á	á
(1) Pending or current TSCM operation.	Secret
á	á
(2) Completed TSCM operation.	Confidential
á	á
(3) A request for TSCM service.	Secret
á	á
(4) Major security vulnerabilities of an area.	Secret
á	á
(5) Minor vulnerabilities.	Confidential
á	á
(6) The discovery of a device.	Secret
á	á
(7) Facility/program threat assessments as part of TSCM service.	Secret
á	á
(8) Penetration techniques.	Up to Secret
á	á
(9) TSCM equipment capabilities/limitations; budget or procurement actions; and/or policies and procedures	Up to Secret
á	á
(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 wi , th 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 REC

If the requirement is for	And the person has this access	Based on this investigation	Ther investi requi
CONFIDENTIAL	None	none	NA(
SECRET; "L"	CONF, SLc; "L"	out of date NACLC or SSBI	
TOP SECRET,SCI; "Q"	None	none	SS
	None; CONF, SEC; "L"	current or out of date NACLC	
	TS, SCI; "Q"	out of date SSBI	SSB

TABLE 2: REINVESTIGATION REQUIREM

If the requirement is for	And the age of the investigation is	Type required if t has been a break service of ___
CONFIDENTIAL	0 to 14 yrs. 11 mos.	0-23 months
	15 yrs. or more	None (NOTE 1

Appendix B: SPB Issuance 2-97 - Adjudicative Guidelines

**Adjudicative Guidelines
for Determining Eligibility
for Access to
Classified Information**

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. These guidelines 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.
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 eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative 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, must be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator must 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 voluntariness of participation.
5. The presence or absence of rehabilitation and other pertinent behavioral changes.
6. The motivation for the conduct.
7. The potential for pressure, coercion, exploitation, or duress.
8. 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 as to whether access to classified information is clearly consistent with national security shall be resolved in favor of the national security.

c. 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 determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

GUIDELINE A: Allegiance to the United States.
GUIDELINE B: Foreign influence.
GUIDELINE C: Foreign preference.
GUIDELINE D: Sexual behavior.
GUIDELINE E: Personal conduct.
GUIDELINE F: Financial considerations.
GUIDELINE G: Alcohol consumption.
GUIDELINE H: Drug involvement.
GUIDELINE I: Emotional, mental, and personality disorders.
GUIDELINE J: Criminal conduct.
GUIDELINE K: Security violations.
GUIDELINE L: Outside activities.

GUIDELINE M: Misuse of Information Technology Systems.

d. Although adverse information concerning a single criterion shall not be sufficient for an unfavorable determination, the individual shall 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 shall 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 must consider the following about the person:

1. Voluntarily reported the information.
2. Was truthful and complete in responding to questions.
3. Sought assistance and followed professional direction, where appropriate.
4. Resolved or appears likely to favorably resolve the security concern.
5. Has demonstrated positive changes in behavior and employment.
6. Must 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 shall be appropriate to recommend approval with a warning that future incidents of a similar nature shall 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 shall be disqualifying include the following:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of Government by unconstitutional means.
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 the overthrow of the United States Government, or any State or subdivision, by force or violence or by other unconstitutional means.
d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to 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 the following:

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 person has had no recent involvement or association with such activities.

GUIDELINE B
Foreign Influence

6. The Concern. A security risk shall exist when an individual's immediate family, including cohabitants and other persons to whom he or she shall be bound by affection, influence, or obligation are not citizens of the United States or shall be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.
7. Conditions that could raise a security concern and shall be disqualifying include the following:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country.
b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse

foreign influence or duress exists.
c. Relatives, cohabitants, or associates who are connected with any foreign Government.
d. Failing to report, where required, associations with Foreign Nationals.
e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service.
f. Conduct which shall make the individual vulnerable to coercion, exploitation, or pressure by a foreign Government.
g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure.
h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

8. Conditions that could mitigate security concerns include the following:

a. A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States.
b. Contacts with foreign citizens are the result of official United States Government business;
c. Contact and correspondence with foreign citizens are casual and infrequent.
d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country.
e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

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 shall 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 shall be disqualifying include the following:

a. The exercise of dual citizenship.
b. Possession and/or use of a foreign passport.
c. Military service or a willingness to bear arms for a foreign country.
d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country.
e. Residence in a foreign country to meet citizenship requirements.
f. Using foreign citizenship to protect financial or business interests in another country.
g. Seeking or holding political office in the foreign country.
h. Voting in foreign elections.
i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another Government in preference to the interests of the United States.

11. Conditions that could mitigate security concerns include the following:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country.
b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship.
c. Activity is sanctioned by the United States.
d. Individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D
Sexual Behavior

12. The Concern. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, shall subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. Sexual orientation or preference shall not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance. (NOTE: The adjudicator must also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders.)
13. Conditions that could raise a security concern and shall be disqualifying include the following:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted.
b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is 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 which reflects lack of discretion or judgment.

14. Conditions that could mitigate security concerns include the following:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature.
b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature.
c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability.
d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

GUIDELINE E
Personal Conduct

15. The Concern. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person might not properly safeguard classified information. The following shall normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility (NOTE: (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.):

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing.
b. Refusal to complete required security forms, releases, or 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 shall be disqualifying also include the following:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances.
b. The deliberate omission, concealment, or falsification of relevant and material 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.
c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination.
d. Personal conduct or concealment of information that shall increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, shall affect the person's personal, professional, or community standing or render the person susceptible to blackmail.
e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency.
f. Association with persons involved in criminal activity.

17. Conditions that could mitigate security concerns include the following:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability.
b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily.
c. The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts.
d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided.
e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress.
f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information.

g. Association with persons involved in criminal activities has ceased.

GUIDELINE F
Financial Considerations

19. The Concern. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.
20. Conditions that could raise a security concern and shall be disqualifying include the following:

a. A history of not meeting financial obligations.
b. 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.
c. Inability or unwillingness to satisfy debts.
d. Unexplained affluence.
e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

20. Conditions that could mitigate security concerns include the following:

a. The behavior was not recent.
b. It was an isolated incident.
c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation).
d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control.
e. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G
Alcohol Consumption

21. The Concern. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.
22. Conditions that could raise a security concern and shall be disqualifying include the following:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use.
b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job.
c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence.
d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.
e. Habitual or binge consumption of alcohol to the point of impaired judgment.
f. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

23. Conditions that could mitigate security concerns include the following:

a. The alcohol related incidents do not indicate a pattern.
b. The problem occurred a number of years ago and there is no indication of a recent problem.
c. Positive changes in behavior supportive of sobriety.
d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed 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.

a. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence shall impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.
b. 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),
2. Inhalants and other similar substances.

c. 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 shall be disqualifying include the following:

a. Any drug abuse (see above definition).
b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution.
c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence.
d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program.
e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, shall almost invariably result in an unfavorable determination.

26. Conditions that could mitigate security concerns include the following:

a. The drug involvement was not recent.
b. The drug involvement was an isolated or aberrational event.
c. A demonstrated intent not to abuse any drugs in the future.
d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

GUIDELINE I
Emotional, Mental, and Personality Disorders

27. The Concern. Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social, and occupational functioning. These disorders are of security concern because they shall indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the Government, must be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.
28. Conditions that could raise a security concern and shall be disqualifying include the following:

a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that shall indicate a defect in judgment, reliability, or stability.
b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication.
c. A pattern of high-risk, irresponsible, aggressive, antisocial or emotionally unstable behavior;
d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

29. Conditions that could mitigate security concerns include the following:

a. There is no indication of a current problem.
b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation.
c. 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 is no longer emotionally unstable.

GUIDELINE J
Criminal Conduct

30. The Concern. A history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness.
31. Conditions that could raise a security concern and shall be disqualifying include the following:

a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged.
b. A single serious crime or multiple lesser offenses.

32. Conditions that could mitigate security concerns include the following:

a. The criminal behavior was not recent.
b. The crime was an isolated incident.
c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life.
d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur.
e. Acquittal.
f. There is clear evidence of successful rehabilitation.

GUIDELINE K
Security Violations

33. The Concern. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.
34. Conditions that could raise a security concern and shall be disqualifying include the following:

a. Unauthorized disclosure of classified information.
b. Violations that are deliberate or multiple or due to negligence.

35. Conditions that could mitigate security concerns include the following actions:

a. Were inadvertent.
b. Were isolated or infrequent.
c. Were due to improper or inadequate training.
d. Demonstrate a positive attitude towards the discharge of security responsibilities.

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 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 shall be disqualifying include any service, whether compensated, volunteer, or employment with the following:

a. A foreign country.
b. Any Foreign National.
c. A representative of any foreign interest.
d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

38. Conditions that could mitigate security concerns include the following:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities.
b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M
Misuse of Information Technology Systems

39. The Concern. Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems shall raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.
40. Conditions that could raise a security concern and shall be disqualifying include the following:
    a. Illegal or unauthorized entry into any information technology system.
    b. Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system.
    c. Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
    d. Introduction of hardware, software, or media, into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

41. Conditions that could mitigate security concerns include the following:

    a. The misuse was not recent or significant.
    b. The conduct was unintentional or inadvertent.
    c. The introduction or removal of media was authorized.
    d. The misuse was an isolated event.
    e. The misuse was followed by a prompt, good faith effort to correct the situation.

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.

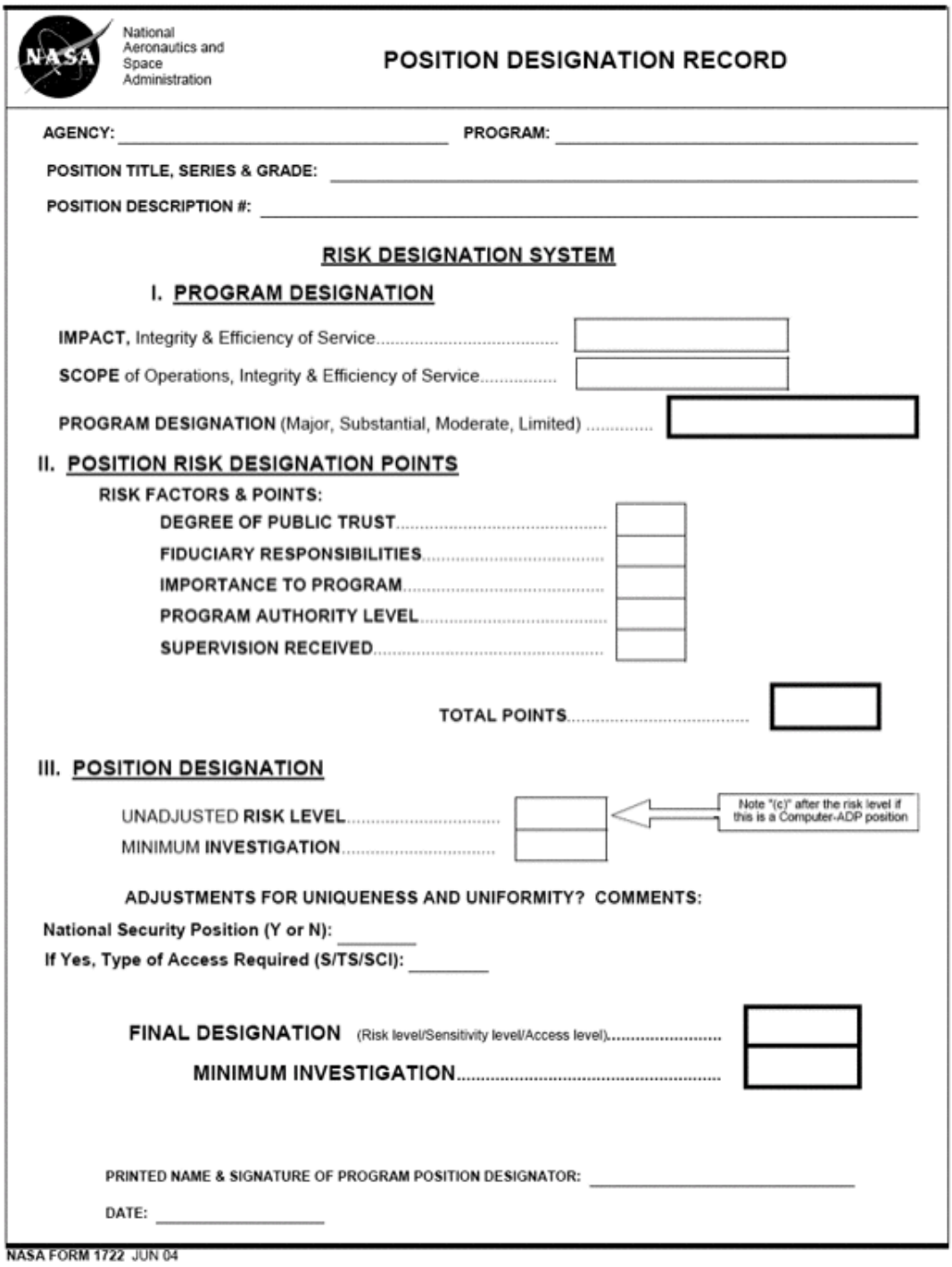
Position Designation Records. Each NASA Center shall complete and maintain the Position Designation Record or its equivalent for each Agency civil service position and will also maintain similar records for NASA contractor personnel.

- 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.