovered.

f. Recommendations that either mitigate or eliminate the security vulnerabilities.

g. Name of local person who received the out-brief.

2. Reports shall be signed by the responsible senior security official who has operational oversight of the TSCM team. Copies of TSCM reports shall be provided to the DSMD.

7.15.1.6 Discovery of a Device

Upon discovery of a suspected eavesdropping device, the following actions shall be taken:

a. The area shall be secured and placed under continuous surveillance.

b. A report, classified Secret, shall be submitted, without delay, to the DSMD. At a minimum, the report shall contain the following.

(1) Date and time of the discovery.

(2) Facility and area where found.

(3) Specific location of the suspected find.

(4) Description of suspected device (e.g., wired microphone, modified telephone, RF transmitter, etc.).

(5) Method of discovery.

(6) Name(s) and any additional information of personnel who discovered the suspected device.

(7) Best estimate as to whether any foreign intelligence service was alerted to the discovery.

b. Only the responsible official at the facility shall be notified of the discovery and the actions taken. Information of the suspected discovery shall not be released to other persons, until such release has been coordinated with and approved by the DSMD.

c. No effort shall be made to test the specific device or to attempt to remove the suspected device, until such actions have been authorized by the DSMD.

7.15.1.7 Classification Requirements

a. NASA TSCM Security Classification Guide SCG-17, dated August 1992 is hereby rescinded.

b. The following is classification requirements for NASA TSCM operations as outlined in USSPB Procedural Guide 1 and shall serve as the TSCM classification Guide for the Agency:

Information that Reveals	Shall be Classified
(1) Pending or current TSCM operation.	Secret
(2) Completed TSCM operation.	Confidential
(3) A request for TSCM service.	Secret
(4) Major security vulnerabilities of an area.	Secret

(5) Minor vulnerabilities.	Confidential
(6) The discovery of a device.	Secret
(7) Facility/program threat assessments as part of TSCM service.	Secret
(8) Penetration techniques.	Up to Secret
(9) TSCM equipment capabilities/limitations; budget or procurement actions; and/or policies and procedures	Up to Secret
(10) TSCM team membership, orders, or agency affiliation.	Up to Secret

2. The following shall be used for the Classified by Line, Reason, and Declassification:

Classified by: USSPB Procedural Guide 1

Reason: 1.4c

Declassify on: March 24, 2024

7.16 Dealing With Demonstrations

7.16.1. Objectives.

The primary objectives in dealing with demonstrations are to restrict demonstration activity to areas outside Centers and to preserve peace while protecting the rights of demonstrators to assemble peacefully and exercise free speech.

7.16.2. Use of Force.

7.16.2.1. Demonstrators who have illegally entered NASA property shall be politely requested to leave voluntarily.

7.16.2.2. Only the minimum amount of physical force necessary shall be used to remove demonstrators who refuse to leave NASA buildings or grounds.

7.16.2.3. Verbal abuse or verbal threats alone by a demonstrator cannot be the basis for use of physical force.

7.16.3. Law Enforcement.

7.16.3.1. The CCS for each Center shall make reasonable efforts to use non-arrest methods to manage crowds.

7.16.3.2. If demonstrators are disorderly or refuse to leave NASA buildings or grounds, then law enforcement officers who have the appropriate jurisdiction shall be summoned for support.

7.16.3.3. Ensure that sufficient law enforcement personnel are on hand and then inform the demonstrators that they must leave the NASA building or grounds within a brief period of time, such as 15 minutes, or face arrest for trespassing.

7.16.3.4. If the demonstrators still refuse to leave, law enforcement personnel shall take necessary action to effect an arrest for, at a minimum, trespassing and remove them from the building or grounds as quickly as possible.

7.16.4. Center Directors; Director, Headquarters Operations; and AA/OSPP shall make the following decisions:

7.16.4.1. When to request outside Federal, State, county, or local law enforcement personnel to enter a Center to enforce the law.

7.16.4.2. When to curtail activities or to close the gates of the Center.

7.16.4.3. When to dispatch response teams to demonstrations.

7.16.5. The CCS of each Center has the following responsibilities:

7.16.5.1. Identify the group leadership and purpose of the demonstration.

7.16.5.2. Determine the expected size, type, activity, and time of planned demonstrations.

7.16.5.3. Evaluate and dispatch information to the DSMD.

7.16.5.4. Upon instructions from the Center Director, coordinate a plan of action with local law enforcement officials.

7.16.5.5. Obtain support from the Center's Public Affairs Office (PAO), the local Office of Inspector General, the Center's Office of the Chief Counsel, and the U.S. Attorney's Office, as necessary and appropriate.

7.16.5.6. Ensure that the Statement of Work for the contract security force includes training in dealing with demonstrators as annual in-service training, and as refresher training immediately prior to a demonstration, when possible.

7.16.5.7. Ensure that all personnel who are authorized to carry firearms under the provisions of paragraph 7.9 of this Chapter and all personnel whose actions are governed by the limitations and regulations at 14 CFR Part 1203b, Arrest Authority and Use of Force receive training in dealing with demonstrators as an annual in-service training and as refresher training immediately prior to a demonstration.

7.16.5.8. Maintain an event log, commencing at the time information is first received, of a demonstration and detailing thereafter all significant events, times, places, and actions with the name of the NASA official authorizing such actions.

7.17 Threat Conditions (THREATCONS) Program

7.17.1. General.

7.17.1.1. The protection of NASA employees and assets from acts of terrorism at NASA-owned or leased property in the United States or abroad shall be given priority, especially during periods of heightened threat.

7.17.1.2. Although absolute protection against such acts is not possible, protective procedures shall

be based on the threat level and reflect a balance among the degrees of protection required, the resources available, Agency mission requirements, and other pertinent factors.

7.17.1.3. In addition to assistance from the DSMD, the Center shall obtain support from local representatives such as the FBI, Department of State, NASA OIG, and state and municipal law enforcement agencies.

7.17.2. THREAT CONDITIONS (THREATCONS).

7.17.2.1. This section explains the establishment of the NASA Threat Condition (THREATCON) program designed to meet the requirements of the National Threat Warning System developed and implemented by the Department of Homeland Security (DHS).

7.17.2.2. NASA Centers hosting military organizations as tenants, residing as a tenant on a military installation, or situated contiguous to a military installation, shall establish mutually agreed upon notification systems for ensuring Department of Defense's use of ALPHA designators under the DoD Force Protection Condition (FPCON) concept vice COLOR coded designators under the DHS Threat Condition concept does not conflict with NASA's implementation of Agency Threat Conditions established under Homeland Security Presidential Directive (HSPD) 3, Homeland Security Advisory System.

7.17.2.3. The warning system ranges from NASA's basic, level 1, everyday security policy (THREATCON GREEN) through additional four graduated levels of increased security, culminating at the most stringent level (THREATCON RED).

7.17.2.4. The warning system is intended to standardize terms and establish standardized security measures that can be initiated by the AA/OSPP and Center Directors through the Agency-wide emergency notification system.

7.17.2.5. Every Government agency is required to use this Threat Condition Program that provides for a greater consistency to threat reactions at both the national and Agency-level.

7.17.2.6. The AA/OSPP shall initiate, and shall change, or rescind NASA-wide THREATCONS.

7.17.2.7. Center Directors shall implement THREATCONS initiated by the AA/OSPP and may implement higher THREATCONS for their Center based on the local threat situation. They shall not lower or rescind a THREATCON initiated by the AA/OSPP.

7.17.2.8. The DSMD shall monitor the threat status in the Agency and maintain close liaison with the Department of Homeland Security and National-level intelligence and security agencies for timely and accurate threat information.

7.17.2.9. The CCS shall maintain close liaison with the local FBI offices and local law enforcement agencies for threat information.

7.17.2.10. NASA THREATCONS and associated actions are outlined in Appendix L, NASA THREATCON Actions.

7.18 Hazardous Material Security

7.18.1. NASA programs use many different hazardous materials in meeting mission objectives. It is imperative that the use, storage, and protection of these materials be given the highest priority necessary to ensure the safety of NASA personnel and the general public.

7.18.2. In coordination with Center safety, logistics, environmental, and Transportation officials,

Center Security Offices shall develop and implement security plans specifically designed to provide maximum protection in the transportation, receipt, access, use, storage, and accountability of hazardous materials used by NASA. Security Plans shall include:

a. Review of shipping/transportation procedures to ensure appropriate precautions are in place. Recommend changes/adjustments as appropriate.

b. Appropriate sharing of threat information associated with the targeting of hazardous materials.

c. Establishment of Center-specific receipt, escort, and hand-off procedures, as appropriate.

d. Establishment of security procedures for permanent and temporary storage/holding areas.

Chapter 8: Program Security

8.1 General

8.1.1. This chapter provides the requirements for establishing a system security approach in the development of a NASA program or in enhancing the protection level of an active program.

8.1.2. The objective is to identify security provisions as early as possible in system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

8.2 Responsibilities

8.2.1. The CCS for each Center is responsible for the following:

8.2.1.1. Establishing a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.

8.2.1.2. Incorporating appropriate security measures, outlined in the various Chapters of this NPR, into project plans, facility plans, and requests for proposals.

8.2.2. Project and program managers at NASA Centers are responsible for ensuring provisions contained in Chapter 4, section 4.7 of NPR 7120.5B, NASA Program Project Management Processes and Requirements, are appropriately addressed with the CCS.

8.2.3. The DSMD shall compile and maintain the Agency Mission Essential Infrastructure (MEI) Inventory of NASA mission essential infrastructure assets. The List shall consist of:

8.2.3.1. Critical or Key Asset description (Cyber, Physical or both).

8.2.3.2. Owning Center/Program

8.2.3.3. Physical Location

8.2.3.4. Responsible Enterprise

8.2.3.5. Whether part of Agency Continuity Of Operations (COOP) Planning Program.

8.2.4. Center program/project managers shall ensure that critical programs or assets are identified for inclusion on the consolidated inventory and that program planning includes security provisions and funding.

8.3 Acquisition Systems Protection (ASP)

8.3.1. ASP enables the establishment of definitive security requirements in the acquisition or modification of systems, equipment, and facilities; the analysis of security design and engineering vulnerabilities; and the development of recommendations consistent with other design and operational considerations.

8.3.2. ASP supports the development of programs and standards that provide life-cycle security for critical NASA resources.

8.3.3. ASP establishes, as part of each major acquisition development and upgrade program,

appropriate procedures to identify security risks and actions to eliminate or minimize associated vulnerabilities.

8.3.4. ASP provides a means to ensure that necessary security requirements (physical, personnel, technical, communications, and information) are adequately considered and, when appropriate, incorporated into the overall system development program.

8.3.5. The ASP plan for each Center shall incorporate security into major systems, as applicable, to support economical achievement of overall program objectives.

8.3.6. The plan shall include those security tasks applicable to each phase of the acquisition process.

8.4 NASA Critical Infrastructure and Key Resources -Mission Essential Infrastructure (MEI) Protection Program

8.4.1. Homeland Security Presidential Directive (HSPD) 7 "Critical Infrastructure Identification, Prioritization, and Protection," directs every Government agency to establish a program to identify critical essential infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as MEI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

8.4.2. An effective critical asset protection program provides affordable, practical, and responsible protection, within acceptable risks, to those vital NASA resources that cannot reasonably be replaced or that have unique capabilities to support NASA goals.

8.4.3. Designated MEI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate security vulnerability risk assessment.

8.4.4. NASA MEI may include IT resources managed under the "Special Management Attention (SMA)" designator; critical components; communication, command, and control capability; Government-owned flight or experimental flight vehicles, shuttles, international space station and apparatus; and one-of-a-kind irreplaceable facilities.

8.4.5. Supporting infrastructure called "interdependencies" shall not be designated as MEI.

a. "Interdependencies" includes those external and internal commercial elements that the Center MEI depend on to operate; e.g., electrical power, gas, communications hubs, local area networks, telephone systems, etc.
b. "Interdependencies" must nevertheless be evaluated for their vulnerability and assessed for their impact if lost, especially if they are "single points of failure." Vulnerability mitigation activity regarding NASA assets designated as "interdependencies" must also take the "single point of failure" aspect into account when developing their mitigation plans.

8.4.6. The NASA Mission Essential Infrastructure Protection Program (MEIPP) shall replace the NASA Resource Program (NRP). All existing NRP assets must be reevaluated against MEI criteria to determine if they warrant continued designation as a critical NASA asset under the MEI designation.

8.4.7. Policy and procedures shall be developed and implemented at each Center that accurately reflect Agency requirements for assessing MEI as outlined in this and other Agencywide requirements. This ensures Agencywide uniformity and consistency in the approach to performing

the appropriate risk vulnerability risk assessments for each identified MEI.

8.4.8. Criteria and procedures NASA Centers shall use in identifying NASA's MEI are contained in Appendix H, Identifying and Nominating NASA Assets for the MEIPP.

8.4.9. Minimum security requirements for MEI facilities or facilities housing MEI assets are provided in Chapter 7, paragraph 7.7.4.

8.5 Operations Security (OPSEC)

8.5.1. National Security Decision Directive (NSDD) 298 establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program.

8.5.2. Security programs and procedures already exist to protect classified information. However, items of information generally available to the public and certain detectable activities can reveal the existence of and possible details regarding classified or sensitive information. Such indicators could potentially benefit those seeking to neutralize or exploit U.S. actions in areas of National security.

8.5.3. OPSEC is a systematic and proven process through which the Government and its supporting contractors can promote operational effectiveness. The process can deny potential adversaries information by identifying, controlling, and protecting generally unclassified evidence concerning the planning and execution of sensitive activities.

8.5.4. Agencies with minimal activities affecting National security are not required to establish a formal OPSEC program; therefore, NASA does not require a formal Agency-level OPSEC program, although some Centers have programs that do require OPSEC application.

8.5.5. The NASA minimum security standard is to employ OPSEC measures on all classified programs.

8.5.6. If OPSEC planning is warranted, program and project managers, in coordination with the Center Counterintelligence (CI) Office, shall develop and implement a project OPSEC plan that shall identify critical information or activity, analyze threat and vulnerability, assess risk, and apply appropriate countermeasures.

8.6 Risk Management Process

8.6.1. NASA has adopted a Risk Management approach in which the risk of loss must be weighed against the cost and operational impact of implementing established minimum-security standards.

8.6.2. Risk management provides a mechanism that allows security and program/project managers to recommend waivers to security standards based upon a threat assessment and the determined risk to an asset.

8.6.3. Risk management is an integrated process of assessing the threat, vulnerabilities, and value of the resource and then applying appropriate safeguards and/or recommending the assumption of risk.

8.6.4. The CCS shall ensure that security standards, established in this and other NPR, are met or that appropriate requests for waivers are submitted and approved by the AA/OSPP.

8.6.4.1. Each Center Director (or for Headquarters, the Director for Headquarters Operations) is designated as the Risk Acceptance Authority (RAA) for the Center.

8.6.4.2. The RAA shall make the final determination on requests for waivers to security standards when the CCS has determined that the waiver shall pose a serious risk on the program.

8.7 Special Access Programs

8.7.1. A Special Access Program shall be created within NASA only upon specific written approval of the Administrator, and coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure required security protocols are implemented and maintained. .

8.7.2. All personnel security requirements for NASA personnel to establish and participate in Special Access Programs external to NASA must be coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure accountability of NASA equities..

8.7.3. All NASA security activity associated with Special Access Programs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG).

8.8. Secure Compartmented Information (SCI) Programs

8.8.1. SCI Programs shall only be created within NASA upon specific written approval of the Administrator and coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure required security protocols are implemented and maintained.

8.8.2. All requests for NASA personnel, including NASA contractors, to participate in SCI Programs external to NASA must be coordinated with the Chief, Intelligence and Special Access Programs Support Division to ensure accountability of NASA equities.

8.8.3. Failure to comply with the requirements of this section may result in denial of security clearance and suspension of SCI activity.

8.9 NASA Security Education and Training, and Awareness (SETA) Program

8.9.1. General.

8.9.1.1. The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them.

8.9.1.2. Management and employee involvement is essential to an effective security program.

8.9.1.3. An integral part of the overall NASA Security Program relies on the education and training of individuals regarding their security responsibilities.

8.9.2. Responsibilities.

8.9.2.1. As a minimum, the Center Director shall ensure that adequate procedures are in place whereby all NASA employees and contractor personnel, regardless of clearance status, are briefed annually regarding Center security program responsibilities.

8.9.2.2. The CCS for each Center shall ensure that appropriate and knowledgeable security personnel provide and receive the applicable types of briefings or training as described in paragraph 8.8.3. below.

8.9.2.3. NASA supervisors shall ensure job-related, facility-oriented security education, and awareness instruction or training for newly assigned personnel are timely and properly coordinated

with the CCS.

8.9.3. Required Briefings and Training.

8.9.3.1. Initial orientation briefings are given by security personnel (i.e., NASA and/or security services contractor) to acquaint new employees with local security procedures and employee responsibilities to protect personnel and Government property from theft, loss, or damage.

8.9.3.2. Initial orientation briefings must be conducted within 20 days of the new employee/contractor arrival.

8.9.3.3. Security orientation briefings are given by the responsible supervisor or designee to each new employee and shall include all security requirements and procedures for which the employee is to be specifically responsible.

8.9.3.4. Upon conclusion, the supervisor or designee must ensure that NASA Form 838, Employee Security Orientation/Indoctrination Record, is completed by both individuals.

8.9.3.5. The supervisor shall ensure that the record copy of the form is promptly forwarded to the CCS for processing and permanent filing.

8.9.3.6. The CCS shall ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance.

a. This briefing shall include general security aspects affecting employment and a summary of restrictions and obligations associated with access to classified information that are imposed by statute or executive order. The briefing shall also include standards of behavior expected of persons in sensitive positions and the responsibility of security clearance holders to report behavior that shall disqualify an individual from security clearance eligibility.
b. The security person giving the briefing shall ensure that the employee is made aware of the most current executive order number if the briefing form has not been revised to reflect that change.
c. Upon conclusion of the briefing, a Standard Form 312, Classified Information Nondisclosure Agreement, is signed by both individuals (employee and person giving the briefing).
d. Annual briefings are required for all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Clearances may be suspended or revoke for failure to attend annual training.

8.9.3.7. Classified custodians and any other custodians responsible for CNSI safes, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

8.9.3.8. Security personnel shall give other special security training or briefings to employees, as appropriate, related to SAP's, SCI, MEI, and the Mission Critical Space Systems Personnel Reliability Program.

8.9.3.9. Security personnel shall conduct foreign travel briefings to NASA travelers to enhance their awareness of potential hostile intelligence, terrorist, and criminal threats in the countries to which they are traveling. These briefings must also provide defensive measures and other practical advice concerning safety measures.

8.9.3.10. Security personnel shall conduct security termination briefings to employees whose personnel security clearances are being terminated due to termination of employment, transfer to another Center, or other reasons. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their responsibilities and penalties for

unauthorized disclosure of CNSI even after termination of the clearance or employment.

8.10. Self-Inspections

8.10.1. This section sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the Information, Industrial, Personnel, Physical and Program Security at all NASA Centers.

8.10.2 The objective is to ensure that each Center is implementing their security program in accordance with all applicable NASA and Federal regulations and to identify areas that need to be addressed that are not in compliance with appropriate rules and regulations. The review will also pinpoint commendable areas of each security operation and identify areas that need additional support to complete their mission.

8.10.3 Responsibilities.

8.10.1.1. The Director, Security Management Division (DSMD) is responsible for the agency's self-inspection. The DSMD shall designate agency personnel to assist in carrying out this responsibility. The DSMD shall determine the means and methods for the conduct of self-inspections. These may include:
(a) A review of relevant security directives, guides, training material and instructions
(b) Interview with security representatives and customers
(c) Review of Information, Industrial, Personnel and Physical Security Programs
(d) Review of various files and documents pertaining to day to day operations

8.10.1.2. The DSMD shall develop a standard self-inspection guide/checklist to be used by the inspectors conducting the review. Each Center shall be inspected at least every 2 years. The format for documenting findings shall be set by the DSMD. The DSMD, in its oversight capacity, may schedule inspections of Centers on an as needed basis.

8.10.4. Coverage of Inspections

These standards are not all-inclusive. Each inspection may be adjusted to meet the coverage of the security programs in place at that particular center.

8.10.4.1. Personnel Security Coverage
a. Personnel Security Program Oversight
b. Basic Principles of Personnel Security Clearance Management
c. Processing Personnel Security Clearance Request
d. Coding of Position Sensitivity Level Designations for National Security Positions
e. Temporary/Interim Access to CNSI
f. Access to CNSI by Non-U.S.Citizens
g. Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations from Other Government Agencies and Organizations.
h. Guiding Principles for Adjudication, Suspension, Denial or Revocation of Personnel Security Clearances
i. Database, File, and recordkeeping management.
j. Suitability Investigations and Determinations
k. Review of Questionnaires for Suitability Investigations.
l. Reinvestigation Requirements
m. Designation of Security Risk Levels for Civil Servants and Contractors
n. Personnel Security Investigative Processing Requirements for Non-NASA employees.
o. Adjudication Process for Center, Facility, and IT System Access.

8.10.4.2. Information Security Coverage

a. Original and Declassification Management
b. Classifying, Marking, and Declassifying Classified National Security Information (CNSI) and Foreign Government Information (FGI)
c. Access to CNSI and FGI
d. Accountability and Control of CNSI and FGI
e. Storage of CNSI and FGI
f. Reproduction of CNSI and FGI
g. Transmission of CNSI and FGI
h. Release of Classified Information to Foreign Governments
i. Destruction of CNSI and FGI
j. Security Violations and Compromise of CNSI and FGI
k. CNSI and FGI Meetings and Symposia
l. Security Container, Vault, and Strong Room Management
m. Access, Storage, Reproduction, Transmission, Destruction and Release of Sensitive But Unclassified Information (SBU).
n. Agency Information Security Program Data Report, SF-311
o. Security Classification Reviews for NASA Programs and Projects
p. Security Education, Training and Awareness Program

8.10.4.3. Industrial Security Program
a. Department of Defense Support Review
b. Processing of DD Form 254
c. Classified Security Contract Management
d. Suspension, Revocation, and Denial of Access to Classified Information

8.10.4.4. Physical Security Program
a. Security Control at NASA Centers
b. NASA Photo Identification Badge Program
c. NASA Photo -ID Issuance Criteria
d. Inspection of Persons and Property
e. Security Areas
f. Facility Security
g. Airfield and Aircraft Security
h. Control and Issuance of Arms, Ammunition, and Explosives (AA&E)
i. Standards for Secure Facilities and Conference Rooms
j. Threat Management
k. Security Force Procedure Review
l. Review of Incident and Threat Report
m. NASA Security Office Special Agent Badge and Credentials Review
n. TSCM Procedures
o. Threat Condition (THREATCONS) Program

8.10.4.5. Program Security
a. Acquisition Systems Protection Review
b. Review of NASA Critical Infrastructure and Key Resources - Mission Essential Infrastructure (MEI) Protection Program.
c. Operations Security Review
d. Risk Management Review
e. Special Access Program Review
f. NASA Security Program Education, Training and Awareness review

Chapter 9: The NASA Security Program - Security Personnel, Federal Arrest Authority and Use of Force Training and Certification

9.1 General

42 U.S.C. 2456a grants authority for the NASA Administrator to prescribe regulations approved by the Attorney General of the United States for the exercise of security program authority, including the assignment of Federal Arrest Authority. Those regulations are set forth in 14 CFR Part 1203b. This chapter identifies the requirements for granting Federal Arrest Authority and discusses use of force in conjunction with Federal Arrest Authority. If expeditious action is not required, the exercise of Federal Arrest Authority granted in accordance with this policy shall be coordinated with the responsible Office of the Federal Bureau of Investigation (FBI) and local Office of the U.S. Attorney.

9.2 Applicability

This chapter applies to all NASA security personnel performing duties in a position to which they shall reasonably be expected to effect an arrest or use varying degrees of physical force to subdue or apprehend an individual. (NOTE: The provisions of this chapter do not apply to NASA Inspector General personnel, whose arrest authority is derived from other sources.)

9.3 Responsibility

9.3.1. The AA/OSPP is the designated Senior Agency Official for the NASA Federal Arrest Authority and Use of Force program and is responsible for:

9.3.1.1. Directing the Federal Arrest Authority and Use of Force program in accordance with applicable laws, NASA regulations, directives, and this NPR.

9.3.1.2. Reviewing and concurring on all Center nominations and plans to implement Federal Arrest Authority and Use of Force, in consultation with representatives designated by the OGC, and the appropriate Mission Directorate Associate Administrator.

9.3.1.3. Reviewing and and approving appropriate administrative actions to correct abuse or violations of any provisions of this NASA regulation.

9.3.2. The DSMD is designated the Federal Arrest Authority and Use of Force Program Manager. The DSMD is responsible for:

9.3.2.1. Informing the Senior Agency Official for Federal Arrest Authority and Use of Force of any unresolved problems or any areas of interest in which Federal Arrest Authority and Use of Force requirements are lacking and any other matters likely to impede NASA objectives in meeting Federal Arrest Authority requirements.

9.3.2.2. Periodically reviewing the Federal Arrest Authority and Use of Force Program and recommending to the Senior Official any changes necessary.

9.3.2.3. Recommending to the Senior Official adequate internal safeguards and management procedures.

9.3.2.4. Coordinating, managing, and summarizing NASA's implementation of the Federal Arrest Authority and Use of Force Program.

9.3.2.5. Accrediting training courses in Federal Arrest Authority and Use of Force in accordance with the qualifications listed in Appendix D, Federal Arrest Authority and Use of Force Qualifications and Training.

9.3.2.6. Seeking the direction and concurrence of the OGC and/or Department of Justice or their designee on matters related to the Federal Arrest Authority and Use of Force Program.

9.3.3. Center Directors have the following responsibilities:

9.3.3.1. Implementing and maintaining the NASA Federal Arrest Authority program at their respective Center. Essential to implementing and maintaining a viable NASA Federal Arrest Authority and Use of Force program at the Center level is ensuring that adequate numbers of qualified civil service personnel and contract security force personnel are identified, selected, and properly trained under NASA Federal Arrest Authority and Use of Force requirements per Appendix D, Federal Arrest Authority and Use of Force Qualifications and Training. This will be accomplished by:

(NOTE). Essential to implementing and maintaining a viable NASA Federal Arrest Authority and Use of Force program at the Center level is ensuring that adequate numbers of qualified civil service personnel and contract security force personnel are identified, selected, and properly trained under NASA Federal Arrest Authority and Use of Force requirements per Appendix D, Federal Arrest Authority and Use of Force Qualifications and Training.

a. Providing the names and qualifications of any personnel nominated for FAA to the AA/OSPP for concurrence prior to assigning duties as a uniformed armed law enforcement official and/or armed, plain clothed, NASA Special Agent.

b. Immediately reporting any abuse or violation of this directive in writing to the DSMD.

c. Upon notification, immediately suspending from duty with pay or reassigning to other duties not requiring exercising Federal Arrest Authority, any person with Federal Arrest Authority accused of violations of Federal Arrest Authority procedures or instructions, pending investigation of the incident. In consultation with the Center Office of Chief Counsel, determining the case's disposition at the conclusion of the investigation.

9.3.4. Federal, State, and/or local law enforcement agencies generally have law enforcement jurisdiction at most NASA Centers. When State, and local law enforcement agencies do not have legal jurisdiction or, when they, and local federal law enforcement are unable to provide essential and consistent onsite law enforcement services in a timely and effective manner the CCS shall select NASA security employees and/or contractors for Federal Arrest Authority to ensure appropriate arrest capabilities.

9.3.4.1. Upon implementation of Federal Arrest Authority, the CCS shall coordinate with their supporting office of the FBI regarding procedures for the appropriate and timely transfer of arrested persons.

9.3.5. In consultation with the Center Office Chief Counsel, local Office of Inspector General, and responsible United States Attorney, the CCS shall develop appropriate chain of custody procedures and establish the necessary relationships with local law enforcement and Federal law enforcement

agencies to ensure issuance and execution of necessary arrest warrants.

Chapter 10: Glossary of Terms, Abbreviations, and Acronyms

Access - Used under two separate and distinct contexts within this NPR:

(1). The ability, opportunity, and authority, to gain knowledge of classified information or gain authorized entry onto a NASA classified IT resource. (Refer to Chapters 2 and 6), or;

(2). The act of obtaining authorized physical entry onto a NASA Installation, facility, or unclassified NASA IT resource (Refer to Chapters 3 and 4).

Access Control System - Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information technology system is approved to operate in a particular security mode for the purpose of processing CNSI, using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

ACI (Administratively Controlled Information) - Official NASA or other government information and material, of a sensitive but unclassified nature, which does not contain National security information (and therefore cannot be classified), nonetheless, must still be protected against unauthorized disclosure.

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, or access to NASA facilities, information, or IT resources, is in the best interest of National security or efficiency of the Government.

Administrative Downgrade - A determination that an individual's level of access to classified information requires reduction or removal based solely upon a change in the individual's "Need to Know." It is not an adverse action.

Adverse Impact - An act or occurrence that results in a negative outcome and/or damage of an asset, program, mission, or operation thereby delaying or interrupting performance for a specified short period of time.

Arrest Authority - The power to execute arrests, without a warrant, and to conduct searches incident to an arrest, granted to designated NASA Security Officials and Security Services Contractors, pursuant to Section 104(f) of the National Aeronautics and Space Act of 1958, as amended, and 14 CFR Part 1203b.

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.

Asset Value - The established worth of a particular asset or resource. May be assessed relative to: monetary value, current replacement value, historic value, political value, prestige, or a combination.

Background Investigation (BI) - The BI consists of a Personal Subject Interview, a basic National

Agency Check (NAC) including credit search, personal interviews with employment, residence (neighbors), educational sources, and law enforcement searches. Total coverage is for a 5-year period. A BI is required for all High Risk positions.

Baseline Physical Security Posture - An initial determination, based on a physical security vulnerability assessment that describes the Center's existing security posture, from which the CCS can recommend or require adjustments in order to bring the security posture up to minimum standards, if necessary.

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

Central Adjudication Facility (NASA CAF) - Facility established at the DSMD level responsible for adjudicating all requests for clearances to access CNSI.

Certifying Authority (CA) - Individual responsible for ensuring and certifying, to the DAA, that requisite security measures are implemented for IT Systems identified for processing of classified information.

Certifying Officials - The AA/OSPP, DSMD, Center Directors, or the Center Chief of Security who are, by virtue of this NPR, authorized to certify that an individual has met established requirements (training, firearms qualification, etc.), can perform those security functions designated in their position description, and can carry a firearm in performance of their security duties. They can also approve the use of a security room, vault, or container for storage of CNSI.

Certification - Used under two separate contexts in this NPR:

(1) 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.

(2) A formal process implemented at the CCS level to ensure a room, vault, or security container meets minimum structural and physical security attributes necessary to ensure adequate protection of CNSI. Certified Tempest Technical Authority (CTTA) - Designated official responsible for performing Tempest countermeasures cost and security analyses prior to the implementation of Tempest countermeasures.

Classification Category - The specific degree of security classification that has been assigned to CNSI to indicate the extent of protection required in the national interest:

(1) **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.

(2) **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.

(3) **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.

Classification Guide - The written direction issued or approved by a Top Secret Original Classification Authority (TS/OCA) that identifies the information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material.

Classified National Security Information (CNSI) - Information that must be protected against

unauthorized disclosure IAW Executive Order (EO) 12958, "Classified National Security Information," as amended, and is marked to indicate its classified status when in documentary form. See definition for "Classification Category" above.

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.

Cleared Person - An individual who has been granted a security clearance making them eligible to access CNSI up to and including the cleared level.

Closed Area - A space in which security measures are applied primarily to safeguard CNSI and material with entry to that space being equivalent to access to such classified information and material.

Competent NASA Medical Authority - A NASA civil service or contract physician responsible for reviewing medical records, providing results of medical evaluations, and interpreting evaluations as they relate to reliable performance of duties for the NASA Mission Critical Space Systems Personnel Reliability Program.

Component Facilities - NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, NASA IV&V).

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

Communications Security (COMSEC) - The protection resulting from the application of crypto security, transmission security, and emission security measures to telecommunications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value that might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

Continuous Evaluation Program (CEP) - A process, established under this NPR, to ensure personnel employed by NASA or its contractors maintain eligibility for employment and access to CNSI, NASA facilities, information, and resources.

Contractor - For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

Counterintelligence - Information gathered and activities conducted to protect against espionage and sabotage and other intelligence activities conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document, or communications security.

Credit Searches - Credit searches are conducted as part of the Minimum Background Investigation (MBI), Limited Background Investigation (LBI), Background Investigation (BI), Single Scope Background Investigation (SBI), Periodic Reinvestigation (PRI), Upgrade, and Update cases. Credit searches shall be conducted in conjunction with a National Agency Check and Inquiries (NACI) upon initial entry of duty (EOD) for all appointees and as needed to review the suitability of an employee who is moving from a low or moderate risk position to a high risk position. Credit searches shall also be completed upon reinstatement or transfer of a federal employee whose BI is otherwise in order. Credit searches are not routinely performed on current employees.

Amendments to the Fair Credit Reporting Act (FCRA) (15 U.S.C. - 1681, et seq) address permissible purposes for which consumer reports may be furnished and conditions for furnishing and using consumer reports for employment purposes. Subsection 1681b (b)(2) of Title 15 requires that the applicant/employee must authorize this use in writing before the consumer report is obtained.

Subsection 1681b (b)(3) of Title 15 requires that, before taking an action adverse to the employee or applicant for employment based in whole or in part on a consumer report, the agency must notify the consumer of the proposed negative action and provide the consumer with a copy of the report and a copy of the Federal Trades Commission's (FTC) Consumer Rights Notice.

Critical-Sensitive (CS) (EO 10450) - 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.

Critical Infrastructure - Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Public Law 107-56, U.S. Patriot Act Section 1016 (e))

Cryptographic Information - All data and material, including documents, devices, equipment and apparatus, essential to the encryption, decryption, or authentication of telecommunications. Whenever such cryptographic information is classified, the material is marked "CRYPTO," and the specific security classification is indicated.

Custodian (Classified Material) - Any authorized person who possesses the appropriate security clearance and is in possession of and responsible for safeguarding classified information or material.

Deadly Force - A degree of force that a reasonable person would consider likely to cause death or serious bodily harm.

Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

Decertification - Used in the context of rooms, vaults, or security containers designated for approved storage of classified material. Indicates a formal process developed and implemented to remove a room, vault, or security container from the Center inventory of approved CNSI storage mediums.

Declassification - The authorized change in the status of information from classified information to unclassified information.

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 EO 12968 have been exercised.

Derivative Classification - The incorporating, paraphrasing, restating or generating, in new form, information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification direction. The duplication or reproduction of existing classified information is not derivative classification.

Designated Approving Authority (DAA) - Official who formally assumes responsibility for operating an ITS or network at an acceptable level of risk.

Designated Country (Foreign National) - Citizen of a Foreign Country to which the United States has no official diplomatic relationship due to the country having ties to or sponsors terrorists, nuclear proliferation concerns, missile technology concerns, or is engaged in supporting the illegal trafficking in arms or drugs, or both.

Downgrading - the authorized reduction of the classification category of information to a lower classification category.

Duress Alarm - A mechanical or electronic device that enables threatened personnel to alert a response force in order to obtain immediate assistance without arousing the suspicion of the perpetrator.

Escort - The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, authorized topics of discussion, etc.

Executive Order (EO) - Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Foreign National - 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. Includes 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.

Foreign Person - Any person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). Also means any foreign corporation, business association, partnerships, trust, society or any other eneitity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

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.

Grant Recipient - Organization (Universities, nonprofits, etc.) or individual that has received official designation and funding to perform specific research on behalf of NASA.

High Risk Position - Any position whose duties involve responsibilities and authorities that if misused can reasonably be expected to cause exceptionally serious adverse impact on NASA's mission.

HRO - Human Resources Office.

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.

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. Can include Foreign Nationals.

Infrastructure - A collection of assets. See definitions for asset and system.

IT-1 Position - Any IT position whose duties, responsibilities, and authorities involve accessing information or system controls that if misused can reasonably be expected to cause exceptionally serious adverse impact.

IT-2 Position - Any IT position whose duties, responsibilities, and authorities involve accessing information or systems that if misused can reasonably be expected to cause serious adverse impact or allow for great personal gain.

IT- 3 Position - Any other IT position whose duties, responsibilities, and authorities involve accessing information that if misused could reasonably be expected to have minimum adverse impact on the Agency's mission.

Integrity - The condition that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

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.

Interim Clearance - Temporary clearance granted; while awaiting completion of the completed investigation and issuance of final security clearance, as a result of a favorable review of submitted investigative forms.

Intermediate Use of Force - Term used to define an escalation in necessary force required to subdue a suspect that is between minimum force and deadly force.

International Partners - Foreign Nationals or U. S. citizen representatives of foreign governments, who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

International Traffic in Arms Regulation (ITAR) - Regulations governing exports of national defense articles and national defense services (22 CFR Part 120).

Interdependency - Used in the context of the NASA mission essential infrastructure (MEI) protection program. Any asset that an MEI is dependent upon; NASA or other agency owned or operated that the MEI uses to perform its mission (e.g. power, communications, facility, other utilities, etc.) that if destroyed or otherwise interrupted could adversely impact the continued viability of the MEI asset.

Intrusion Detection System (IDS) - A security alarm which consists of one or more various types of components used to detect, assess, and notify of unauthorized access into a protected area.

Information Security Oversight Office (ISOO) - Office established under the Executive Office of the President (EOP) tasked with policy development and oversight of Federal agency compliance with National-level policy for management of CNSI.

Key Resources - Publicly or privately controlled resources essential to the minimal operations of the economy and government (Public Law 107-296, The Homeland Security Act, Section 2(9)). Key resources include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

Lautenberg Ammendment - The Lautenberg Amendment to the Gun Control Act of 1968 became effective 30 September 1996. The Lautenberg Amendment makes it a felony for anyone convicted of a misdemeanor crime of "domestic violence" (e.g., assault or attempted assault on a family member) to ship, transport, possess, or receive firearms or ammunition. There is no exception for law enforcement or security personnel engaged in official duties. The Amendment also makes it a felony for anyone to sell or issue a firearm or ammunition to a person with such a conviction. This includes

NASA personnel and contractors who furnish weapons or ammunition to persons knowing, or having reason to believe, they have qualifying convictions.

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 CFR, Part 7, Section 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.)

Level of IDS Protection - Number of sensor types used in an IDS system to protect an area, i.e., door switches and motion detectors in use in one area constitute two levels of protection.

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 CFR, Part 7, Section 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. See definitions for Foreign National, Foreign Persons, and U.S. Persons in this chapter).

Likelihood of Aggressor Activity - A determination by qualified security, law enforcement, and intelligence professionals, based on thorough knowledge and evaluation of intelligence data, that an "aggressor" is or is not likely to be interested in compromising a NASA asset.

Limited Area - A space in which security measures are applied primarily for the safeguarding of classified information and material or unclassified property warranting special protection and in which the uncontrolled movement of visitors would permit access to such classified information and material or property. But within such space, access shall be prevented by appropriate visitor escort and other internal restrictions and controls.

Limited Background Investigation (LBI) - The LBI consists of a personal subject interview, a basic National Agency Check (NAC) including a credit search, personnel interviews with employment, residence (neighbors), and educational sources, and law enforcement searches. Coverage is for a 3-year period while record searches are for a 5-year period. The MBI or LBI may be conducted for Moderate Risk positions.

Local Records Check (LRC) - Process of checking with local law enforcement agencies and courthouses for the purpose of obtaining, substantiating, or refuting information related to an individual(s) undergoing a background investigation.

Limited Privileged Access - Granted to a user to use system-level commands and files to bypass security controls for part of a system.

Low Risk Position - Any position whose duties involve responsibilities and authorities that if misused could reasonably be expected to have limited to no adverse impact on the Agency's mission.

Mandatory Declassification Review - The review for declassification of cl , ass , ifi , ed information in response to a request for declassification that meets the requirements under PART 3 of EO 12958.

Minimum Background Investigation (MBI) - The MBI consists of a personal subject interview, a basic National Agency Check (NAC), and a credit search covering a 5-year period. The MBI or LBI may be conducted for Moderate Risk positions.

Mission-Critical Space Program Personnel Reliability Program - Any Personnel Reliability Program (PRP) status and duties, which, if performed by employees in a faulty, negligent, or malicious manner, could jeopardize mission-critical space systems and delay a mission.

Mission-Essential Infrastructure (MEI) - Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations. These resources may include critical components and facilities associated with the Space Shuttle, expendable launch vehicles, associated upper stages, Spacelab, International Space Station, command communication and control capability, Government-owned flight or experimental flight vehicles and apparatus, and one-of-a-kind irreplaceable facilities.

Mission Essential Infrastructure Protection Program (MEIPP) - The planning and implementation , of an enhanced protection level for Agency key resources identified by an NASA organization to be so crucial to the success of NASA missions as to warrant protection over that which would be routinely provided to NASA assets.

Moderate Risk Position - Any position whose duties involve responsibilities and authorities that if misused can reasonably be expected to cause moderate adverse impact on NASA's mission.

NASA Employee - NASA Civil Service personnel.

NASA-Controlled Facility - NASA Centers and individual facilities where access is c , ontrolled by issuance and mandatory use of photo-identification badges, armed security force personnel, and electronic access control systems to ensure only authorized personnel are admitted.

NASA PHOTO-ID - refers to the NASA photo-ID that has any number of imbedded and external technology capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded "smart card" chip.

NASA National Agency Check - Conducted electronically by NASA Security Offices of the files of the Federal Bureau of Investigation (including fingerprint files), Office of Defense Central Index of Investigations (DCII), the Office of Personnel Management, or other Government agencies, as appropriate. The files of the Bureau of Immigration and Customs Enforcement (BICE), the Central Intelligence Agency, and the U.S. State Department shall be reviewed, as available, when the individual is a resident alien or naturalized citizen of the United States.

National Agency Check (NAC) - The NAC is a search of the following four indices:

(1) U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.

(2) Federal Bureau of Investigation (FBI) Identification Division (FBIF) contains a fingerprint index and name file.

(3) FBI Records Management Division (FBIN) contains files and records of all other investigations (e.g., background, criminal, loyalty, intelligence); and

(4) Defense Clearance and Investigations Index (DCII) contains investigations, including criminal investigations, conducted on civilian and military personnel in the Department of Defense.

(Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)

National Agency Check and Inquiries (NACI) - The NACI is a NAC that also includes written inquiries sent to employers, educational sources, law enforcement agencies, and references. The NACI is the minimum acceptable investigation for access to government facilities.

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:

(1) **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.

(2) **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.

(3) **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.

Need to Know - An administrative determination made by the authorized holder of classified information, that a prospective recipient has the requisite security clearance and requires access to specific classified information in order to perform or assist in lawful and authorized Governmental functions.

Noncritical Sensitive (NCS) (EO 10450) - One of the three levels for designating national security-related positions and the degree of risk involved. Includes any position involving access to Secret or Confidential information.

Non-deadly Physical Force - Pursuant to a lawful arrest by a security force officer, only that physical force which is reasonable and necessary to apprehend and arrest the offender; to prevent the escape of the offender; or to defend himself, herself or a third person from what is reasonably believed to be the use or threat of imminent use of non-deadly physical force by the offender. Verbal abuse alone by an offender cannot be the basis under any circumstances for the use of non-deadly physical force.

Nondesignated Country - Country with which the United States has favorable diplomatic relations.

Nondisclosure Agreement - Generally in the form of an SF 112 (Nondisclosure Form) signed by the individual receiving a security clearance or given access to CNSI that acknowledges responsibility to share information of a classified nature only with personnel possessing the appropriate clearance and a demonstrable need-to-know.

Non-NASA Employee - Any individual, (e.g., other Federal Agency Civil Service personnel on detail to NASA, contractor, grantee, research associate) who is not a NASA Civil Service employee.

Nonsensitive Position Designation -

Nonsensitive Position Designation - Any NASA position that does not require access to CNSI.

Open Storage - Storage of CNSI in a security vault or strong room that does not incorporate secondary level storage in security containers.

Ordinary Force - A degree of force that is neither likely nor intended to cause death or great harm.

Original Classification Authority (OCA) - An individual authorized in writing, either by the President or by agency heads or other senior Government officials designated by the President, to classify information in the first instance.

Periodic Reinvestigation (PRI) - The PRI consists of a National Agency Check, a credit search, a Personal Subject Interview, selected record searches (e.g., law enforcement, personnel security files, and official personnel files (OPF)). Coverage is for a 5-year period. A PRI is required for all High Risk positions.

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 CFR, Part 7, Section 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.)

Presidential Decision Directive - Official documents whereby the President of the United States promulgates Presidential decisions on national security matters.

Personal Subject Interview (PRSI) - A Personal Subject Interview is an essential element of a background investigation and provides the subject of an investigation the opportunity to update, clarify, and explain information on their investigative questionnaire.

Physical Security Vulnerability Risk Assessment - A formal review, conducted by security professionals, that evaluates the physical security posture of an asset to assist in determining the overall security vulnerability of the asset.

"Private" NASA IT System - Those NASA IT systems to which access is restricted and appropriately controlled through a formal process. Granting of access is contingent upon a favorable security background investigation commensurate with the risk level of the system.

Privileged Access - That which is granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

Protected Persons - A non-U.S. citizen allowed into the country under "refugee," "displaced person," "religious," or "political" persecution status.

"Public" NASA IT System - Those NASA IT systems to which access is unrestricted.

Public Trust Positions - Public Trust Positions have the potential for affecting the integrity, efficiency, and/or effectiveness of NASA's mission, and when breached, diminishes public confidence. Classic public trust positions include law enforcement and public safety and health. Positions with responsibility for managing programs or operations require a high degree of public trust because of their ability to significantly affect the accomplishment of NASA's mission.

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

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

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

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

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

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

(5) **R** elatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization of disbursement from systems of dollar amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system.

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

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

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

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

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

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

(5) **P** ositions with responsibility for the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the high risk level to ensure the integrity of the system. Such positions may include but are not limited to:

(a) **A** ccess to and/or processing of sensitive but unclassified information and/or data, including, but not limited to: proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

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

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

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

Reasonable Force - Only that force necessary to overcome an opposing force.

Reimbursable Suitability/Security Investigation (RSI) - The RSI is a concentrated investigation to obtain additional information to resolve issues or to establish a history or pattern of behavior.

Reliability - Term used to denote contractor employee fitness for unescorted access to NASA Centers, facilities, and information technology. Determined by the conduct of a background investigation appropriate for the risk level of the position to be occupied.

Restricted Area - A space in which security measures are applied to safeguard or control property or to protect operations and functions that are vital or essential to the accomplishment of the mission assigned to a Center or Component Facility.

Restricted Data (RD) - Data developed by the Department of Energy (DOE) with extremely strict access restrictions.

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 EO 12968 have been exercised.

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 the risk.

Risk Acceptance Authority (RAA) - An individual designated in writing who makes the final determination on waivers to security standards and requirements when a security deficiency has been determined to pose a serious risk to a program.

Risk Assessment - A formal process whereby a project, program, or event is evaluated to determine the types and level of risk associated with its implementation.

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

Security Adjudication Review Panel (SARP) - A group of senior management officials designated by the AA/OSPP who are responsible for assessing and determining the appropriateness of a removal or denial of a security clearance.

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.

Security Survey - A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

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

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

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.

Sensitive But Unclassified (SBU) Controlled Information/Material - Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the

source of information, or to meet access restrictions established by laws, directives, or regulations:

(1) ITAR - International Traffic in Arms Regulations
(2) EAR - Export Administration Regulations
(3) MCTL - Militarily Critical Technologies List
(4) FAR - Federal Acquisition Regulations
(5) Privacy Act
(6) Proprietary
(7) FOIA - Freedom of Information Act
(8) UCNI - Unclassified Controlled Nuclear Information
(9) NASA Developed Software
(10) Scientific and Technical Information (STI)
(11) Source Selection and Bid and Proposal Information
(12) Inventions

Significant Adverse Impact - An act or occurrence that results in a negative outcome and/or damage/destruction of an asset, program, mission, or operation thereby delaying, interrupting, or prohibiting performance and mission accomplishment for an unspecified period of time.

Single Scope Background Investigation (SSBI) - The SSBI consists of a Personal Subject Interview, National Agency Check, credit search, personal interviews of sources, written inquiries, and record searches, which cover specific areas of the subject's background during the past 10 years.

Special Access Program (SAP) - Any program established and approved under EO 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Special Security Office - Organization responsible for managing security programs related to special access and SCI operations.

Special Sensitive (SS) (EO 10450) - One of the three sensitivity levels for designating National security-related positions and the degree of risk involved, including any position that the head of the Agency determines to be in a level higher than Critical-Sensitive because of the greater degree of damage that an individual, by virtue of occupancy of the position, could cause to the National security or because of investigative requirements for this position under authority other than EO 10450 (e.g., NSD 61 which standardizes the scope and coverage for all investigations conducted for access to Collateral Top Secret/National Security Information, and Sensitive Compartmented Information).

Strong Room - Any room within a NASA building that has been modified to meet minimum construction and physical security standards for storage of CNSI. Generally established for "open storage" of CNSI.

Subject Matter Expert (SME) - An individual who possesses in-depth, expert knowledge of a program, process, technology, or information sufficient to establish classification caveats or determine the need or appropriateness of an existing national security classification.

Suitability - Refers to identifiable character traits and past conduct which are sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of a Federal job. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

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

System Security Engineering - A process established to identify and incorporate security provisions as early as possible in program or project system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

Systematic Review for Declassification - The review for declassification of CNSI contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with the requirements under PART 3, Section 3.4 of EO 12958.

TEMPEST - An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations" which are unintentional emissions that could disclose information being transmitted, received, or handled by any automated information processing equipment.

TEMPEST Test - A laboratory or onsite (field) examination to determine the nature and amplitude of conducted or radiated signals containing compromising information, which normally includes detection and measurement of these signals and analysis to determine correlation between received signals, and potentially compromising transmitted signals.

Technical Surveillance - Covert installation or modification of equipment to monitor (visually or audibly) activities within target areas or to acquire information by specialized means.

Technical Surveillance Countermeasures (TSCM) - The means taken to prevent, detect, and neutralize efforts to acquire information by technical surveillance.

Temporary Eligibility for Access - Based on a justified need that meets the requirements of EO 12968, temporary access to CNSI shall be granted before investigations are complete and favorably adjudicated when official functions must be performed prior to completion of the investigation and adjudication process. See Apendix C: SPB Issuance 1-97.

Threat Assessment - A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets.

TSCM Surveys and Inspections - A thorough physical, electronic, and visual examination to detect surveillance devices, technical security hazards, and attempts at clandestine penetration of an area for hostile collection of information.

Update Investigations - (LDI - Update of Previous LBI Completed, BDI - Update of Previous BI Completed, SDI - Update of Previous SSBI Completed). These investigations are conducted due to break in service or to fulfill Agency requirements. They consist of the same coverage as the prior investigation (LBI, BI, and SSBI) from 13 to 60 months of the previous investigation's closing date. (Update LBI=LDI, updated BI=BDI, and updated SSBI=SDI.)

Upgrade Investigations - (BGI - Upgrade to BI from LBI Completed, LGI -Upgrade to LBI from an MBI Completed, SGI - Upgrade to SSBI from BI Completed). These investigations are conducted when there is a change in an employee's position risk level form a lower to a higher sensitivity designation. These investigations provide the proper coverage for the level of investigation currently required and also take into account the scope of the previous investigation. This investigation is for movement upward in sensitivity and covers the period form 0 to 60 months of the previous investigation's closing date. (BGI=LBI to BI, LGI=MBI to LBI, SGI=BI to SSBI.)

Unauthorized disclosure (EO 12958) - A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

UNCI (Unclassified Controlled Nuclear Information) - Sensitive unclassified Government

information concerning nuclear material, weapons, and components, whose dissemination is controlled under Section 148, of the Atomic Energy Act

Uncleared Person - An individual who does not possess a security clearance. This makes them ineligible to access CNSI.

Unreasonable use of Force - Use of force in excess of the degree required to overcome resistance.

Unsupervised environment - (Used in the context of NASA child-care providers) An environment within or outside a NASA Childcare Center that provides for no direct continuous observation of an uninvestigated child-care worker by a properly investigated employee. Observation may take the form of direct personal participation or through video surveillance.

Use of Force Report - A written report, submitted by the arresting officer and supervisor, used to document details of the force used to lawfully subdue an individual.

U.S. Person (non-U.S. Citizen) - For the purpose of implementing protection and accountability under the ITAR; A person who is a lawful permanent resident (LPR) as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do bus , iness in the United , States. It also includes any governmental (federal, state, or local) entity. It does not include any foreign person as defined in this chapter.

Vulnerability Risk Assessment - A formal evaluation, conducted by security professionals, of a critical asset's (e.g., facility, person, equipment, aircraft, spacecraft) risk from theft, sabotage, death, or destruction, resulting in a determination of level of vulnerability and subsequent development and implementation of security measures (physical and procedur , al) designed to negate or eliminate those vulnerabilities.

Waiver - The approved continuance of a condition authorized by the AA/OSPP that varies from a requirement and implements risk management on the designated vulnerability.

Appendix A: Security Policy Board (SPB) Issuance 1-97 - Investigative Standards

Investigative Standards
for Reliability Investigations
for Access to Classified Information

1. Introduction. The following investigative standards 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, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by Government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures, in addition to these requirements, in order to resolve any issue identified in the course of a reliability investigation or reinvestigation.
2. The Three Standards. There are three standards (Table 1 in the appendix summarizes when to use each one):

a. The investigation and reinvestigation standards for "L" access authorizations and for access to Confidential and Secret (including all Secret level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section 4.4 of EO 12958).
b. The investigation standard for "Q" access authorizations and for access to Top Secret (including Top Secret Special Access Programs) and Sensitive Compartmented Information.
c. The reinvestigation standard for continued access to the levels listed in paragraph 2(b).

3. Exception to Periods of Coverage. Some elements of standards specify a period of coverage (e.g., 7 years). Where appropriate, such coverage shall be shortened to the period from the subject's 18th birthday to the present or to 2 years, whichever is longer.
4. Expanding Investigations. Investigations and reinvestigations shall be expanded under the provisions of EO 12968 and other applicable statutes and EOs.
5. Transferability. Investigations that satisfy the requirements of a given standard, are current, and meet the investigative requirements for all levels specified for the standard shall be mutually and reciprocally accepted by all agencies.
6. Breaks in Service. If a person who requires access has been retired or separated from U.S. Government employment for less than 2 years and is the subject of an investigation that is otherwise current, the agency regranting the access shall, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person shall no longer satisfy the standards of EO 12968 (see Table 2).
7. The NAC. The NAC is a part of all investigations and reinvestigations. It consists of a review of the following:

a. a. Investigative and criminal history files of the FBI, including a technical fingerprint search.
b. b. Office of Personnel Management Security/Suitability Investigations Index (OPM SSII).
c. c. DoD Defense Clearance and Investigations Index (DCII).
d. d. Such other national agencies (e.g., CIA, INS) as appropriate to the individuals reliability.

Standard A

NAC with Local Agency Checks and Credit Check (NACLC)

8. Applicability. Standard A applies to investigations and reinvestigations for;

a. Access to Confidential and Secret (including all Secret-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section 4.4 of EO 12958);
b. "L" access authorizations.

9. For Reinvestigations - When to Reinvestigate: The reinvestigation shall be initiated at any time following completion of, but not later than 10 years (15 years for Confidential) from the date of the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)
10. Investigative Requirements. Investigative requirements are as follows:

a. a. Completion of Forms: Completion of Standard Form 86, including applicable releases and supporting documentation.
b. b. NAC: Completion of a NAC.
c. c. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for 6 months or more for the past 7 years.
d. d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.
e. e. Local Agency Checks: As a minimum, all investigations shall include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last 5 years and, if applicable, of the appropriate agency for any identified arrests.

11. Expanding the Investigation. The investigation shall be expanded, if necessary, to determine if access is clearly consistent with the national security.

Standard B

Single Scope Reliability Investigation (SSBI)

12. Applicability. Standard B applies to initial investigations for:

a. Access to Top Secret (including Top Secret Special Access Programs) and Sensitive Compartmented Information (SCI);
b. "Q" access authorizations.

13. Investigative Requirements. Investigative requirements are as follows:

a. Completion of Forms: Completion of Standard Form 86 including applicable releases and supporting documentation.
b. NAC: Completion of a National Agency Check.
c. NAC for the Spouse or Cohabitant (if applicable): Completion of a NAC, without fingerprint cards, for the spouse or cohabitant.

d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.
e. Citizenship: For individuals born outside the United States, verification of U.S. citizenship directly from the appropriate registration authority; verification of U.S. citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).
f. Education: Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the subject during the most recent 3 years.
g. Employment: Verification of all employment for the past 7 years; personal interviews of sources (supervisors, coworkers, or both) for each employment of 6 months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior Federal and military service, including discharge type. For military members, all service within one branch of the armed forces shall be considered as one employment, regardless of assignments.
h. References: Four references, of whom at least two are developed; to the extent practicable, all shall have social knowledge of the subject and collectively span at least the last 7 years.
i. Former Spouse: An interview of any former spouse divorced within the last 10 years.
j. Neighborhoods: Confirmation of all residences for the last 3 years through appropriate interviews with neighbors and through record reviews.
k. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for 6 months or more for the last 7 years.
l. Local Agency Checks: A check of appropriate criminal history records covering all locations where, for the last 10 years, the subject has resided, been employed, and/or attended school for 6 months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds 6 months, local agency checks shall be performed as deemed appropriate.)
m. Public Records: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.
n. Subject Interview: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews shall be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations shall be taken whenever appropriate.
o. Polygraph (only if agencies with approved personnel security polygraph programs): In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation shall include a polygraph examination, conducted by a qualified polygraph examiner.

14. Expanding the Investigation. The investigation shall be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals shall be conducted.

Standard C

Single-Scope Reliability Investigation

Periodic Reinvestigation (SSBI-PR)

15. Applicability. Standard C applies to reinvestigations for:

a. Access to Top Secret (including Top Secret Special Access Programs) and Sensitive Compartmented Information;
b. "Q" access authorizations.

16. When to Reinvestigate. The reinvestigation shall be initiated at any time following completion, but not later than 5 years from the date of the previous investigation (see Table 2).
17. Reinvestigative Requirements. Reinvestigative requirements are as follows:

a. Completion of Forms: Completion of Standard Form 86, including applicable releases and supporting documentation.
b. NAC: Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).
c. NAC for the Spouse or Cohabitant (if applicable): Completion of a NAC, without fingerprint cards, for the spouse or cohabitant. The NAC for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.
d. Employment: Verification of all employments since the last investigation.
e. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of 6 months or more. For military members, all service within one branch of the armed forces shall be considered as one employment, regardless of assignments.
f. References: Interviews with two character references who are knowledgeable of the subject; at least one shall be a developed reference. To the extent practical, both must have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews shall be conducted, including with cohabitants and relatives.
g. Neighborhoods: Interviews of two neighbors in the vicinity of the subject's most recent residence of 6 months or more. Confirmation of current residence regardless of length.
h. Financial Review:

1. Financial Status: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for 6 months or more for the period covered by the reinvestigation;
2. Check of Treasury's financial database: Agencies shall request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

h. Local Agency Checks: A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for 6 months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds 6 months, local agency checks must be performed as deemed appropriate.)
i. Former Spouse: An interview with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.
j. Public Records: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.
k. Subject Interview: A subject interview is conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject interviews shall be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations shall be taken whenever appropriate.

18. Expanding the Reinvestigation. The reinvestigation shall be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals shall be conducted.

Decision Tables

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
CONFIDENTIAL	None	none	NACLC	A
SECRET; "L"	CONF, SLc; "L"	out of date NACLC or SSBI		
TOP SECRET,SCI; "Q"	None	none	SSBI	
	None; CONF, SEC; "L"	current or out of date NACLC		
	TS, SCI; "Q"	out of date SSBI	SSBI-PR	C

TABLE 2: REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service of ___	
CONFIDENTIAL	0 to 14 yrs. 11 mos.	0-23 months	24 months or more
	15 yrs. or more	None (NOTE 1)	NACLC
SECRET; "L"	0 to 9 yrs. 11 mos.	None (NOTE 1)	
TOP SECRET, SCI; "Q"	10 yrs. or more	NACLC	
	0 to 4 yrs. 11 mos.	None (NOTE 1)	SSBI
	5 yrs. or more	SSBI-PR	

NOTE 1: As a minimum, review an updated Standard Form 86 and applicable records. A

NOTE 1: As a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation (NACLC or SSBI-PR) is not required unless the review indicates the person shall no longer satisfy the standards of EO 12968.

Appendix B: 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

3. 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.

4. 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.

5. 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 coercioon 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

12. 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.

13. 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.

14. 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

15. 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 (e.g. 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 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, e.g. 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 (e.g., 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, gameboard, 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;

(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.

Appendix C: SPB Issuance 3-97 - Investigative Standards for Temporary Eligibility for Access

Investigative Standards
for
Temporary Eligibility for Access

1. Introduction. The following minimum investigative standards, implementing section 3.3 of EO 12968, Access to Classified Information, are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.
2. Temporary Eligibility For Access. Based on a justified need meeting the requirements of sect. 3.3 of Executive Order 12968, temporary eligibility for access shall be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility shall be valid until completion of the investigation and adjudication; however, the agency granting it shall revoke it at any time based on unfavorable information identified in the course of the investigation.
3. Temporary Eligibility for Access at the Confidential and Secret Levels and Temporary Eligibility for "L" Access Authorization. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).
4. Temporary Eligibility for Access at the Top Secret and SCI Levels and Temporary Eligibility for "Q" Access Authorization for someone who is the subject of a favorable investigation not meeting the investigative Standards for access at those Levels: As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for a Single Scope Reliability Investigation (SSBI).
5. Temporary Eligibility for Access at the Top Secret and SCI Levels and Temporary Eligibility for "Q" Access Authorization - for someone who is not the subject of a current, favorable personnel or personnel-security investigation of any kind: As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited Single Scope Reliability Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/ Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).
6. Additional Requirements by Agencies. Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads shall establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for reliability investigations developed under section 3.2(b) of EO 12968.

Temporary eligibility for access is valid only at the agency granting it and at other agencies that expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of EO 12968, Access to Classified Information.

Appendix D: NASA Federal Arrest Authority And Use of Force Program Qualifications and Training

D1.1 General

D1.1.1. 42 U.S.C. 2456a, Section 304(f) of the National Aeronautics and Space Act of 1958, as amended, and 14 CFR Part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel authorizes the Administrator to implement an Agency Federal Arrest Authority and Use of Force program to ensure appropriate protection for NASA employees, facilities, information, and missions.

D1.1.2. The Agency Federal Arrest Authority and Use of Force programs shall be managed in strict compliance with the requirements established by the Attorney General of the United States and direction provided in the following paragraphs.

D1.1.3. Failure to maintain qualification, training and certification requirements established under this NPR shall result in denial of Center authorization to arm personnel.

D1.2 Federal Arrest Authority Program

D1.2.1. Qualifications. Federal Arrest Authority shall not be performed unless the Center Director has the following assurances:

a. All Federal Arrest Authority candidates must be physically fit in order to graduate from the NASA Federal Arrest Authority course of instruction.
b. NASA civil service supervisors shall insure that all civil service employees and security contractor personnel nominated for Federal Arrest Authority are physically and emotionally stable.
c. Federal Arrest Authority authorization shall be withheld or suspended pending an assessment of a Federal Arrest Authority candidate's physical and mental health by a qualified physician.
d. That the candidate is currently a certified graduate in accordance with the training described in, but not limited to this Appendix.

D1.2.2. Attendance at the full Federal Arrest Authority basic training course may be waived for civil service candidates only, under the following circumstances:

a. The candidate is a retired or former law enforcement officer who has met all imposed hiring criteria and who has graduated from an appropriate Federal Law Enforcement Training Program (e.g., FLETC, FBI Academy) and has retired within the last 24 months or has attended FLETC, FBI Academy) training within the past 24-months. Under these circumstances, the candidate must only attend the Federal Arrest Authority refresher course, and;
b. The candidate must complete required in-service Use of Force training, intermediate to deadly force; semiannual qualification with assigned firearm (Appendix E); judgmental shooting with the FATS or equivalent training system; and NASA regulations and Center implementing instructions and training concerning Federal Arrest Authority, or;

c. The candidate is not identified as requiring Federal Arrest Authority and therefore, must attend and graduate from the NASA Security Officer Fundamentals Certification Course (SOFCC).

D1.2.3. Selection and Attendance at NASA Federal Arrest Authority Training.

D1.2.3.1. Attendance at Federal Arrest Authority training is required for all Civil Service personnel (CS) tasked with performing duties related to:

a. Investigations.
b. Frequent duty related interactions with outside law enforcement.
c. Oversight of security services contractor guard force.
d. VIP and special event protection details.
e. Activity requiring an individual to be under arms.
f. SWAT, K-9 and other LE emergency response members.

D1.2.3.2. Attendance at Federal Arrest Authority training for security services contractor personnel shall be determined by the CCS and may be limited to:

a. Shift Supervisors (e.g., Capt, Lt., Sgt.).
b. Those conducting investigations.
c. Those performing VIP and special event security details on NASA property.
d. Those uniformed personnel performing duties with responsibility for responding to and managing incidents with the potential for involving a lawful arrest (i.e., traffic enforcement, property crimes, crimes against persons, disturbances, etc.).

   (Note: Duties with the potential for the lawful detaining of a person while waiting to release to proper law enforcement authorities does not meet criteria for attendance at Federal Arrest Authority training.)

(Note: Duties with the potential for the lawful detaining of a person while waiting to release to proper law enforcement authorities does not meet criteria for attendance at Federal Arrest Authority training.)

1.2.3.3. Special Response Teams, K-9 Teams, other LE Emergency Response Teams Centers that utilize specialized contractor security teams, e.g. SWAT, K-9 shall utilize standardized selection criteria that will include a physical fitness test, an oral interview, a job specific physical test, a written test, and a review of employment files (to insure the officer has completed probationary periods and to confirm that the officer is not under any disciplinary cloud.) Each Center may develop their own specific details on what to include within these criteria but, as minimum, must include the requirements identified in Section 1.4, subparagraph b.

1.2.3.4. CS/Contractor personnel performing duties solely as security specialists within the personnel, information, SAP/SCI, IT, and physical security areas; and whose responsibilities center around managing and performing traditional security program duties as: classified material management; facility security inspections; interviews and research for the purpose of adjudicating access or suitability, shall not be armed.

1.2.3.5. Contractor personnel standing static security posts are not required to attend Federal Arrest Authority training. However, in lieu of attendance at NASA FLEA, these personnel must complete the SOFC course, either at KSC or at their home Center. They are not required to receive "Arrest Authority" training.

1.2.4. To ensure consistency Agencywide, the SOFC course shall be developed by KSC-FLEA, and

taught at KSC or at each Center by either KSC or Center-based Federal Arrest Authority certified trainers. The SOFC shall include adequate training on:

a. Use of Force and Intermediate Use of Force.
b. Lawful Detaining of Persons.
c. Unarmed Defensive Tactics.
d. Weapons Qualification.

1.2.5. Mandatory Pass/Fail Testing Program.

To ensure only qualified individuals are afforded the privilege of assuming Federal Arrest Authority status, the following standards shall apply:

a. Must pass all portions of the designated program with minimum 80 percent passing grade.
b. Shall retake the section test one time after inital testing. A repeat failure after retaking the course of instruction shall result in the nominee being dropped from the Federal Arrest Authority program. CCSs are NOT authorized to reduce any training standards established under this NPR.

1.2.6. Individuals authorized Federal Arrest Authority shall carry the appropriate Miranda Advisement of Rights cards.

D1.3 Use of Force

1.3.1. Under NASA Federal Arrest Authority rules and procedures, Security Force personnel performing security duties may find themselves in a situation where they are required to take a person into custody or defend themselves or someone else. How much force the NASA security officer is allowed to use in a tense and potentially dangerous situation depends on the situation and how well the officer is trained and equipped.

1.3.2. Center CCS shall establish and conduct, at least semiannual, Use of Force training concurrent with required weapons qualification. Established training must include the complete "Use of Force Continuum" theory and currently recognized practices to ensure an appropriate level of understanding and practical application is present among security force personnel.

1.3.3. Use of Force Continuum

The use of force continuum always begins with the adage "Reasonable Force," meaning simply: "the level of force necessary to overcome the obstacle." The use of force continuum is termed "a measured continuum" ranging from no force to deadly force. Choosing just the level of force necessary to overcome the obstacle shall usually be judged as "reasonable."

1.3.4. If it becomes necessary to use a firearm as authorized in 14 CFR Section 1203b.107, NASA CCS shall comply with the following procedures:

1.3.4.1. The incident shall be reported to the CCS, who in turn, shall report it to the appropriate supporting law enforcement agency and then to the AA/OSPP as expeditiously as possible with as many details supplied as are available.

1.3.4.2. The officer shall be promptly suspended from duty with pay or reassigned to other duties not involving the use of a firearm, as the Center Director or as the AA/OSPP deems appropriate, pending investigation of the incident.

1.3.4.3. The respective Center Director or AA/OSPP shall appoint an investigating officer to conduct a thorough investigation of the incident. Additional personnel shall also be appointed as needed to assist the investigating officer. Upon conclusion of the investigation, the investigating officer shall submit a written report of findings and recommendations to the appropriate Center Director or AA/OSPP.

1.3.4.5. Upon conclusion of the investigation, the Center Director and/or the AA/OSPP, with the advice of the OGC or Office of Chief Counsel, shall determine the appropriate disposition of the case. If the investigation determines that the officer committed a crime, the information shall be promptly reported to the supporting law enforcement agency.

1.3.5. Prohibitions.

1.3.5.1. Unreasonable use of force is considered misconduct. Such misconduct shall result in administrative, civil, and/or criminal action against the perpetrator.

1.3.5.2. Verbal abuse, verbal threats of violence, nonphysical threats, or nonviolent resistance cannot be the basis for the use of force.

1.3.6. Security Equipment

Security and law enforcement equipment with use of force applications must be authorized by the Center Director or DMSO with the concurrence of the OGC and AA/OSPP, as appropriate.

1.4 Training Curriculum

The NASA Federal Law Enforcement Training Program is developed and managed by the Kennedy Space Center Protective Services Office. The curriculum is approved by the AA/OSPP. Training shall consist of the following topics:

- Legal Studies
- General Law Enforcement Studies and Exercises
- Weapons Familiarization and Qualification

b. Additional standards are required to qualify for SRT, K-9 and other LE emergency response teams. Each Center may set their own specific standards for each of these teams but these standards shall meet the following minimum requirements.

(1). Applicants must meet and maintain a physical fitness standard that includes:

- Obstacle / Agility Course
- o At least 22 Push ups
- o At least 25 Sit ups
- o At least a 1 mile run. (Centers shall set a qualifying time limit.)
- o A task specific physical fitness test; e.g., controlling a dog, running with a breaching ram, carrying/dragging a hostage dummy.

(2). Weapons Qualification: The following weapons qualification scores must be achieved the same day as the physical fitness exam.

- Handgun - 90 or higher
- Shotgun - 90 or higher (if issued)
- Rifle - 90 or higher (if issued)
- Sub-machine gun (if issued)

(3). A written test - (Score 90% or better)

(4) Successful completion of an oral interview.

1.5 Federal Arrest Authority and Use of Force Refresher Training

Personnel trained and certified under the NASA Federal Arrest Authority and Use of Force Training Program will attend and complete 2-week refresher training every 2 years.

Appendix E: NASA Firearms Qualification Courses

NASA Handgun Qualification
and
Course Of Fire Standards

Order	Position	Rounds	Time	Distance	Target
Phase I: Practice					
1. (See note 1)	Standing	6 (3, 2 shot strings)	3 sec.	3 yds.	IPSIC
2. (See note 1)	Standing	8 (4, 2 shot strings)	2 sec.	3 yds.	IPSIC
3. (See note 1)	Standing	6 (3, 2 shot strings)	3 sec.	5 yds.	IPSIC
4. (See note 1)	Standing	6 (3, 2 shot strings)	4 sec.	7 yds.	IPSIC
5. (See note 2)	Standing	6 (4, reload fire 2)	12 sec.	7 yds.	IPSIC
6. (See note 2)	Standing	12 (6, reload fire 6)	30 sec.	15 yds.	IPSIC
7. (See note 3)	High Barricade	6 (3,& 3)	20 sec.	25 yds.	IPSIC
50 Total Rounds					
Phase II: Evaluation					
1. (See note 1)	Standing	6 (3, 2 shot strings)	3 sec.	3 yds.	IPSIC
2. (See note 1)	Standing	8 (4, 2 shot strings)	2 sec.	3 yds.	IPSIC
3. (See note 1)	Standing	6 (3, 2 shot strings)	3 sec.	5 yds.	IPSIC
4. (See note 1)	Standing	6 (3, 2 shot strings)	4 sec.	7 yds.	IPSIC

5. (See note 2)	Standing	6 (4, reload fire 2)	12 sec.	7 yds.	IPSIC
6. (See note 2)	Standing	12 (6, reload fire 6)	30 sec.	15 yds.	IPSIC
7. (See note 3)	High Barricade	6 (3,&3)	20 sec.	25 yds.	IPSIC
50 Total Rounds					
100 Total Rounds for course					
Phase III: Qualification					
1. Each round striking the target counts as 1 hit.					
2. Minimum passing score is 40 hits (80 percent), 45 hits (90percent) for Emergency Response Team (ERT) personnel.					

Notes:

Note 1: Shooter will start with the weapon in the low ready position, finger off the trigger, and weapon for each string of fire.

Note 2: Shooter will start with the weapon secure in the holster.

Note 3: Shooter will start in the right barricade position fire three rounds, ensure finger is off the trigger, move to the left barricade position, and fire three more rounds.

NASA Shotgun Qualification
And
Course of Fire Standards

Order and Position	Rounds	Time	Distance	Target
Phase I: Practice (See notes)				
1.Standing, strong hand	2	see note 1	15 yds.	IPSIC
2. Standing, weak hand	2	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	2	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	2	see note 1	7 yds.	IPSIC
8 Total Rounds				

Phase II: Evaluation (See notes)				
1. Standing, strong hand	3	see note 1	15 yds.	IPSIC
2. Standing, weak hand	3	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	3	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	3	see note 1	7 yds.	IPSIC
12 Total Rounds 20 Total Rounds (for course)				
Phase III: Qualification				
1. Each pellet striking the target counts as 1 hit. 2. Minimum passing score is 86 hits (80 percent), 97 hits (90 percent) for Emergency Response Team (ERT) personnel.				

Notes:

Note 1: Time limit for practice is 45 seconds and evaluation is 60 seconds.

Note 2: Shooter will start in with six rounds in the weapon. On the fire command they start the course firing three rounds from the strong side standing, and three rounds form the weak side standing. Keeping the weapon pointed down range, reload as you move to the ten-yard line and fire three shots strong hand kneeling. Move to the seven-yard line, reload the remaining three rounds from behind cover, and fire from the kneeling position, weak side barricade.

Note 3: Practice course is fired with two rounds from each position.

NASA Rifle Qualification
and
Course of Fire Standards

Order	Position	Rounds	Time	Distance	Target
Phase I: Zero					
1.	Shooter's choice	3	N/A	100 yds.	IPSIC
2.	Shooter's choice	3	N/A	100 yds.	IPSIC
3.	Shooter's choice	4	N/A	100 yds.	IPSIC
10 Total Rounds					

Phase II: Practice					
1.	Prone Supported	10	30 sec.	100 yds.	IPSIC
2.	Prone Unsupported	10	30 sec.	100 yds.	IPSIC
3.	Kneeling /Sitting	10	30 sec.	100 yds.	IPSIC
4.	Kneeling/Sitting	10	30 sec.	50 yds.	IPSIC
5.	Standing	10	30 sec.	25 yds.	IPSIC
50 Total Rounds					
Phase III: Evaluation					
1.	Prone Supported	10	30 sec.	100 yds.	IPSIC
2.	Prone Unsupported	10	30 sec.	100 yds.	IPSIC
3.	Kneeling /Sitting	10	30 sec.	100 yds.	IPSIC
4.	Kneeling/Sitting	10	30 sec.	50 yds.	IPSIC
5.	Standing	10	30 sec.	25 yds.	IPSIC
50 Total Rounds 110 Total Rounds for course					
Phase IV: Qualification					
All hits on the IPSC target count. The Shooter must have 40 hits out of 50 for successful qualification. Emergency Response Team (ERT) officers must have 45 hits out of 50.					

NASA Submachine Gun Qualification
and
Course Of Fire Standards

Order	Position	Rounds	Time	Distance	Target
Phase I: Practice					
1. (See note 1)	High Barricade	10 (5, 2 shot strings)	4 sec.	25 yds.	IPSIC
2. (See note 2)	Standing	16 (15, reload fire 1)	25 sec.	15 yds.	IPSIC

3. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	7 yds.	IPSIC
4. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	3 yds.	IPSIC
50 Total Rounds					
Phase II: Evaluation					
1. (See note 1)	High Barricade	10 (5, 2 shot strings)	4 sec.	25 yds.	IPSIC
2. (See note 2)	Standing	16 (15, reload fire 1)	25 sec.	15 yds.	IPSIC
3. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	7 yds.	IPSIC
4. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	3 yds.	IPSIC
50 Total Rounds 100 Total Rounds for course					
Phase III: Qualification					
1. Each round striking the target counts as 1 hit. 2. Minimum passing score is 40 hits (80 percent), 45 hits (90 percent) for Emergency Response Team (ERT) personnel.					

Notes:

Note 1: Semiautomatic, shooter will start in the strong barricade position, (may use barricade for support) and ensure finger is off the trigger.

Note 2: Semiautomatic, shooter will start in position, finger off the trigger.

Note 3: Automatic, shooter will start in position, finger off the trigger.

Appendix F: NASA Serious Incident Report Format

TO: X/Assistant Administrator for Security and Program Protection

FROM: Center Chief of Security

SUBJECT: NASA Serious Incident Report

1. DATE/TIME OF INCIDENT:
2. CENTER:

a. Summary of Incident:
b. Responses to Incident:

1. Actions Completed:
2. Actions in Progress:
3. Actions Pending:

3. EMPLOYMENT OF RESOURCES:

a. Center Security Office:
b. Center Safety Office:
c. Local, State, and Federal Law Enforcement:

4. ACTIONS FOR ASSISTANT ADMINISTRATOR FOR SECURITY AND PROGRAM PROTECTION:
5. COMMENTS/RECOMMENDATIONS:

Center Security Officer

Appendix G: Security Area Signs

R E S T R I C T E D A R E A

BY THE ORDER OF
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Unauthorized persons who enter shall be subject to prosecution under 18 U.S.C. 799.

Procedures for Ordering Signs

Outdoor signs are metal, measuring approximately 40.64 cm/16 inches high and 50.8 cm/20 inches wide.

Indoor signs are of cardboard measuring approximately 22.86 cm/9 inches high and 12 inches wide.

Centers must order signs as needed through their normal supply source for NASA Forms.

Restricted Area Sign (Outdoors), NASA Form 1506
Restricted Area Sign (Indoors), NASA Form 1506A
Limited Area Sign (Outdoors), NASA Form 1507
Limited Area Sign (Indoors), NASA Form 1507A
Closed Area Sign (Outdoors), NASA Form 1508
Closed Area Sign (Indoors), NASA Form 1508A

Appendix H: Identifying and Nominating NASA Assets for the NASA Mission Essential Infrastructure Protection Program (MEIPP)

1. Introduction. Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection," directs that every Government agency establish a program to identify their critical infrastructure or key resources, prioritize and evaluate their critical infrastructure or key resources for vulnerabilities, and fund appropriate security enhancements necessary to mitigate identified vulnerabilities. NASA has elected to designate their critical infrastructure or key resources as "mission" essential vice "minimum" essential infrastructure (MEI) to better facilitate designation of vital, mission oriented critical infrastructure and key resource, operations, and equipment.

2. Purpose. To establish the roles and responsibilities of key Agency and Center personnel in the implementation and support of HSPD 7 and the Agency Critical Infrastructure Protection Plan (CIPP).

3. Critical Infrastructure Protection Plan (CIPP). The Agency CIPP implements the Agency critical infrastructure and key resources protection strategy. The CIPP shall be consulted whenever action impacting an MEI asset is being considered.

4. Criteria for Determining Agency Mission Essential Infrastructure (MEI). Agency MEI is defined as those essential facilities, missions, services, equipment, and interdependencies that enable the Agency to fulfill its national goals and Agency essential missions. For the purposes of the NASA MEI Protection Program, asset owners will use the following definitions when considering assets for inclusion:

a. A NASA infrastructure is to be considered critical, or a resource considered key, if its destruction or damage cause significant impact on the security of the nation - national economic security, national public health, safety, psychology, or any combination.

b. A NASA infrastructure or resource is to be considered mission critical if its damage or destruction would have a debilitating impact on the ability of NASA to perform its essential functions and activities.

c. Using paragraphs a & b above as guidance, NASA will use the following criteria to determine Agency critical infrastructure or key resource:

(1) Impact to National Security. Does the loss or compromise of the asset enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy critical missions in support of the National defense? Examples:

(a) Intelligence Functions
(b) Emergency Management Network
(c) Protection and Storage
(d) Nuclear Reactors Programs
(e) Defense and Transportation Programs

(2) Impact on Public Safety, Health, or Continuity of Government Services.

(a) Does the loss or compromise or the asset endanger or otherwise threaten the safety and health of

the general public? Refers to:

1. NASA facilities and systems that protect the general pubic from hazardous materials.

2. Situations that could be generated using materials owned by NASA to create safety and health hazards.

3. Utilities, communications, or other similar systems on which other Agencies depend to accomplish their essential missions serving the general public.

4. Weather prediction or other systems on which other Agencies depend to accomplish their essential missions serving the general public.

(3) Impact on Economic Security. Does the loss or compromise of the asset enable the hostile entity to disrupt or otherwise threaten NASA's ability to satisfy its critical mission in support of the economic well being of the Nation? Refers to:

(a) Assets operated or controlled by NASA, its contractors, or its agents that, if compromised or destroyed, would cause irreparable harm to the economic stability of the Nation.

(4) Impact on Essential NASA Missions that:

(a) Have very high public visibility in terms of the general public's perception of NASA as a symbol of national pride.

(b) Are integral to the performance of NASA's mission, have a very large dollar value, or are difficult or impossible to replace in a reasonable period of time.

(c) The loss or compromise of the asset would enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy its Essential Missions. Refers to:

1. Critical elements of the NASA Strategic Enterprises that are absolutely required for NASA's Essential Mission capability.

2. Critical Infrastructure Interdependencies (e.g., IT resources, data, electric power, water, oil and gas, environmental control components, transportation, security and safety, buildings or facilities, telecommunications, telephone system, local area networks, wide-area networks, etc.) that are dependent on or support NASA's MEI and whose loss could directly impact NASA's essential mission capability. These assets need not be identified as separate MEI but shall be integrated into the Center MEI asset protection scheme, evaluated for security risk vulnerability and protected accordingly.

(5) Impact on Human Life. Does the loss or compromise of the asset endanger or otherwise threaten the life, health, or safety of personnel engaged in the performance of NASA's missions?

5. Appointment of Agency and Center Critical Infrastructure Assurance Officer (CIAO). Per the CIPP, the NASA Administrator and Center Directors shall appoint, in writing, a senior member of their staff to perform the duties as the CIAO.

a. The Assistant Administrator for Security and Program Protection has been designated by the NASA Administrator as the NASA CIAO. The NASA CIAO, in coordination with Center CIAO's, shall coordinate and oversee all aspects of the Agency MEIPP.

b. The Agency Chief Information Officer (CIO) and Center CIO's, respectively, are responsible for coordinating and overseeing all aspects of the protection of Agency and individual Center cyber-infrastructure assets and interdependencies and will coordinate all critical and/or key cyber-infrastructure identification, prioritization, and protection requirements with the NASA CIAO.

Together, the NASA CIAO and CIO set the tone for the success of the Agency MEIPP.

6. Procedures for Nominating NASA Assets for Consideration for Inclusion Under the NASA MEIPP.

Procedures for identifying, nominating, and assessing initial Agency and Center MEI were established and implemented in 1999 to enable the Agency to meet National level mandates. Those procedures were implemented, and the Agency successfully identified and assessed all existing MEI and met all initial milestones.

7. Procedures for Adding/Deleting NASA Assets to the MEI Inventory. At a minimum, all proposed changes to the MEI list shall be coordinated by the Center with the responsible Headquarters Mission Directorate Associate Administrator, the Center's CIO, Center Chief of Security, and CIAO, as appropriate.

Using the criteria outlined in paragraph 4 above, personnel responsible for the Center and/or Agency asset deemed a candidate for inclusion or deletion under the MEIPP shall follow the below procedure to determine the appropriateness of the MEI designation or deletion.

a. For IT Assets:

(1) System owner, in coordination with the Center CIO, Chief of Security, IT System Security Manager, and the Center CIAO, shall propose IT System inclusion/deletion on the Agency MEI inventory to the Center Director.

(2) Upon final determination that the asset must be designated or deleted as an MEI, a written proposal shall be prepared for the Center Director's approval.

(3) Upon the Center Director's approval, the Center CIO shall forward the fully justified proposal to the NASA Deputy CIO for ITS with copies to the manager of the Principal Center of Information Technology Security (PCITS) and the Mission Associate Administrator CIO.

(4) The NASA Deputy CIO for ITS, in consultation with the Manager PCITS, Center ITS Manager, and Mission Directorate Associate Administrator CIO shall recommend acceptance or rejection of the proposal to the NASA CIO.

(5) Based on the recommendation of the NASA Deputy CIO for ITS, the NASA CIO shall coordinate with the NASA CIAO and either approve or reject the proposed change.

(6) Upon approval, the Center IT Security Manager and System IT Security Manager shall conduct an appropriate IT MEI system assessment using requirements established in NPR 2810.10.

(7) Appropriate mitigation plans shall be prepared and implemented to address all vulnerabilities, or if the proposal is disapproved, the NASA CIO shall coordinate with the affected Center CIO and Mission Directorate Associate Administrator to establish the appropriate appeals process, if warranted.

(8) Upon approval to delete an IT asset from the MEI list, the NASA CIO shall notify the requesting Center Director, Center CIO, and Center CIAO of the decision and submit appropriate information to the NASA CIAO so they shall update/distribute the MEI list, accordingly.

b. For physical assets:

(1) Facility owner, in coordination with the Center Chief of Security (CCS) and the Center CIAO, shall propose facility inclusion or deletion on the Agency MEI inventory to the Center Director.

(2) Upon final determination that the asset must be designated or deleted as an MEI, a written

proposal shall be prepared for the Center Director's approval.

(3) Upon Center Director's approval, the Center CCS shall forward the fully justified proposal to the NASA CIAO, with copies to the manager of the Mission Directorate Associate Administrator.

(4) The NASA CIAO, in consultation with the CCS and Mission Directorate Associate Administrator, shall recommend acceptance or rejection of the proposal to the NASA CIAO.

(5) The NASA CIAO shall either approve or reject the proposed change.

(6) If the proposal is approved, the NASA CIAO shall modify and distribute the updated NASA MEI list, and notify the requesting Center Director, Center Chief of Security, and Center CIAO of the decision.

(7) Upon approval of request for designation as an MEI, the CCS and Center CIAO, shall ensure the following is accomplished.

(a) Conduct of an appropriate physical security assessment.

(b) Prepare and implement appropriate mitigation plans to address all vulnerabilities.

(8) If the proposal is disapproved, the CIAO shall coordinate with the affected Center CIAO and Mission Directorate Associate Administrator to establish the appropriate appeals process, if warranted.

(9) Upon approval to delete a physical asset from the MEI list, the NASA CIAO shall notify the requesting Center Director, Center Chief of Security, Agency CIO, and Center CIAO of the decision and update and distribute the MEI list, accordingly.

Appendix I - NASA Photo-Identification Badge Standards

NASA PHOTO-ID STANDARDS	COLOR-FONT	POINT
1. LETTERING		
a. Badge No: ######	Black-Helvetica	6pt. Upper & lower case. Left Justified.
b. First/MI/Last Name	Black-Helvetica	12 pt. Upper & lower case. Lower left justified.
c. Center Numerical Designation	Black-Helvetica	18 pt. Lower left.
d. PO Box	Black-Helvetica	6 pt. Upper & lower case. Bottom centered.
2. NASA PHOTO-ID STANDARDFEATURES	**CHARACTERISTIC**	**SIZE**
a. Photograph	COLOR	(2.9cm x 3.9cm) 7 x 9 picas.
b. Card Stock	Standard	(5.5cm x 8.6cm) 13 x 20.3 picas.
c. Strap Slot (authorized for Center-specific photo-ID only.	Precut & Centered	(1.4cm x .3cm) 3.5 x 7 picas.
d. Logo	Silhouette of Space Shuttle	
e. Reliability Color for all Photo-ID	White	
3. COLOR CODING	**CARD COLOR**	
a. Civil Service	GOLD	

b. Consultant/Contractor	BLUE
c. Military/Other Agency (Detailee)	GREEN
d. Interns/CO-Ops, Summer Students	VIOLET
e. U.S. National Press	BROWN
f. Foreign National (Non-Designated/Press)	ORANGE
g. Foreign National (Designated)	RED
h. Jet Propulsion Laboratory	SILVER
4. CENTER	**CENTER ALPHA DESIGNATOR**
a. Ames Research	ARC
b. Dryden Flight Research Center	DFRC
c. Glenn Research Center	GRC
d. Goddard Space Flight Center	GSFC
e. NASA Headquarters	HQS
f. Jet Propulsion Laboratory	JPL
g. Johnson Space Center	JSC
h. Kennedy Space Center	KSC
i. Langley Research Center	LARC
j. Marshall Space Flight Center	MSFC
k. Stennis Space Center	SSC

PART 2.

Privacy Act Notice

General - Pursuant to Public Law 93-579, Privacy Act of 1974, as amended (5 U.S.C. 552a), the following information is being provided to persons who are asked to provide information in order to obtain a NASA Common Access Card (NCAC).

Authority - This information is collected under the authority of the National Aeronautics and Space Act (Section 304a), 42 U.S.C. 2455, and Executive Order 9397.

Purposes and Uses - The primary use of collecting the information requested by this form is to

facilitate the issuance of a NCAC. Social Security numbers are requested to keep NASA records accurate because other employees may have the same birth date. When collected, this information shall be maintained in NASA Privacy Act Systems of Records (10SECR). Generally, the information contained in this category of records is used within NASA for determining suitability for Federal employment and access to classified information (security clearances), as well as access to security areas, NASA Centers, and other matters connected with security programs and operations.

In addition to the internal uses of such information, it shall also be disclosed to Federal, State, local, or foreign agencies in connection with official business, including law enforcement, intelligence activities, determinations concerning access to classified information, and matters concerning immigration. Information connected with a law enforcement or administrative inquiry or investigation shall be disclosed to NASA contractors, subcontractors, or grantees. Disclosure shall also be made to the White House or Congressional offices in the course of certain inquiries. Additionally, in the event of a courts or formal administrative proceeding, information shall be disclosed in the course of presenting evidence or during pretrial discovery. NASA shall disclose information to the Department of Justice or other agencies in connection with such a proceeding.

Effect of Non-Disclosures - Providing this information is voluntary. However, if the form is not completed, a NCAC shall not be obtained. This shall result in various undesired actions such as disqualification for employment or access.

Appendix J: NASA Foreign National Visitor Security/Technology Control Plan Sample Template

SECURITY/TECHNOLOGY TRANSFER CONTROL PLAN (STTCP)
FOR

//Name of International Visitor//

PREPARED BY:

//Center IVC, Security Office and Sponsoring Organization//

//CENTER//
//ADDRESS//
//CITY, STATE, ZIP CODE//

//DATE SIGNED AND IMPLEMENTED//

Sponsor Signature	*Security Office Representative*
Foreign National Visitor	*Escort (If required)*

SECURITY/TECHNOLOGY CONTROL PLAN

I. INTRODUCTION

This Security/Technology Control Plan (STTCP) has been prepared by the International Visit Coordinator Office (IVC), the Center Security Office, and visit sponsor to ensure that //Type of Technology/// is protected in accordance with NASA policy and procedure, and in accordance with the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR).

The //Sponsoring Organization// is ultimately responsible for implementation and compliance with the policies set forth in the STTCP.

II. SCOPE

This STTCP covers technical data/know-how to be transferred to //Name of Individual// for tasks associated with //Type of Technology// at //Center// for the period beginning //Month, Day and Year// and ending //Month, Day and Year//. Appendix J(1) contains an overall description of the Program/Project, a description of the tasks to be performed by the Foreign National (FN), a description of technical data (including software), access to hardware (including computers), and know-how to be transferred to the FN in connection with tasks to be performed. Appendix J(2) contains security requirements. Appendix J(3) contains a general briefing on the export control regulations of the State and Commerce Departments and established security requirements for this STTCP.

III. TECHNOLOGY TRANSFER REQUIREMENTS

A. Training Requirements

The //Center// has developed the technology transfer control briefing (see Appendix J(3)) for those individuals on //Program/Project// who shall regularly have contact with //Name of Individual// on the Program/Project. The briefing contains an overview of export regulations. Appendix J(2) contains security and technology transfer requirements (e.g., IT security and interfaces, hours of access, facility access, movement restrictions) as they relate to the //Program/Project Name//. The Center IVC shall maintain a record of all personnel briefed.

B. U.S. Personnel Briefing

1. All U.S. //Center Name// personnel working with //Name of Individual// on the //Program/Project// shall read this plan and sign a Non-Disclosure Statement.

2. All //Program/Project// personnel signing the Non-Disclosure Statement do so by acknowledging that they understand what is required of them with respect to technology transfer and security issues regarding their work with //Name of Individual//. All questions regarding the transfer of technology falling outside the described scope contained in Appendix J(3) of this STTCP, or any questions with regard to what falls within the scope of this STTCP, shall be directed to the Center Export Administrator (CEA). All questions regarding Security Program aspects to include IT Security (Appendix J(2)) of this STTCP shall be directed to the International Visits Coordinator (IVC) or Security Office. In all cases, new personnel working with //Name of Individual// on a regular basis must sign a Non-Disclosure Statement before they enter the program/project.

C. Foreign Nationals Briefing

1. Any Foreign Nationals (FN) authorized by NASA to be assigned or to work for //Center Name// on the //Program/Project//shall be required to sign a Non-Disclosure Statement.

2. All authorized FN personnel working at //Center Name// on the //Program/Project Name// shall be provided a security/technology transfer control plan (STTCP). The STTCP shall include an oral and written briefing (see Appendix J(3) for written briefing), as well as a description of the task that specifically details the hardware, technology, know-how, data, drawings, software, and information which shall or shall not be exported (divulged) to //Name of Individual//.

IV. PHYSICAL SECURITY

All FN are required to appropriately display their issued NASA Photo-Id badge that identifies them as foreign persons (i.e., Orange Badge for Non-Designated Country Nationals and Red Badge for Designated Country Nationals) at all times while on NASA premises. Security requirements are spelled out in Appendix J(2).

Appendix J

(1) Project Description

In collaboration with the International Visits Coordinator, Security Office, and Center Export Administrator (CEA), Program/Project Managers shall provide a detailed description of the project the FN is to work on, the technology and information to which they are authorized access (transfer), the types of hardware, software and, data they need and have access to, and other pertinent information associated with the visit approval. Sample description is provided below:

Using this data as a constraint, the FN visitor shall, in collaboration with Drs. Jones and Miller, develop simple models of CMEs, which shall be compared to the observations. The known size and orientation of the flux rope at the surface shall be used as a starting point for the simple flux rope models. The model shall be propagated from the Sun and the resulting synthetic coronagraph images computed. The goal is to develop techniques and simple models for the interpretation of data from the STEREO mission. In order to perform these tasks, //Name of Individual// shall need access to technical information that is available in the open literature, a standard PC, and software programs such as IDL and Microsoft Office. These software programs fall under the jurisdiction of the Commerce Department and do not require a license to be exported to //Individuals Country//. //Name of Individual// shall also require access to published SOHO data. All of this work is the level of basic, scientific research, the results of which shall be published in open literature.

The work to be performed and the technical data, hardware and software to be accessed by //Name of Individual// is limited to the specific conditions and restrictions specified in this document. Without approval, //Name of Individual// is not authorized for any other work assignment, and is not authorized for access to any other technical data, hardware or software, or IT system. This STTCP is valid only for the //Program/Project// task specified.

Recordkeeping:

Each NASA employee who transfers controlled information under a license or license exemption must keep appropriate records of their transfers. The records must indicate the following: (1) the exporter (the person transferring the information), (2) date of transfer, (3) recipient, (4) description of the controlled information transferred, (5) title of the document, software program, computer file, etc., (6) method of transfer, and (7) export authorization. The records must be submitted to the IVC.

(2) Security

I. Responsibilities

A. NASA Personnel - All //Name of Center// personnel are responsible for being knowledgeable of all aspect of NASA and //Name of Center// security processes and procedures as they relate to the protection of information, assets, and resources that is entrusted to them as part of their NASA assignment. Specifically, //Name of Center// employees and contractors working on programs requiring access to classified, sensitive, or export controlled data or items, or employees working within controlled areas where classified, sensitive, or export controlled data or items exist or is discussed, must practice due diligence to ensure that the data or items are not exposed to access by any foreign person unless they are aware of a prior approval for that access. In addition, Security shall brief people on what this means during the STTCP briefing. All //Name of Center// personnel who shall have regular contact with the Foreign National addressed by this specific STTCP shall be briefed on and be knowledgeable of the specific restrictions stated in this STTCP.

B. Foreign National - Any Foreign National issued a NASA photo-ID for access to //Name of Center// must be knowledgeable of all aspects of //Name of Center // security processes related to issuing of photo-ID, access control, and internal security procedures. Specifically, the Foreign National must be aware of and comply with all imposed restrictions related to the physical access to the Center, facilities, and controlled areas and visual or audible access to information not approved as part of this STTCP agreement.

C. Foreign National's Host/Supervisor - The //Name of Center// employee who is hosting or supervising a Foreign National for photo-ID access to //Name of Center// must be aware of all security process at //Name of Center// that relate to the protection of information, assets, and

resources. Specifically, the host or supervisor of the Foreign National addressed by this specific STTCP shall be briefed on and be knowledgeable of the specific restrictions stated in this documents.

II. Identification

A. All personnel who access //Name of Center// for any purpose other than tours or open house are provided a NASA-photo-ID or visitors pass. This identification must be worn visibly above the waist at all times while accessing and on //Name of Center//. In addition, all personnel are responsible for challenging anyone who is not wearing a NASA photo-ID or //Name of Center// visitor pass, particularly in their work area.

B. Foreign Nationals who are employed by, reside at, or who frequent //Name of Center// on a regular, continuous, and long-term basis are provided an appropriate NASA photo-ID which allows unescorted business hours only access to //Name of Center//. The NASA photo-ID provided to Foreign Nationals shall be color-coded in accordance with the requirements established in Chapter 7, NPR 1620.1B, NASA Security Procedural Requirements.

C. The NASA photo-ID issued to a Foreign National signifies that the Foreign National has met all security reliability investigation requirements and has negotiated and implemented the appropriate STTCP. All rights and privileges associated with the implementation of the STTCP and issuance of a NASA photo-ID shall expire at the end of the visit approval or at the expiration of the Foreign National's Passport and Visa, whichever is shorter. It is the responsibility of the FN and their host/supervisor to complete the processes necessary to extend the photo-ID and STTCP beyond this date.

D. Upon departure from //Name of Center// for travel to any foreign destination, the FN is required to surrender the photo-ID to the Security Office. The photo-ID shall be returned to the FN upon return from the travel.

III. Controlled Areas

A. For the most part //Name of Center// is considered open and accessible to the general population that is authorized for unescorted access. There are areas which are designated "Security Areas" as part of //Name of Center// requirement to comply with Federal guidelines for the protection of classified information, NASA critical resources, sensitive data and materials, and safety requirements.

B. Unescorted access by Foreign Nationals to any Security Area established to protect classified information is prohibited.

C. Unescorted access by Foreign Nationals to areas where NASA critical resources or sensitive data and materials are protected must be agreed upon approved in writing by the cognizant //Name of Center// employee responsible for the area and Security Office.

D. Unescorted access by Foreign Nationals to the open and general work areas of //Name of Center// other than those the FN is assigned to work is prohibited.

IV. Reporting Requirements

A. All //Name of Center// personnel briefed on the information stated in this STTCP are required to report to the Security Office any deviation from the policies, guidelines, or procedures stated within.

B. In addition, all //Name of Center// personnel are required to report any suspicious or unusual behavior or activity by a FN at //Name of Center//.

(3) Briefing on Export Administration Regulations (EAR) - International Traffic in Arms Regulations (ITAR)

I. Export Administration Regulations (EAR) [15 CFR 730-7741]

The Export Administration Regulations (EAR) are administered by the Commerce Department under the authority granted by the Export Administration Act of 1979 as amended.

Controlled Commodities

Information not controlled under the ITAR shall be controlled by the Commerce Department. The counterpart to the United States Munitions List of the State Department's ITAAR is the Commerce Control List (CCL) of the Commerce Department's EAR.

Foreign National

The definition of a Foreign National is the same as the definition under the ITAR. It is a person who does not have permanent resident status or is not a protected individual (has not been granted political asylum or has not been granted refugee status.

Technical Data

Specific information necessary for the "development," "production," or "use," of an item specified within the Commodity Control List (CCL).

Publicly Available

Information which has been made available to the public or to a community of persons free or at no more than the cost of reproduction and distribution. This includes information that has been published or place in libraries. It also includes fundamental research in basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly with the scientific community.

Export

An export is a release of commodity, technology, or software to a Foreign National in this country or abroad. An export to a Foreign National in this country is deemed an export to the home country of the Foreign National.

Examples of Commodities Controlled by the CCL

The following is an example directly from the Commerce Department regulations. You shall notice that while the State Department specifies general items that are controlled (e.g., remote sensing satellites), the Commerce Department specifies controlled thresholds for each commodity:

3A001 - Electronic Components - is the general heading under the Export Classification Number (ECCN).

a. 2 EEPROMs, flash memories and SRAMS having any of the following:

- Rated for operation at an ambient temperature above 398K (125 degrees C);
- Rated for operation at an ambient temperature below 218K (-55 degrees C); or
- Rated for operation over the entire ambient temperature range from 218K (-55 degrees C) to 398K (125 degrees C).

If the item in question is controlled because it exceeds the specified thresholds above, the exporter must then determine whether the item is controlled to the specific country of destination. In addition, one or more different exemptions shall be available.

This is just one example from the approximate four hundred pages of commodities and specifications listed under the Commodity Control List (CCL). Each commodity then lists specific controls for those specifications which would apply to certain countries for certain policy reasons (e.g., antiterrorism, missile technology, national security, regional stability, etc.). Since publication outside NASA would involve all countries, the lowest thresholds would apply. To publish all the parameters would virtually require a republication of the regulations. What follows is an illustrative list, not an exhaustive list, of general commodities, which, depending in the specifications, could be sensitive.

1. Electronics - design, development, and production

a. Integrated circuits
b. Monolithic circuits
c. Hybrid integrated circuits
d. Multichip integrated circuits
e. Film type integrated circuits
f. Optical integrated circuits
g. Field programmable gate arrays
h. Microwave or millimeter wave devices
i. Superconductive electromagnetic amplifiers
j. Space qualified and rad hardened photovoltaic arrays
k. Space qualified magnetic tape recorders
l. Signal analyzers exceeding 31 GHz
m. Spectrometers
n. Vacuum microelectronic devices
o. Hetero-structure semiconductor technology
p. Superconductive devices or circuits

2. Computers

a. High speed digital computers
b. Electronic computers operating at temperature extremes (below -45 deg. C or above 85 deg. C)
c. Equipment designed for image enhancement
d. Specially designed computers for signal processing

3. Information Security

a. Systems, equipment, and software designed or modified to use cryptography.

4. Sensors

a. Certain "space-qualified" focal plan arrays
b. Multispectral imaging sensors
c. Image intensifier tubes
d. Deformable mirrors
e. Lasers
f. "Space-qualified" laser radar and LIDAR equipment
g. Magnetometers

5. Materials

a. Composite structures or laminates
b. Ceramic matrix composite materials
c. Piezoelectric polymers and thin films

Penalties for Failure to Adhere to the EAR

There are both substantial criminal and civil penalties for violations of the EAR. A criminal conviction could lead to fines of up to $1M and 10 years imprisonment. In addition, one could incur civil penalties of up to $100,000. Also, NASA could lose its export privileges.

II. International Traffic in Arms Regulations (ITAR [22 CFR 120 - 130])

Section 38 of the Arms Export Control Act (22 USC 2778) authorizes the President of the United States to control the export and import of defense articles. The Presidential authority to promulgate regulations with respect to the export and import of defense articles was delegated to the Secretary of State by Executive Order 11958. The ITAR implements this delegated authority.

Defense Article

A defense article is any commodity listed on the United States Munitions list (USML) of the ITAR (Section 121.1). Defense articles on this list include all spacecraft including communication satellites, remote-sensing satellites, scientific satellites, research satellites, navigation satellites, experimental and multi-mission satellites as well as ground control stations for those satellites (the DSN). In addition, the list includes all components, parts, accessories, attachments, and associated equipment specifically designed or modified for those remote sensing satellites or the DSN.

Export

Sending or taking a defense article out of the U.S.; or transferring control of a defense article to a Foreign National whether in the U.S. or abroad; or disclosing technical data to a Foreign National whether in the U.S. or abroad.

Foreign National

A Foreign National is anyone who is not a permanent resident or anyone who has not been granted refugee status, or anyone who has not been granted political asylum.

Technical Data

Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes all classified information. Tech data also includes drawings, blueprints, photographs, instructions, and documentation.

Software

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis, and repair of a defense article. In addition, software employing cryptographic techniques shall require a license.

Publicly Available

Information which is published and which is generally available to the public. This includes general scientific, mathematical, and engineering principles taught in schools and colleges. It also includes

general marketing information on function, purpose, or general system descriptions of defense articles. Additionally, fundamental research in science and engineering, which is ordinarily published and widely disseminated, is also considered to be publicly available.

NASA Exemptions

In addition to general exemptions available to any "exporter," such as publicly available information, there are specific exemptions available to NASA. If there is a signed NASA international agreement with a foreign Governmental body and a NASA Task Order which allows NASA to transfer date to a foreign partner, then such things as operational, repair, assembly, modification, maintenance or test technical data would typically be allowed if the information is properly marked in accordance with the international agreement.

Additionally, controlled "interface" information, even including some design details, could also be sent where there is an international agreement. Interface information means that NASA can exchange design information, with "non-proscribed" countries, as long as the design details are limited to the interface and do not describe sufficient design information to enable the production of the entire component. In addition, the information transferred must be marked in accordance with the international agreement to indicate that the information is being transferred under an exemption (125.4 (b) (3)), is for use exclusively on a particular project and that is not for re-export without the permission of NASA or the State Department.

Additional Examples of Unclassified Defense Articles on the Munitions List

1. Energy conservation devices for producing electrical energy from solar energy or chemical reaction and designed for military use.
2. Infrared focal plane array detectors specifically designed for military use.
3. Infrared, visible, and ultraviolet devices specifically designed for military use.
4. Radar systems specifically designed for military use with capabilities such as:

a. Search
b. Acquisition
c. Tracking
d. Imaging radar systems

5. Command, control and communications systems designed for military use.
6. Computers specifically designed or developed for military use.
7. Inertial platforms and sensors for weapons.
8. Guidance control and stabilization systems.
9. Astro-compasses and star trackers.
10. Accelerometers and gyros designed for military use.
11. Information security systems utilizing cryptographic systems.
12. Photointerpretation, stereoscopic plotting, and photogrammetry specifically designed for
13. military purposes.
14. Solid state devices specifically designed or modified for military use.
15. GPS receivers that employ any of the following:

a. encryption or decryption capabilities (e.g., Y-Code) of PPS signals;
b. produce navigation results above 60,000 feet and 1,000 knots velocity or greater;
c. are designed or modified for use with a null steering antenna designed to reduce or avoid jamming signals or designed or modified for use with unmanned air vehicle systems capable of delivering at least 500 kg payload to a range of at least 300 km. (if less capability but designed for military then captured here).

15. Submersible vessels, manned and unmanned, tethered or untethered, designed or modified for military use.
16. Space launch vehicles and their components, parts, accessories, attachments, and associated equipment. (NO NASA EXEMPTION FOR LAUNCH VEHICLE INTERFACE DATA).
17. Heat shields and components thereof fabricated of ceramic or ablative materials.
18. On-board navigation software which corrects the trajectory and achieves system accuracy of 3.33 percent or less of the range.
19. Structural materials for space launch vehicles such as composite structure, laminates, ceramic, and composite materials.
20. Launch vehicle attitude control equipment.
21. Design technology for shielding or rad hardening of spacecraft electrical circuits and subsystems.

Penalties for Failure to Adhere to the ITAR

There are both substantial criminal and civil penalties for violations of the ITAR. A criminal conviction could lead to fines of up to $1M and 10 years imprisonment for each violation. In addition, one could incur civil penalties of up to $100,000. Also, NASA could lose its privilege to export goods and services.

Appendix K: NASA Security Statistics Format

Center Law Enforcement and Security Statistics - Qtr #/CY##

LAW ENFORCEMENT ACTIVITY

1. **Crimes Against Persons: NASA C/S Other**

a. Murder
b. Rape
c. Attempted Murder
d. Assault
e. Armed Robbery

2. **Crimes Against Property (Government and Private) (include $ value of loss, nomenclature, report number, date):**

a. Theft
b. Burglary
c. Vandalism

3. **Recovered Stolen Property: $ amount**
4. **Illegal Drugs:**
5. **Other Categories:**

A. Bomb Threats:
B. DUI/DWI:
C. Traffic Management Program

a. Speeding Tickets issued:
b. Parking Tickets issued:
c. # Drivers barred:

SECURITY PROGRAM

1. Visitor Escort Policy and Procedure Violations:
2. Number of Classified Contracts (DD Fm 254):
3. Security Incidents:

a. Compromise of CNSI:
b. Unauthorized Access to Security Area:
c. Suspension of Security Clearance:
d. Denial/Revocation of Security Clearance:
e. Debarment Actions:
f. Other (suspicious activity; etc.):

Appendix L: NASA Threatcon Actions

1.1. THREAT CONDITION (THREATCON) GREEN Minimum Actions:

1.1.1. Definition: Low risk of terrorist activity.

1.1.2. Threat condition GREEN employs everyday, routine security measures determined by the CCS and endorsed by the Center Director as being appropriate for the optimum protection of NASA assets at that Center.

1.1.3. The program shall include antiterrorism measures such as ID checks for entry, enforcing NASA policy on the wearing and display of the NASA photo-ID badge, random vehicle inspections, consistent and current mandatory security training, exercising emergency response capability; to include response to increase in threat condition, periodic security assessments of individual Centers and facilities to ensure all reasonable measures are taken to mitigate vulnerabilities.

1.2. THREATCON BLUE Minimum Required Actions:

1.2.1. Definition: General Risk of Terrorist activity.

1.2.2. Advise continuously all employees of the condition, through training, briefings, and other mediums;

1.2.3. Increase general security awareness, through training, briefings, and other mediums;

1.2.4. Secure buildings, rooms, and storage areas not in regular use;

1.2.5. Increase security inspections of packages;

1.2.6. Check all deliveries at mailrooms and shipping and receiving departments;

1.2.7. Periodically test emergency communications capability with command locations;

1.2.8. Review and update emergency response plans, as appropriate;

1.2.9. Keep Center personnel updated, as appropriate.

1.3. THREATCON YELLOW Minimum Required Actions:

1.3.1. Definition: Significant risk of terrorist activity.

1.3.2. Continue all THREATCON BLUE measures;

1.3.3. Conduct random vehicle and package inspections;

1.3.4. Monitor visitors, as appropriate;

1.3.5. Curtail special events and visitors, as appropriate;

1.3.6. Increase surveillance of critical locations;

1.3.7. Coordinate with local law enforcement and emergency response agencies, as required;

1.3.8. Assess the threat characteristics for further refinement of established/planned protective measures;

1.3.9. Review and implement as necessary contingency, COOP, and emergency response plans.

1.4 THREATCON ORANGE Required Actions:

1.4.1. Definition: High risk of terrorist activity.

1.4.2. Continue all THREATCON YELLOW measures;

1.4.3. Inspect all incoming packages at a centralized receiving point;

1.4.4. Admit only essential visitors under escort;

1.4.5. Establish random Center checkpoints;

1.4.6. Cancel special events, as appropriate;

1.4.7. Limit number of entry and exit points;

1.4.8. Perform a consent search on all entering vehicles and conduct random searches of exiting vehicles;

1.4.9. If necessary, cancel vacations for security personnel;

1.4.10. Establish additional 24-hour patrols as necessary;

1.4.11. Coordinate with local law enforcement agencies as appropriate.

1.5. THREATCON RED Required Actions:

1.5.1. Definition. Severe risk of terrorist activity.

1.5.2. Continue all THREATCON ORANGE measures;

1.5.3. Close the Center to all visitors;

1.5.4. Limit entry and exit to a single point;

1.5.5. Augment security forces as necessary to ensure adequate response capability;

1.5.6. Minimize all administrative journeys and visits;

1.5.7. Frequently check the exterior of buildings and parking areas for suspicious items and activity.

Appendix M: Designation of Public Trust Positions and Investigation Requirements

A. Public Trust Designation Model

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

Through this Appendix and Chapters 2, 3, and 4 of this NPR, NASA has established a consistent and uniform method for determining the risk level of civil service positions and functions and for those positions occupied by NASA contractor personnel. Because contractors play such a major role in all areas of Agency operations, their reliability and suitability are of equal importance. This Appendix meets the requirements established by the Office of Personnel Management (OPM) for federal employment and provides the appropriate mechanism for position risk designation for NASA contracts and contractor personnel.

Position Designation Records. Each NASA Center shall complete and maintain the Position Designation Record or its equivalent for each Agency civil service position and will also maintain similar records for NASA contractor personnel.

- Center personnel offices shall maintain the record of Public Trust suitability designations for all NASA civil service employees. These Position Designation Records are subject to review by OPM during periodic appraisals of NASA suitability programs, or on a case-by-case basis, to assure that NASA is considering all pertinent factors when designating positions relative to the integrity and efficiency of the service.
- Center security offices shall maintain copies of civil service designations and shall establish and maintain records for all contractor personnel, as well. These records will be subject to review during security program audits and reviews.

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

- ***Program Designation.*** The Agency identifies both the impact and scope of an Agency program as related to the integrity and efficiency of the service. This determines the "program designation."
- ***Position Risk Designation Points.*** The Agency determines the degree of risk that a position poses to the Agency or an Agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total "position risk designation points" for a position.
- ***Position Designation.*** The Program Designation and Position Risk Designation Points are applied to determine the risk level "position designation."

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

National Aeronautics and Space Administration

POSITION DESIGNATION RECORD

AGENCY: _____ PROGRAM: _____

POSITION TITLE, SERIES & GRADE: _____

POSITION DESCRIPTION #: _____

RISK DESIGNATION SYSTEM

I. PROGRAM DESIGNATION

IMPACT, Integrity & Efficiency of Service.....

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

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

II. POSITION RISK DESIGNATION POINTS

RISK FACTORS & POINTS:

DEGREE OF PUBLIC TRUST.....

FIDUCIARY RESPONSIBILITIES.....

IMPORTANCE TO PROGRAM.....

PROGRAM AUTHORITY LEVEL.....

SUPERVISION RECEIVED.....

TOTAL POINTS.....

III. POSITION DESIGNATION

UNADJUSTED **RISK LEVEL**.....

MINIMUM **INVESTIGATION**.....

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

ADJUSTMENTS FOR UNIQUENESS AND UNIFORMITY? COMMENTS:

National Security Position (Y or N): _____

If Yes, Type of Access Required (S/TS/SCI): _____

FINAL DESIGNATION (Risk level/Sensitivity level/Access level).....

MINIMUM INVESTIGATION.....

PRINTED NAME & SIGNATURE OF PROGRAM POSITION DESIGNATOR: _____

DATE: _____

NASA FORM 1722 JUN 04

Figure 1

FILLING OUT THE POSITION DESIGNATION RECORD

Program Designation

? Program Designation. The appropriate management official identifies both the impact and scope of a program as related to the integrity and efficiency of the service. This determines the "program designation."

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

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

decision must be based on the best interests of the mission.

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

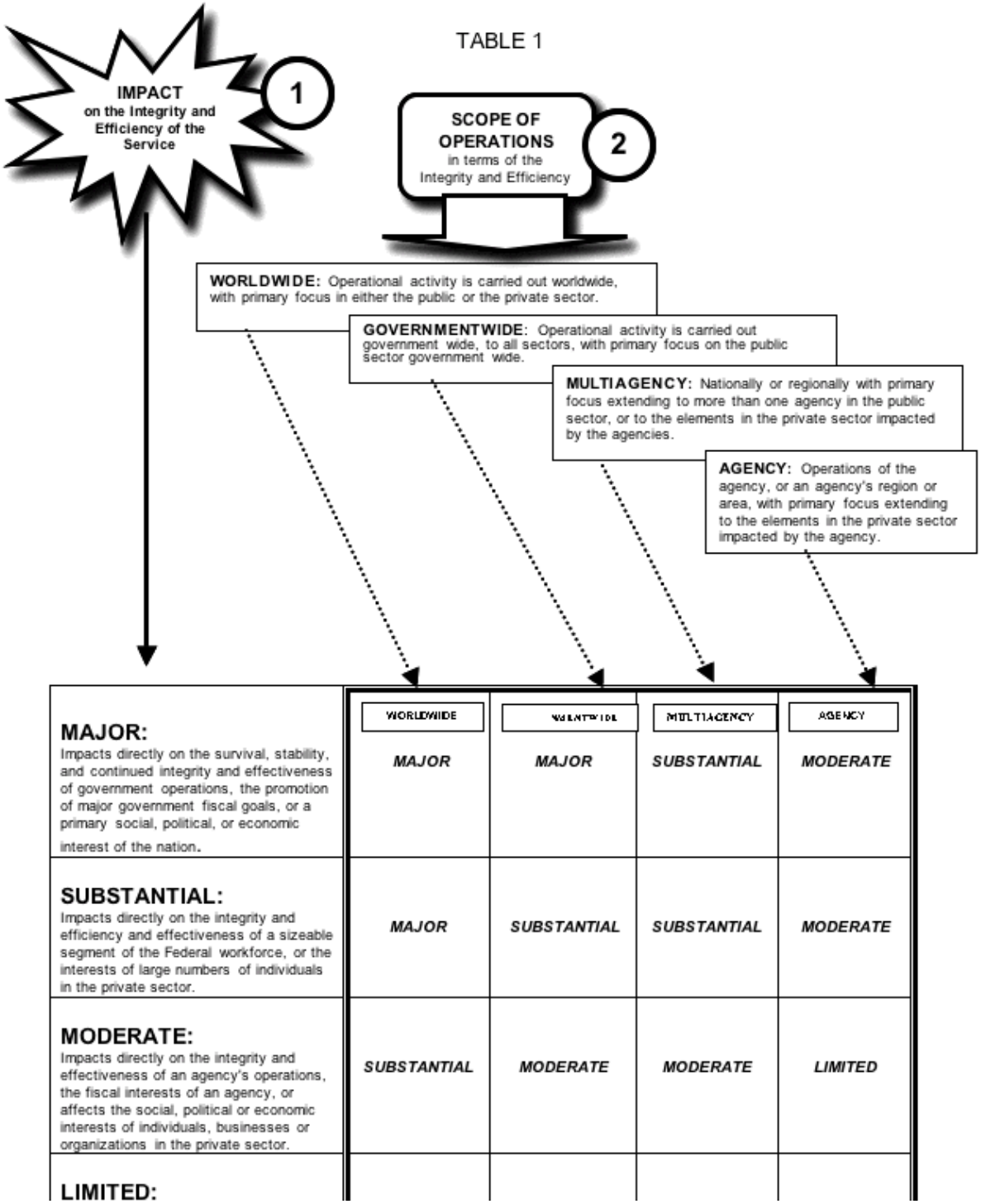
3) Determining Program Designation: The box at the intersection of the IMPACT row and SCOPE column identifies the program designation.

Examples:

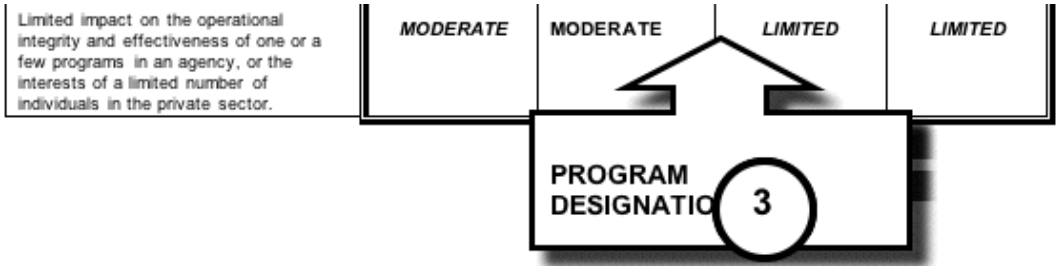
(1) SUBSTANTIAL IMPACT and (2) MULTIAGENCY SCOPE = (3) SUBSTANTIAL Program Designation.

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

TABLE 1



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



Designating Position Risk Points

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

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

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

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

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

Example:

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

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

TABLE 2

1

RISK FACTOR DESCRIPTIONS

DEGREE OF PUBLIC TRUST: The consensus of confident expectation for honesty, integrity, reliability, responsibility, or justice placed in a position.

FIDUCIARY (MONETARY) RESPONSIBILITY: Authority or ability to obligate, control or expend public money or items of monetary (bonds, etc.) value.

IMPORTANCE TO PROGRAM: Impact individual position has, due to status in, or influence, direct or indirect, on program as a whole, either individually or collectively.

PROGRAM AUTHORITY: Ability to manipulate authority or control the outcome or results of all or key portions of a program or policy.

SUPERVISION RECEIVED: Frequency work is reviewed and nature of the review.

DEGREE OF RISK

						Degree of supervision:
MAJOR: Potential for independently compromising integrity or effectiveness of a major program element or component, or in conjunction with others, damaging all phases of program operations.	7 6	7 6	7 6	7 6	7 6	**Limited:** Occasional review only with respect to major policy issues by superior without expertise in the technical aspects of program policy and operations.
SUBSTANTIAL: Potential for reducing integrity or efficiency of overall program operations, or overall operations of major program elements/components independently, or through collective action with others.	5 4	5 4	5 4	5 4	5 4	**Periodic:** Ongoing spot review of policy and major operational considerations of work by superior, with some knowledge of program operations, but with minimal technical program expertise.
MODERATE: Potential for reducing integrity or efficiency of overall or day-to-day operations of a major program element or component, through independent action or collectively with others.	3 2	3 2	3 2	3 2	3 2	**Moderate Technical:** Ongoing spot review of work in connection with important operational issues by superior with technical program expertise.
LIMITED: Potential for damage not meeting above criteria.	1	1	1	1	1	**Close Technical:** Continuing review of all phases of work by supervisor with technical program expertise.

POSITION RISK DESIGNATION POINTS

2

3

TOTAL POINTS:

Position Designation

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

At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation shall

result in a higher risk level, the other steps may not be needed.

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

TABLE 3

TABLE 3

I. PROGRAM DESIGNATION

II. POSITION RISK POINTS

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

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

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

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

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

Adjustments: Some positions, by the very nature of the duties and responsibilities of the program or the position, may require designation at a certain level of risk. Final adjustment in the designation process must take into account unique factors specific to positions and the organizational need for uniformity of operations. Adjustments serve to raise the risk level designation of a position or convert the designation from a risk level to a sensitivity level. As a consequence, the level of investigation is often raised.

Uniqueness. Some factors that can cause a uniqueness adjustment, that are unique and are not fully accounted for in the program or position designation system, are listed here:

- Special investigative or criminal justice duties.
- Positions requiring possession and use of a firearm.
- Significant public health duties.
- Significant public safety duties.
- Access to or control of highly sensitive but unclassified information.
- Access to sensitive financial records.
- Potential for realizing significant personal gain.
- Control of an automated monetary system (such as key access entry).

- Few-of-a-kind positions with special duties (such as Special Assistant to Agency Head).
- Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans but involving regular contact with, and ongoing knowledge of, all or most of such material (such as Budget Analyst, Special Assistant).
- Any of the criteria appearing in 5 CFR 732 or E.O. 12968.
- Computer-ADP; any of the criteria under OMB Circular A-130 or Federal Information Security Act (FISMA) of 2002.
- Any other factors the Agency thinks relevant (these must be documented).

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

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

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

RISK LEVELS	SENSITIVITY LEVELS	ACCESS LEVELS
High Risk	Special-Sensitive	Sensitive Compartmented Information (SCI)
Moderate Risk	Critical-Sensitive	Top Secret (TS)
Low Risk	Noncritical-Sensitive	Secret (S)
	Nonsensitive	Confidential (C)

See adjustment examples on the next page.

I. PROGRAM DESIGNATION	II. POSITION RISK DESIGNATION POINTS	III. POSITION DESIGNATION	MINIMUM INVESTIGATION	ADJUSTMENTS Uniqueness, Uniformity	FINAL DESIGNATION	REQUIRED INVESTIGATION
MODERATE	20	MR	MBI	Criminal Justice Duties	HR	BI
SUBSTANTIAL	29	MR	LBI	None	MR	LBI
MAJOR	25	HR	BI	TS Access (E.O. 12968)	CS	SSBI
MODERATE	30	MR	LBI	Special Assistant to Agency Head	HR	BI
MAJOR	25	HR	BI	5 CFR 732 (No Access)	CS	BI

B. COMPUTER/ADP POSITION RISK LEVELS

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

COMPUTER/ADP RISK LEVELS

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

Risk Levels.

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

- Responsibility for the development, direction, implementation, and administration of Agency computer security programs, including direction and control of risk analysis or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for preparing or approving data for input into a system which does not necessarily involve personal access to the system, but which creates a high risk for effecting grave damage or realizing significant personal gain.
- Assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to insure the integrity of the system.
- Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of systems hardware and software.
- Access to a system during the operation or maintenance in such a way to permit high risk for causing grave damage or realizing a significant personal gain.
- Other positions as designated by the NASA Administrator that involve high risk for effecting grave damage or realizing significant personal gain.

Moderate Risk: Includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the High Risk level to insure the integrity of the system. Such positions may involve responsibility for systems design, operation, testing, maintenance, or monitoring that is carried out under technical review of higher authority at the High Risk level, to insure the integrity of the system. This level includes, but is not limited to:

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

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

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

C. NATIONAL SECURITY POSITION SENSITIVITY LEVELS

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

SPECIAL-SENSITIVE
(SS)

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

CRITICAL-SENSITIVE
(CS)

Potential for exceptional or grave damage to the national security.

Positions that involve any of the following:

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

NONCRITICAL-SENSITIVE
(NCS)

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

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

NOTE: The designation of Non-Sensitive is not shown in the table because a Non-Sensitive position is the same as a Low Risk position; both require the same level of investigation, a NACI.

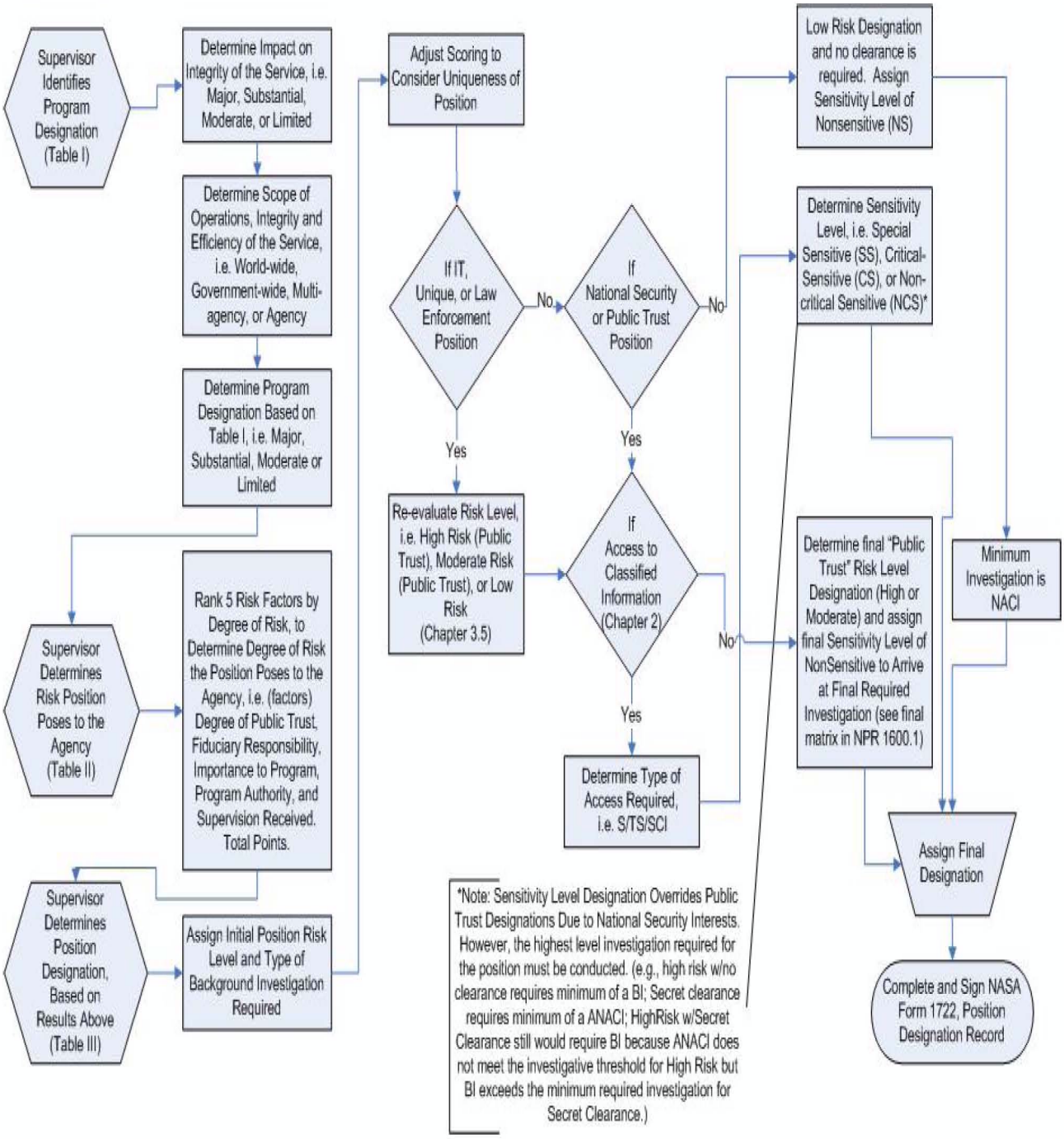
Apply the sensitivity levels described in this part as an Adjustment in the Risk Designation System to arrive at a final designation. This Appendix references 5 CFR 732 as one of the uniqueness adjustment factors. The reference pertains to Subpart B of the section on "Sensitivity level designations and investigative requirements." The table on the previous page shows the sensitivity level designations, as well as their definitions and examples of the types of duties and responsibilities that correspond to the Critical-Sensitive and Noncritical-Sensitive levels. Centers shall consider the information displayed in this table when deciding if a position must have a sensitivity designation.

Sensitivity level designations override Public Trust (i.e., HR and MR) designations due to the national interest or security. However, the basic risk level of a position needs to be determined first. If National security duties and responsibilities are no longer a part of a position, the position then reverts to its Public Trust designation. Additionally, if the Public Trust risk level designation requires a higher level of investigation than the National security sensitivity level, the higher level of investigation must be conducted. For example, if the basic position designation is HR, but the position requires Secret access, the position would have an adjusted designation of Noncritical-Sensitive because of the Secret access. The investigation required would be a BI for the HR position, and not an ANACI for the Noncritical-Sensitive designation due to Secret access. The higher level of investigation prevails because of the more intensive screening required of an HR position, a BI investigation being a higher level of investigation than an ANACI.

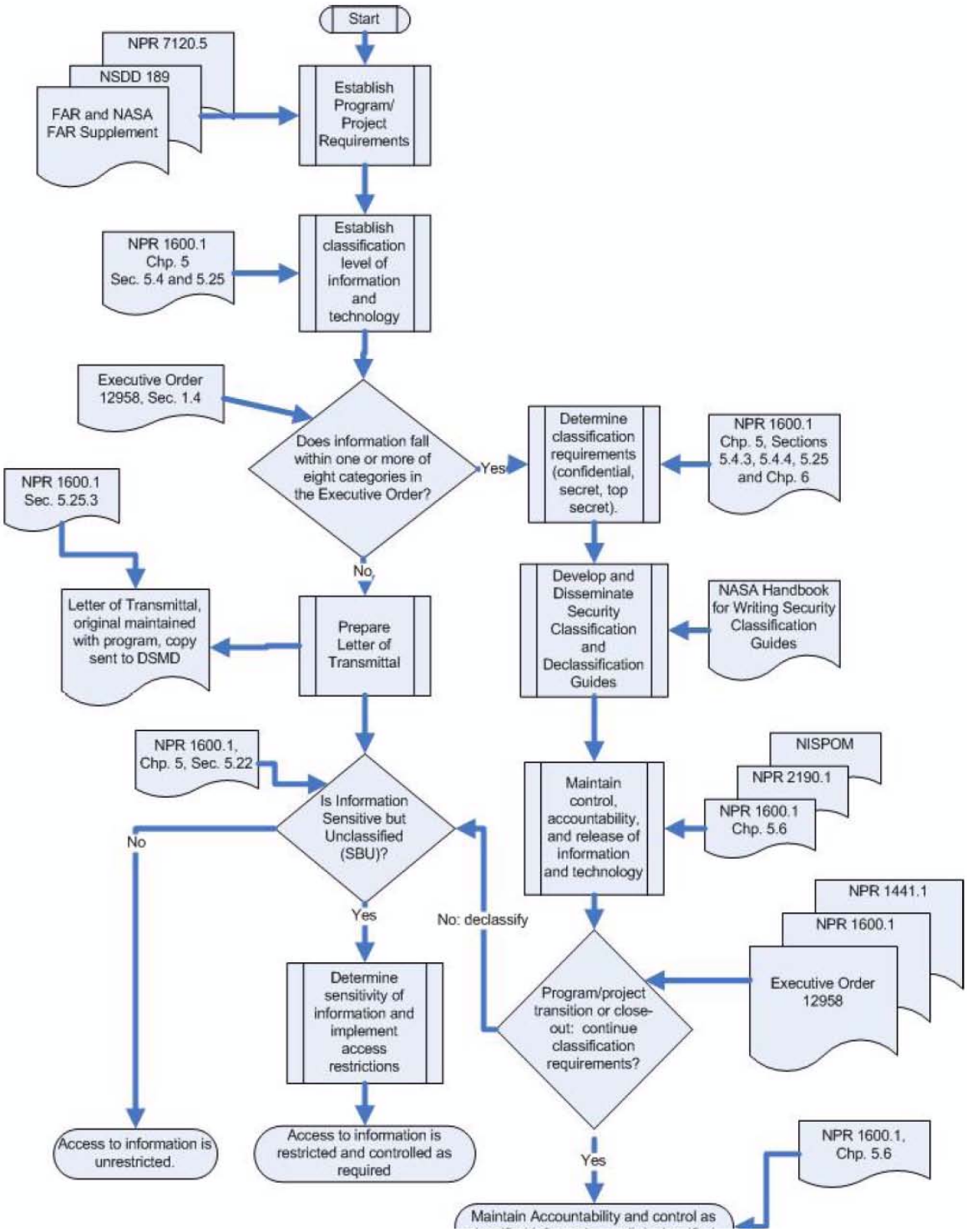
5 EXAMPLES:

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

APPENDIX N: Process Flow Chart for Determining Position Risk and Sensitivity Levels



APPENDIX O: Process Flow Chart for Mandatory Determination for Classification and/or Sensitivity Level of Program/Project Information and Technology



classified information until declassified.