NASA Procedural Requirements

NPR 1600.1A
Effective Date: August 12, 2013
Expiration Date: December 12, 2028

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

NASA Security Program Procedural Requirements (Updated with Change 1)

Responsible Office: Office of Protective Services

Table of Contents

Change History

Ch #	Date	Description/Comments
1	2/22/2023	Updated with Change 1, In Section 4.3.2 removed item a. and re-lettered a-h.

Preface

P.1 Purpose

a. Per Title 51, section 20132, this NASA Procedural Requirement (NPR) establishes Agency protective services implementation requirements set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended.

b. This NPR prescribes NASA protective services procedural requirements for NASA Centers and Component Facilities in executing the NASA security program to protect people, property, operations, and Classified National Security Information (CNSI). It establishes program specifications necessary to achieve uniformity, standardization, centralization, and decision-making authority where appropriate. Policy and procedural requirements for the protection of CNSI is further promulgated in NASA NPR 1600.2, NASA Classified National Security Information.

c. Protection and handling requirements for NASA sensitive unclassified information as of the date of this revision are provided for within the Sensitive But Unclassified (SBU) policy and procedures, NASA Interim Directive (NID) 1600.55, Sensitive But Unclassified (SBU) Information. This policy is scheduled to change in FY 2013 as NASA executes Executive Order 13556, November 4, 2010, Implement Controlled Unclassified Information (CUI). This Executive Order mandates the implementation of a Government-wide program which, when fully implemented, will replace SBU policy and procedures in their entirety. No use of the designation CUI is authorized at this time or until official notification is made by the Office of the Chief Information Officer.

d. NPR 1382.1, NASA Privacy Procedural Requirements, sets forth the requirements for protecting of the privacy of personal information, such as Personally Identifiable Information (PII).

P.2 Applicability

This NPR is applicable to NASA Headquarters and all NASA Centers, including Component Facilities, to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center, and NASA contractors to the extent specified in their contracts. Address comments regarding this NPR to the AA for the Office of Protective Services or the NASA Headquarters designee. Refer questions concerning the application of these requirements to specific NASA Centers to the appropriate NASA Center Protective Services Office.

P.3 Authority

National and Commercial Space Programs, 51 U.S.C. § 20132, § 20133 and § 20134, Pub. L. No. 111—314, 124 Stat. 3328 (December 18, 2010).

P.4 Applicable Documents and Forms

a. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799.

b. Unlawful Acts, 18 U.S.C. § 922 (d) (9).

c. Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2011 et seq.

d. Permission to Use Firearms, 51 U.S.C. § 20133.

e. Arrest Authority, 51 U.S.C. § 20134.

f. The Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

g. Classified National Security Information, Exec. Order No. 13526, 75 C.F.R. 707 (2010).

h. Controlled Unclassified Information, Exec. Order No. 13556.

i. Suitability, 5 C.F.R. Part 731.

j. Chemical Facility Antiterrorism Standards (CFATS), 6 C.F.R. Part 27.

k. Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel, 14 C.F.R Part 1203(b).

l. Inspection of Persons and Personal Effects at NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials, 14 C.F.R. Part 1204, subpart 10.

m. Law Enforcement Officers Safety Act Improvements Act of 2013, as amended.

n. NPD 1000.3D, NASA Organization (w/change 37, dated June 11, 2013).

o. NPR 1382.1, NASA Privacy Procedural Requirements.

p. NPD 1440.6H, NASA Records Management.

q. NPD 1600.2E, NASA Security Policy.

r. NPD 1600.3, NASA Prevention of and Response to Workplace Violence.

s. NPD 1600.4, National Security Programs.

t. NPR 1600.2, NASA Classified National Security Information (CNSI).

u. NPR 1600.3, NASA Personnel Security.

v. NID 1600.55, Sensitive But Unclassified (SBU) Controlled Information.

w. NPR 1620.2, Facility Security Assessments.

x. NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

y. NPR 2810.1, Security of Information Technology.

z. NPR 4200.1, NASA Equipment Management Procedural Requirements.

aa. NPR 8000.4A, Agency Risk Management Procedural Requirements.

bb. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping (w/Change 6, dated October 24, 2011).

cc. NPR 8715.3, NASA General Safety Program Requirements (w/Change 8 dated June 20, 2012).

dd. NASA Technical Standard (NASA-STD) 8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics

ee. Sensitive Compartmented Information Facilities (SCIFs), Director of National Intelligence (DNI) Intelligence Community Directive (ICD) 705.

ff. Technical Surveillance Countermeasures (TSCM) ICD 702. gg. NSDD 298: National Operations Security Program. hh. Critical Infrastructure Security and Resilience Presidential Policy Directive (PPD)-21.

ii. Homeland Security - Interagency Security Committee Standards (ISC), Physical Security Criteria for Federal Facilities (2010).

jj. SF 312, Classified Information Nondisclosure Agreement.

kk. SCI NDI 4414 Sensitive Compartmented Information (SCI) Nondisclosure Agreement.

ll. NF 1506, Controlled Area Sign (Outdoors).

mm. NF 1506A, Controlled Area Sign (Indoors).

nn. NF 1507, Limited Area Sign (Outdoors).

oo. NF 1507A, Limited Area Sign (Indoors).

pp. NF 1508, Exclusion Area Sign (Outdoors).

qq. NF 1508A, Exclusion Area Sign (Indoors).

P.5 Measurement/Verification

a. Center Directors and Center Chiefs of Protective Services/Chiefs of Security (CCPS/CCS) or their designees determine, implement, ensure, and document compliance by applying a verification approach that is tailored to meet the needs of the Center. The Office of Protective Services (OPS) conducts functional reviews of the Centers, spot-checks, and inspections to review Center compliance and implementation.

b. To determine the OPS compliance with the requirements in this NPR, internal and external auditors responsible for verifying Headquarters requirements and processes shall evaluate performance against the requirements contained herein.

P.6 Cancellation

This NPR cancels the remaining chapters of NPR 1600.1, NASA Security Program Procedural Requirements w/Change 2, dated April 1, 2009. The remaining Chapters are: 1, 6-10 and Appendices D, E, F, G, H, K, L, and O.

Original Signed by

Richard J. Keegan
Associate Administrator
Mission Support Directorate

Chapter 1. Introduction

1.1 Overview

1.1.1 This NPR establishes Agency-wide program policy and guidance for security operations, program security, and NASA Federal Arrest Authority (FAA).

1.1.2 This NPR establishes standards and specifications required to maintain consistency and uniformity for the protection of NASA assets, while considering the unique requirements, circumstances, and environments of individual NASA Centers and locations. During emergencies or periods of increased threat, exigent circumstances may require suspension of certain provisions of this NPR. In that event, immediate coordination with the Assistant Administrator, Office of Protective Services (AA, OPS) is required.

1.1.3 This NPR also presents terminology, definitions, and security measures that are intended to facilitate coordination and support with other U.S. Federal agencies such as the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the Department of Defense (DoD).

1.1.4 This NPR provides for the assignment and delegation of certain security and protection responsibilities as required by law, regulation, and sound management practice.

1.2 Responsibilities

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

1.2.2 The NASA Administrator is responsible for implementing a comprehensive and effective security program for the protection of people, property, operations, and information associated with the NASA mission. The Administrator shall appoint an AA, OPS.

1.2.3 The AA, OPS shall:

a. Oversee Agency implementation, integration of, and compliance with the NASA security program by providing executive management policy direction and ensuring through Agency advocacy, adequate resources are identified and committed to accomplish the security mission in support of the overall NASA mission, NASA Strategic Plan, and national-level security requirements.

b. Provide functional and operational support for physical and program security policy formulation.

c. Provide overall focus and direction for protecting the NASA workforce, visitors, programs, and infrastructure.

d. Develop and implement Agency policy and procedural requirements to ensure law enforcement and investigative activity performed in conjunction with OPS security responsibilities at NASA installations are developed and implemented in consistence with authorities granted under the Public Law 111-314. This shall be consistent with the NASA Office of Inspector General (OIG)

investigative authorities and in close coordination and cooperation with local, state, and Federal law enforcement agencies as defined in the appropriate memoranda of agreement (MOA).

e. Serve as the Agency Risk Acceptance Authority (RAA) for all NASA security program risk management determinations that require a waiver of Agency security requirements. This does not include IT Security RAA, which is the Chief Information Officer's (CIO) responsibility.

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

g. Serve as the Agency Critical Infrastructure Assurance Officer (ACIAO) responsible for approving all Center proposals for additions and deletions to the NASA Critical Infrastructure (NCI) Inventory List when such proposals are concurred on by the respective Mission Directorate Associate Administrator.

h. Comply with all relevant Executive Orders, Presidential Directives, Presidential Policy Directives (PPDs), and other binding directives including the requirements of PPD-217, Critical Infrastructure Security and Resilience.

i. Provide central oversight and conduct assessments of the NASA Critical Infrastructure Protection Program (NCIPP).

j. Effectively coordinate and collaborate with the CIO to ensure critical cyber assets are identified and included in the NCI inventory.

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

l. Develop and issue, under separate NPR, facility security assessment requirements and physical security requirements for NASA facilities and property. These NPRs shall include the facility assessment, physical and procedural standards to ensure consistency and uniformity in the application of security measures that comply with Interagency Security Committee (ISC) standards.

m. Establish, disseminate, and enforce comprehensive performance standards that address overall security capabilities, training, response to likely emergencies and contingencies, and general compliance with Agency standards. Conduct inspections, as well as scheduled and unscheduled reviews, to ensure compliance and efficiency.

n. Establish, disseminate, and ensure adherence to NASA Protective Services Contract (NPSC) standards. Serve as the final approving official for technical portions of each Center contract prior to solicitation in order to maintain consistent contract standards.

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

p. Serve as the Agency oversight official for implementation and management of the Agency FAA Program and Use of Force policy in compliance with 51 U.S.C. § 20133, 20134, and 14 C.F.R. Part 1203b-Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

q. Establish and maintain a Central Adjudication Facility to adjudicate all Agency requests for security clearances for access to CNSI.

r. Coordinate security and law enforcement policy with the Office of General Counsel.

s. Evaluate compliance with this NPR and overall effectiveness of the NASA security program through periodic site visits and functional reviews.

t. Ensure that the NASA security program operates in compliance with national security policy, applicable DHS program directives, and other national-level regulations.

u. Coordinate NASA representation on all security policy development forums and committees.

v. Serve as NASA representative to the DHS ISC.

w. Responsible for the NASA TSCM program.

1.2.4 Center Directors shall:

a. Provide current and effective security for all Center and Component Facility personnel, property, facilities, operations, and CNSI consistent with this NPR.

b. Appoint a qualified and experienced CCPS/CCS in coordination with and after obtaining the concurrence of the AA, OPS, in accordance with NPD 1000.3D, The NASA Organization. Minimum qualifications include:

(1) Sufficient authority and resources to accomplish national, Agency, and Center security goals and objectives with coordination and concurrence of the AA, OPS.

(2) Relevant experience in the security management, national security intelligence, emergency management, or law enforcement professions.

(3) Leadership and managerial experience at a proven level commensurate with the expectations and requirements of the CCPS/CCS position.

(4) Ability to obtain and maintain a Top Secret security clearance.

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

(1) Personnel, facilities, and equipment necessary to implement and sustain an effective security program.

(2) Appropriate training and professional certification of security personnel, as established by the AA, OPS.

(3) The development and management of Center-specific security program policy and procedural requirements that implement this NPR's requirements.

d. When recommended by the CCPS/CCS and Center CIAO, propose NCI and Key Resource assets for inclusion in the NCI Inventory to the Mission Directorate Associate Administrator(s).

e. Act as the Designated Official (DO) and RAA for Center security program risk management determinations that are not designated as NCI or do not require waiver of national security requirements.

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

1.2.5 Under authority delegated from the AA, OPS, the CCPS/CCS shall:

a. Act as the principal advisor and authority to the Center Director in all matters relating to the NASA security program, as established and defined in NPD 1600.2, NASA Security Policy, as amended.

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

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

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

e. Coordinate with the Center CIAO and oversee all aspects of the Center NCIPP.

f. Using all available sources of intelligence information (i.e., NASA counterintelligence/counterterrorism program, local law enforcement, the NASA OIG, and other Federal agencies), continuously evaluate Center and program-level criticality and vulnerabilities and local threats and prepare appropriate countermeasures tailored to the resources requiring protection, specifically identifying Center Critical Infrastructure and Key Resources, in coordination with the Center CIO and CIAO, for inclusion in the NCIPP.

g. Establish priorities for the effective deployment of Center security resources and processes during routine and emergency situations.

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

i. Notify the OIG of suspected criminal activity consistent with existing Memoranda of Understanding (MOU) or agreements.

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

k. Ensure appropriate training and professional certifications for security staff and armed security force personnel commensurate with their assigned tasks, weapons, and equipment. To the extent possible, follow NASA standard processes, procedures, and certifications.

l. Ensure the AA, OPS provides concurrence on NPSCs prior to solicitation.

m. Act as the Center Director's primary staff advisor during any security-related crisis or serious incident and as primary representative to all external law enforcement agencies on security matters.

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

o. Participate as a principal member of Center teams dealing with resolution of workplace violence

and protection issues as set forth in NPD 1600.3, NASA Policy Directive on Prevention of and Response to Workplace Violence.

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

q. Maintain Center security program statistics and provide quarterly reports to the AA, OPS utilizing the format in Appendix C, Property Loss and Incident Details of this NPR.

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

s. Establish a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, new construction, major renovations, and modifications.

t. Ensure compliance with NPR 4200.1, NASA Equipment Management Procedural Requirements.

1.2.6 Program, Line Managers, and Supervisors shall:

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

b. Ensure deployment of CCPS/CCS recommended security and loss-prevention measures within their programs and/or project or organizations.

c. Report adverse information discovered to the CCPS/CCS.

d. When an employee's clearance, eligibility for a sensitive position, or access to NASA facilities is suspended or revoked and when an employee violates security rules and procedures, take appropriate action as directed by the CCPS/CCS.

1.2.7 Individual employees shall:

a. Report suspicious activity, criminal activity, violations or suspected violations of national security, and other Center security requirements to the Center Protective Services or Security Office.

b. Recognize and comply with individual responsibilities and roles in maintaining the Agency and Center security program.

c. Protect Government property, programs, IT systems, CNSI, and sensitive information in accordance with the requirements of this NPR, NPR 1600.2, NASA CNSI, and NPR 1382.1, Privacy Procedural Requirements.

d. Cooperate with NASA security officials during inquiries and investigations.

e. Complete security education, awareness orientation, and refresher training as required.

1.3 Best Practices

In conjunction with other programs, directories, or offices, the AA, OPS and CCPS/CCS shall develop and share "best practices" programs and processes where appropriate.

1.4 Exceptions and Waivers

1.4.1 Centers may occasionally experience difficulty in meeting specific security program requirements established in this NPR and may request an exception or waiver.

1.4.1.1 An "exception" is a request for a one-time deviation or exemption from compliance otherwise with a specific procedural requirement, typically for a single event granted by the Associate Administrator, Mission Support Directorate (AA, MSD). Exceptions are for a specified period of time, normally not exceeding one year, and are based upon appropriate justification to allow a Center, organization, or program time to achieve compliance. Upon expiration of the approved exception, compliance is mandatory unless an extension is granted by the AA, MSD.

1.4.1.2 A "waiver" is a request for a permanent or extended deviation or exemption (for the foreseeable future) for compliance with a specific procedural requirement granted by the AA, MSD. Waiver requests may be approved only in part, such as for a period less than requested or for only parts of the measures requested to be waived.

1.4.2 The process for submitting requests for exceptions or waivers to specific elements of the NASA security program requires that the program or project manager and CCPS/CCS justify the waiver request through:

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

b. Effect of potential loss of capability to the Center.

c. Compromise of CNSI.

d. Injury or loss of life; loss of one-of-a-kind capability.

e. Inability of the Center to perform its missions and goals.

(1) Justification will also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

(2) The waiver request shall be submitted to the Center Director.

1.4.3 The Center Director shall either recommend approval or return the waiver request to the CCPS/CCS for further study or closure. The Center Director forwards concurrence to the AA, MSD.

1.4.4 The AA, MSD shall review waiver requests and forward to the AA, OPS requesting concurrence and/or comments.

1.4.5 The AA, OPS shall return the waiver request to the AA, MSD with a recommendation for approval of the waiver, further study, or denial.

1.4.6 The AA, MSD shall return the waiver requests to the Center Director with his approval or disapproval.

Chapter 2. Security Operations

2.1 Security Controls at NASA Centers

2.1.1 Procedures shall be implemented to ensure only authorized personnel are admitted to NASA controlled, owned, and leased property.

2.1.2 Each Center shall apply and maintain appropriate physical security measures necessary to provide for protection of persons, missions, information, and property as promulgated in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

2.1.3 The maintenance of a controlled perimeter and entry access control points (ACPs) are fundamental to NASA's security-in-depth approach to physical security.

2.1.3.1 All Center perimeter entry ACPs open to traffic shall be staffed by armed, uniformed Security Police Officer (SPO)/Security Officer (SO) personnel at all times. The SPO/SO will:

a. Validate the personnel identification and access eligibility of all personnel entering NASA property by visually examining Federal identification or locally produced, temporary visitor identification or passes.

b. Visually match the photograph with the face of the person presenting the identification.

c. Authenticate identification cards and access using automated means where available.

d. Assess entering vehicles for obvious security concerns.

2.1.3.2 To prevent unauthorized access to critical areas, information, or personnel, additional access control measures, including the use of unarmed personnel, electronic access equipment, and passive and active barriers may be established at individually designated ACPs, security areas, and facilities within the Center.

2.1.3.3 Each Center shall be responsible for the procurement, installation, management, and maintenance of all Center premise access control equipment, integrated intrusion detection, closed-circuit video equipment, and any peripheral equipment.

2.1.3.4 SPO/SOs shall be used throughout the Center to provide traffic safety, detect and deter criminal conduct, enforce security rules and policies, detect unauthorized personnel, act as first responders to critical incidents, establish emergency or temporary control points, respond to calls for assistance, and perform other duties as determined by the CCPS/CCS.

2.1.4 Photography at NASA Facilities.

2.1.4.1 Center Directors, in coordination with the CCPS/CCS and the Center Office of the Chief Counsel, shall establish and implement an individual Center photography policy for the general and public access areas consistent with existing security conditions.

2.1.4.2 Photography is prohibited in Limited areas, Exclusion areas, and within NCI facilities without prior approval of the CCPS/CCS.

2.2 Inspection of Persons and Property

2.2.1 General.

2.2.1.1 Consistent with NASA's requirement to ensure appropriate protection for personnel, property, and facilities, NASA reserves the right to conduct an inspection of any person and property in his/her possession as a condition of admission to, continued presences on, or upon exit from any NASA facility. Implementation of requirements, policy, and procedures for all aspects of this program shall be in accordance with 14 C.F.R. Part 1204, subpart 10. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property, Appendix C addresses items prohibited from NASA facilities. Where NASA facilities are located on a military installation or an area of concurrent/proprietary jurisdiction, NASA personnel are subject to their policies and procedures.

2.2.1.2 All entrances to NASA real property or installations shall be conspicuously posted with the following notices:

a. "CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from this installation is contingent upon your consent to inspection of person and property."

b. "UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you may not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

2.2.2 SPO/SOs shall be trained on how to perform inspections and, with appropriate training, may use inspection tools and detection devices (mirrors, x-ray, and other sensing devices) and/or canines, as necessary.

2.2.2.1 Training for security personnel conducting searches shall include:

a. Appropriate search techniques for the type of vehicle being searched.

b. Key locations where devices or other contraband may be secreted.

c. Procedures for confiscating illegal or dangerous items, detaining of individuals, and referring incidents to the NASA OIG or appropriate external law enforcement.

2.2.2.2 Such inspections shall be conducted in accordance with the following guidelines:

a. Consent to Inspection Notices shall be prominently posted at entrances to NASA Centers and Facilities. Language for these notices is contained in 14 C.F.R. §1204.1003, Subpart 10.

b. Only NASA security personnel or members of the installation's uniformed security force will conduct inspections. Such inspections will be conducted in accordance with guidelines established by the AA, OPS.

c. Prior to undertaking an inspection, security personnel not in uniform shall present their NASA credentials to the subject of the inspection.

d. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., CNSI, weapons, drugs, or explosives), or other prohibited items described in NPR 1620.3A, Physical Security Requirements for NASA

Facilities and Property, Appendix C, the items shall be confiscated, and the individual will be denied admission to or be escorted from the Center or detained at the scene as directed by the CCPS/CCS or his/her designee. The NASA OIG or appropriate local law enforcement authorities will be notified immediately.

e. If, during an inspection conducted pursuant to this subpart, an individual is in possession of U.S. Government property without proper authorization, that person will be required to relinquish the property to the security representative pending a determination on the proper authorization for the possession of the property or its removal from the installation. The individual relinquishing the property will be provided with a receipt for the property.

2.3 Violations of Security Requirements

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

2.4 Denial of Access

2.4.1 To address immediate security and safety issues, the AA, OPS has delegated authority to the CCPS/CCS for denial of access. CCPS/CCS, Center Directors, and the Headquarters Operations Director or their designees may order the temporary denial of access or removal from NASA facilities/resources of any person who violates NASA security requirements, national security regulations, or whose continued presence on NASA property constitutes a security or safety risk to persons or property.

2.4.2 The foregoing is a denial of access and is distinct from suspension or removal from Federal employment of Federal civil servants, which is governed by 5 C.F.R. Parts 315, 731, 752, or 359 and in coordination with the Center Office of the Chief Human Capital Officer (OCHCO) and Center OCC/OGC.

2.5 Imminent Security Threat or Safety Risk

2.5.1 The CCPS/CCS, Center Directors, and the Headquarters Operations Director or their designees shall order the temporary removal and/or denial of access to all NASA facilities of any person who violates NASA security requirements and whose continued presence on NASA property constitutes an imminent security threat or safety risk to persons or property. Circumstances of removal and/or denial of access will be articulated in a report to become a matter of official record.

2.5.2 Civil Service Employees.

2.5.2.1 Immediately upon taking such action, the CCPS/CCS will notify the Center Director, Center OCHCO, and Center OGC of the reasons for the decision to temporarily deny access or remove from NASA facilities/resources any civil service employee. As soon as reasonably possible, the CCPS/CCS will notify the AA, OPS. If no imminent security threat or safety risk exists, any contemplated temporary denial of access shall be advised and commented upon prior to action by Center OHCM and Center OCC/OGC. Any non-concurrence requires Center Director decision or

notification.

2.5.2.2 Upon notification by the CCPS/CCS, as designee, of the temporary removal or denial of access of the civil service employee, the Center OCHCO in consultation with OCC/OGC shall then determine the appropriate access status and any other employment limitations of the civil service employee. The employee may continue to be denied access until this status is finalized.

2.5.3 Contractor and Non-NASA Employees.

2.5.3.1 For contractor and non-NASA employees (e.g., visitors and guests) denied access, and immediately after denying access, the CCPS/CCS, as designee, shall notify the appropriate Government sponsor and contracting officer of the reasons for the decision to temporarily deny the individual's access to or remove them from the Center.

2.5.3.2 The CCPS/CCS shall notify the non-NASA employee who is denied access in writing of the reason for the temporary removal or denial of access and of the Denial of Access Reconsideration Process. Should the individual elect not to request reconsideration/appeal, the decision may become final. In his discretion, the AA, OPS may reconsider any denial of an access decision.

2.5.3.3 The CCPS/CCS shall conduct a new determination in consideration of the security violation to determine continued access eligibility of the employee consistent with the HSPD-12 credentialing standards listed in NPR 1600.3, Personnel Security Section 2.16.

2.5.3.4 Should the CCPS/CCS make a final determination to deny access, the individual may initiate the Denial of Access Reconsideration Process. This shall occur in accordance with NPR 1600.3, Personnel Security Section 2.17.

2.5.3.5 If the non-NASA employee denied access declines to appeal, either through communicating in writing or time for the appeal has expired, the original determination will be final. During the reconsideration process the individual is not granted access to any NASA facility unless coordinated with the CCPS/CCS.

2.5.3.6 Upon resignation, termination of employment, or release of the non-NASA employee by his/her employer or sponsor, the reconsideration/appeal process will otherwise continue, per NPR 1600.3, Personnel Security Section 2.17.

2.6 Denial of Access - Security Considerations

2.6.1 As designee of the AA, OPS, the CCPS/CCS shall take appropriate security measures to monitor, control, and restrict physical and logical access by individuals to the Center. These measures may include:

a. Recovery and confiscation of NASA issued access badge(s) and IT resources.

b. Posting of denial of access information at all Center access locations.

c. Notification to Center IT resources to deny IT access.

d. Suspension of access to CNSI.

e. Notification to appropriate supervisory personnel referencing denial of access.

f. Inspections and securing of the individual's Center work space.

g. Notification to other NASA Centers and the AA, OPS.

2.7 NASA Security Areas

2.7.1 Types of NASA Security Areas.

2.7.1.1 NASA Controlled Area (formerly known as "Restricted Area") as defined in 14 C.F.R. Part 1203a. A Controlled Area is a physical area, including buildings or facilities, in which security measures are taken to safeguard and control access to property and hazardous materials or other sensitive material or to protect operations that are vital to accomplishing the mission assigned to a Center or Component Facility. The Controlled Area shall have a clearly defined perimeter, but perimeter physical barriers are not required.

a. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority.

2.7.1.2 NASA Limited Area as defined in 14 C.F.R. Part 1203a. A Limited Area is a physical area in which security measures are taken to safeguard or control access to classified material or unclassified property warranting special protection or property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. A Limited Area shall also have a clearly defined perimeter; but where it differs from a Controlled Area is that permanent physical barriers and access control devices, including walls and doors with locks or access devices are implemented to assist occupants in keeping out unauthorized personnel. All facilities designated as NASA Critical Infrastructure (NCI) or key resources will be designated at minimum as "Limited" areas.

a. During working hours, personnel within the area will be responsible for challenging all persons who may lack appropriate access authority.

b. Sensitive material, property, and hazardous material can be stored in this area in approved containers. All CNSI material will be secured during non-working hours or when no cleared personnel are present in GSA approved security containers or other methods approved by the CCPS/CCS. c. When the Limited Area is not in use, access through the access control devices (i.e., keys, combinations to mechanical/electronic cipher locks, and badge reader controls) will be limited to authorized personnel. To prevent unauthorized access to such property, visitors will be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

2.7.1.3 NASA Exclusion Area (formerly known as a "Closed Area") as defined in 14 C.F.R. Part 1203a. An Exclusion Area is a permanent facility dedicated solely for safeguarding and use of CNSI. It is used when vaults are unsuitable or impractical and where entry to the area alone provides visible or audible access to classified material.

a. To prevent unauthorized access to an Exclusion Area, visitors will be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

2.7.2 Establishment, Maintenance, and Revocation.

2.7.2.1 Establishment.

2.7.2.1.1 Center Directors, Director of Headquarters Operations, or their designee (the designee is CCPS/CCS unless otherwise specified), and the AA, OPS shall establish, maintain, and protect such

areas designated as NASA Controlled (formerly known as a "Restricted Area"), NASA Limited, or NASA Exclusion (formerly known as a "Closed Area") per the foregoing definitions and criteria.

a. Only the AA, OPS or the CCPS/CCS will establish an area functioning for the protection, use and storage of CNSI.

b. Only a coordinating office or the AA, OPS will establish a Special Access Program Facility (SAPF) or Sensitive Compartmented Information Facility (SCIF) based on legal authority, Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with the Cognizant Security Authority and as promulgated in NPD 1600.4, National Security Programs.

2.7.2.2 Maintenance.

2.7.2.2.1 Security measures shall vary according to individual situations; however, the following minimum-security measures will be taken in all security areas:

a. Post appropriate signage at entrances and at intervals along the perimeter of the designated area, for the facility to provide reasonable notice to persons that the area is a security area. SAPFs and SCIFs are not required to use identifying signs due to Operations Security (OPSEC) concerns.

(1) Outdoor signs are metal, measuring approximately 40.64 cm/16 inches high and 50.8 cm/20 inches wide.

(2) Indoor signs are of cardboard or foam board, measuring approximately 22.86 cm/9 inches high and 12 inches wide.

b. Signage shall be ordered through Center supply sources for NASA Forms. Available signage includes:

(1) Controlled Area Sign (Outdoors), NASA Form 1506

(2) Controlled Area Sign (Indoors), NASA Form 1506A

(3) Limited Area Sign (Outdoors), NASA Form 1507

(4) Limited Area Sign (Indoors), NASA Form 1507A

(5) Exclusion Area Sign (Outdoors), NASA Form 1508

(6) Exclusion Area Sign (Indoors), NASA Form 1508A

c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

2.7.2.3 Revocation.

Once the need for a security area no longer exists, the area must return to normal non-secure area procedures as soon as practical.

2.7.3 Access.

2.7.3.1 Only those NASA employees, contractors, and visitors who need access and who meet the following access criteria shall enter a security area unescorted. All other individuals requiring access must be continually escorted by authorized NASA employees or NASA contractors.

2.7.3.2 To enter a NASA Controlled Area (formerly known as "Restricted Area") unescorted,

individuals must undergo the appropriate investigation or training procedures required for that area as established by the individual Center or program. When an investigation is required, at a minimum, a National Agency Check with Inquiries (NACI) shall be initiated for civil service employees and for non-NASA personnel.

2.7.3.3 To enter a NASA Limited Area unescorted, individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a favorably adjudicated NACI for areas with unclassified information and material.

2.7.3.4 To enter a NASA Exclusion Area (formerly known as "Closed Area") unescorted, individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

2.7.3.5 Center Directors and the AA, OPS shall rescind previously granted authorizations to enter NASA Security Areas when an individual's clearance and need-to-know are no longer justified, their presence threatens the security or safety of the property, or when access is no longer required for official purposes.

2.8 Standards for Secure Conference Rooms

2.8.1 When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in Director National Intelligence (DNI) Intelligence Community Directive (ICD) Number 705.

2.8.2 At a minimum, NASA Secure Conference Rooms shall be identified as NASA Limited Areas.

2.8.3 The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with ICD 705.

2.8.3.1 Meetings shall be limited to collateral Secret or below.

2.8.3.2 Meetings shall not be regularly scheduled or re-occurring meetings.

2.8.3.3 Positive access control shall be implemented, and personnel security clearances of all attendees will be validated.

2.8.3.4 A Security Specialist shall conduct a visual inspection and establish security procedures for the meeting.

2.8.4 Special Cases.

2.8.4.1 The preceding specifications do not apply to conference areas in which the level of security exceeds the collateral Secret level.

2.8.4.2 For these areas, guidance on additional requirements will be provided by the CCPS on a case-by-case basis. 2.8.4.3 The AA, OPS or CCPS/CCS shall be contacted for any interpretation of these specifications.

2.9 Technical Surveillance Countermeasures (TSCM)

2.9.1 TSCM Program.

The AA, OPS is responsible for the NASA TSCM program. The program shall be consistent with ICD 702 Technical Surveillance Countermeasures. All matters pertaining to the conduct of TSCM activities throughout the Agency will be directed and coordinated through the AA, OPS.

2.10 National Terrorism Advisory System (NTAS)

2.10.1 General.

2.10.1.1 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.

2.10.1.2 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.

2.10.1.3 In addition to assistance from OPS, the Center shall obtain support from representatives such as the Department of Defense (DoD), Federal Bureau of Investigation (FBI), Department of State, NASA Office of Inspector General (OIG), and state and municipal law enforcement agencies.

2.11 NASA National Terrorism Advisory System (NTAS) Program

2.11.1 This section explains the establishment of the NASA NTAS program which is designed to meet the requirements of the NTAS developed and implemented by the Department of Homeland Security (DHS).

2.11.2 NASA NTAS and associated actions are outlined in Appendix D, NASA NTAS Actions.

2.11.3 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 DoD's use of ALPHA designators under the DoD Force Protection Condition concept are understood and integrated into the Center's threat condition warning system.

2.11.4 NASA's alert system recognizes and utilizes the alert type structure of the DHS NTAS to provide for a greater consistency to threat reactions at both the national and at the Agency level.

2.11.4.1 The alert system types range from "No Current Alerts" (normal operating security policy), "Elevated Threat Alert," and "Imminent Threat Alert."

2.11.4.2 The alert system is intended to standardize terms and establish standardized security measures that can be initiated by the AA, OPS and Center Directors through the Agency-wide emergency notification system.

2.11.4.3 The AA, OPS shall initiate, modify, or rescind NASA-wide NTAS.

2.11.4.3.1 The AA, OPS shall monitor the threat status in the Agency and maintain close liaison with the DHS and national-level intelligence and security agencies for timely and accurate threat information.

2.11.4.4 Center Directors and CCPS/CCS shall implement threat mitigation measures initiated by

the AA, OPS and may implement additional measures for their Center based on the local threat situation. They will not lower or rescind a threat mitigation action initiated by the AA, OPS.

2.11.4.5 The CCPS/CCS shall maintain close liaison with the local FBI offices and local law enforcement agencies for threat information.

2.12 Security Threat and Incident Reporting

2.12.1 General.

2.12.1.1 All Centers shall implement a security threat and incident reporting system, as required by NPD 1600.2, NASA Security Policy.

2.12.1.2 The system's purpose is to keep the Agency's senior management officials advised on a timely basis of serious security-related incidents or threats that may affect the NASA mission.

2.12.1.3 After advising Center senior management officials, CCPS/CCS reports shall be forwarded expeditiously to the AA, OPS. Refer to Appendix E, NASA Serious Incident Report for format.

2.12.2 The CCPS/CCS ensures that incidents are reported to the AA, OPS and followed up with a detailed situation report that describes the incident.

2.12.3 Any type of incident that might have Agency security implications shall be reported to the AA, OPS in a timely manner, including but not limited to the following:

a. All crimes or incidents at a Center requiring notification of NASA OIG, the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), Bureau of Alcohol, Tobacco, Firearms, and Explosive (ATF), or local law enforcement.

b. Suspected Espionage (reported through appropriate classified Center Counterintelligence (CI) channels).

c. Suspected Sabotage (reported through appropriate classified Center CI channels).

d. Suspected terrorist activity (e.g., surveillance, photography, attempted penetrations, and unusual requests for information (reported through appropriate classified Center CI channels)).

e. Bombing incidents, including bomb threats and necessary responses, which severely impact Center activities.

f. Actual or planned demonstrations or strikes.

g. All weapons discharges, including unintentional discharges, or other violent acts. Refer to Appendix H, Discharge of Firearms. Planned and pre-approved scientific or experimental discharges do not require reporting.

h. All incidents (mishaps and close calls) that involve a fatality, the need for professional medical attention, or damage to NASA facilities or equipment and meet NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping classification criteria shall be reported and processed in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

i. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on

NASA property shall be reported to the Center NASA Safety Office in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping).

j. A security-related incident that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities and/or in which the media has become involved and publicity is anticipated.

k. An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incidents shall include unauthorized access, theft, interruption of computer/network services or protective controls, damage, disaster, or discovery of a new vulnerability.

l. Threats against NASA property.

m. Physical threats to the infrastructure that support NASA missions.

n. Threats against NASA personnel.

o. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.

p. Information concerning individuals who are perceived to be acting irrationally in their efforts to make personal contact with Government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American and anti-U.S. Government demonstrations in the United States, involving serious bodily injury or destruction of property; or an attempt or credible threat to commit such acts to further political, social, or economic goals through intimidating and coercive tactics.

2.12.4 The CCPS/CCS will maintain statistics for areas identified in Appendix C, Property Loss and Incident Details. This information will be sent to the AA, OPS quarterly and/or as requested.

2.13 Protective Services Response to Demonstrations and Civil Disturbances

2.13.1 The primary objectives in dealing with demonstrations are to direct demonstration activity to areas outside Centers and to preserve peace while protecting the rights of demonstrators peaceably to assemble and exercise free speech. Centers with property open to the general public must consult with their Center OCC/OGC.

2.13.2 The CCPS/CCS shall make reasonable efforts to safely manage groups or crowds who have assembled. The CCPS/CCS should make appropriate liaison and coordination with local law enforcement, and/or adjacent Federal agency facilities.

2.13.2.1 The CCPS/CCS will 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.

2.13.2.2 If demonstrators trespass onto NASA property, the CCPS/CCS will protect NASA personnel, property, and information in accordance with the law.

2.13.3 The CCPS/CCS shall ensure that the contract security force receives training in dealing with demonstrators during annual in-service training and as refresher training immediately prior to a demonstration, when possible.

2.13.3.1 Ensure that NASA Special Agents, Security Specialists, and contract Security Police Officers/Security Officers (SPOs/SOs) receive training in dealing with demonstrators during in-service training and as refresher training prior to a scheduled demonstration, when possible.

2.14 Hazardous Material Security

2.14.1 Storing certain quantities of hazardous materials may be considered chemicals of interest under the Chemical Facility Antiterrorism Standards (CFATS) program managed by the DHS. When exceeding certain threshold amounts, the storage of these chemicals may have to be reported to the DHS and also require additional site specific security requirements and plans. Complete details of the program requirements are explained in 6 C.F.R. 27 Chemical Facility Antiterrorism Standards.

2.14.2 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.

2.14.3 In coordination with Center safety, logistics, environmental, and transportation officials, Center Protective Services Offices shall ensure the Center develops and implements security plans specifically designed to provide the appropriate level of protection in the transportation, receipt, access, use, storage, and accountability of hazardous materials used by NASA. Security Plans will include:

a. Review of shipping/transportation procedures to ensure appropriate precautions are in place and recommend changes and/or adjustments.

b. Appropriate sharing of threat information associated with the targeting of hazardous materials.

c. Establishment of Center-specific receipt, escort, and hand-off procedures.

d. Establishment of security procedures for permanent and temporary storage/holding areas to include defining secure areas.

2.15 Investigations

2.15.1 The investigative component of Protective Services is directly related to the security and protection mission and may include inquiries into such matters as threats or occurrences of workplace violence, harassment, eligibility and suitability for HSPD-12 requirements, missing or stolen property, misuse of Government property, unauthorized access, and other violations of NASA and Center security policies.

2.15.2 The CCPS/CCS shall closely coordinate investigative activity with the appropriate internal and external organizations (e.g., OIG, CIO, OCHCO, Office of the Chief Counsel, EEO, FBI, ATF, DoD, and local and state police) to ensure that cases are referred to the appropriate organization for follow-up when this is required.

2.15.3 Reports of Investigation shall be thoroughly documented. HQ, OPS will be notified of

investigations of security incidents as prescribed in paragraph 2.12 of this NPR.

2.15.4 The CCPS/CCS shall coordinate the release of information concerning reported missing and stolen controlled Government property with the Center Logistics Management Division on a quarterly basis to ensure accountability of controlled property and compliance with NPR 4200.1, NASA Equipment Management Procedural Requirements.

2.16 Security Education, Training, and Awareness (SETA) Program

2.16.1 General.

2.16.1.1 The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them.

2.16.1.2 Management and employee involvement is essential to an effective security program.

2.16.1.3 An integral part of the overall NASA security program relies on the education and training of individuals regarding their security responsibilities.

2.16.2 Responsibilities.

2.16.2.1 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.

2.16.2.2 The CCPS/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 2.16.3.

2.16.2.3 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 CCPS/CCS.

2.16.3 Required Briefings and Training.

2.16.3.1 Initial Orientation Security Briefing. This briefing shall be 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 to protect Government property from theft, loss, or damage. Orientation briefings should include, but are not limited to, general discussions on:

a. Access/entry and exit control procedures and responsibilities.

b. Property accountability responsibilities.

c. Pilferage control.

d. Identification of restricted areas.

e. Use and security of identification credentials.

f. Key and lock control procedures.

g. Protection of CNSI and/or SBU (includes Personally Identifiable Information (PII), For Official Use Only information, other privacy act information, and sensitive operational information).

h. Emergency reporting procedures.

i. Reporting security violations and/or suspicious activity.

j. Orientation to the local area and criminal trends.

2.16.3.2 Annual Security Training. This training is designed to sustain an appropriate level of awareness throughout the workforce and reinforce the security policies and procedures outlined in initial orientation training.

2.16.3.3 Supervisory Security Briefing. Security orientation briefings shall be given by the responsible supervisor or designee to each new employee and will include all security requirements and procedures for which the employee is to be specifically responsible.

2.16.3.4 Security Clearance Briefing. The CCPS/CCS will ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance and being granted access to classified information. This briefing shall include:

a. Execution of Classified Information Nondisclosure Agreement (SF 312 and/or SCI NDA 4414, where appropriate).

b. General security aspects affecting employment and a summary of restrictions, obligations, and reporting requirements associated with access to CNSI that are imposed by statute or executive order.

c. Employee reporting obligations.

d. Security procedures for handling CNSI, classified meetings and discussions, and how to apply Need-to-Know.

e. Standards of behavior expected of persons in sensitive positions and the responsibility of security clearance holders to report behavior and adverse information which might bear on another individual's security clearance eligibility.

f. The most current Executive Order number and information if the briefing form has not been revised to reflect that change.

2.16.4 Annual Security Clearance Refresher Briefing. The CCPS/CCS will ensure the appropriate security clearance refresher briefing is given to all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Initial and annual refresher briefings are also required for individuals granted accesses to certified National Security Systems that process classified information. Clearances may be suspended or revoked for failure to complete annual training.

2.16.4.1 CNSI Custodian Briefing. The CCPS/CCS will ensure classified material custodians and any other custodians responsible for CNSI security containers, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

2.16.4.2 CNSI Termination Briefing. The CCPS/CCS will ensure security termination briefings are given to employees whose personnel security clearances are being terminated due to termination of

employment, transfer to another Center, or if the individual no longer requires access to CNSI. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their life-long responsibilities and penalties for unauthorized disclosure of CNSI even after termination of the clearance or employment.

2.16.4.3 The CCPS/CCS will ensure other special security training or briefings are given to employees related to SAP's, SCI, and NCI. 2.16.5 Foreign Travel Briefings. CI 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.

a. NASA employees shall report to the Center or Agency CI Office any meetings with foreign nationals from designated countries that are held outside NASA-controlled facilities in advance of the meeting.

(1) NASA employees attending the meeting will make themselves available for intelligence threat awareness pre-briefings and debriefings in accordance with NPD 1660.1B. The Center International Visit Coordinator (IVC) can provide a list of designated countries.

2.16.6 Although the OCIO has authority for SBU policy and procedures, the Center Protective Services Office shall provide both security awareness and guidance to projects and programs regarding protection of unclassified sensitive mission information or technologies. The information provided to programs and projects will be based on industry best practices and real-life lessons learned with the Agency.

2.17 NASA OPS Functional Reviews

2.17.1 This section sets standards for establishing and maintaining an ongoing NASA OPS Functional Review Program. This program shall include the periodic review and assessment of the Information, Industrial, Personnel, Physical Security, Program Security, Emergency Management, Protective Services Contract Review, and COOP operations at all NASA Centers.

2.17.2 The objective is to ensure that each Center is implementing their Protective Services programs 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.

2.17.3 Responsibilities.

2.17.3.1 The AA, OPS is responsible for the NASA OPS Functional Review Program. The AA, OPS shall designate Agency personnel to assist in carrying out this responsibility. The means and methods for the conduct of functional reviews may include:

a. A review of relevant Protective Services directives, guides, training material, and instructions.

b. Interviews with the Center Director (or representative), Center Operations Director (or representative), Protective Services Contracting Officer, Protective Services representatives, and customers.

c. Review of Information, Industrial, Emergency Management, Personnel, and Physical Security Programs.

d. Review of various files and documents pertaining to day-to-day operations and records required to be maintained by this NPR.

2.17.3.2 A standard functional review guide/checklist will be used by the inspectors conducting the review. Each Center will be inspected at least every three years. The format for documenting findings will be set by the AA, OPS. The AA, OPS, in its oversight capacity, may schedule reviews of Centers on an as needed basis.

2.17.3.3 Each review may be adjusted to meet the coverage of the security programs in place at that particular Center.

Chapter 3. Program Security and NASA Critical Infrastructure (NCI)

3.1 General

3.1.1 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.

3.1.2 The objective is to identify security provisions as early as possible in system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

3.2 Responsibilities

3.2.1 The CCPS/CCS for each Center is responsible for the following:

3.2.1.1 Establishing a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.

3.2.1.2 Incorporating appropriate security measures, outlined in the various chapters of this NPR and others, into project plans, facility plans, construction and modernization projects, and requests for proposals impacting program security.

3.2.2 Project and program managers at NASA Centers are responsible for ensuring provisions contained in NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, are appropriately addressed with the CCPS/CCS.

3.2.3 The AA, OPS shall compile and maintain the NCI inventory of NASA mission-essential infrastructure assets. The AA, OPS will identify critical infrastructure where a cyber-security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The list will consist of:

a. The critical or key asset description (cyber, physical, or both).

b. The owning Center/program.

c. The physical location to include defining the whole or partial facility.

d. The responsible enterprise.

e. Whether the asset is part of the Agency continuity of operations planning program.

f. Contingency plans to ensure sufficient redundancies exist for key systems and infrastructure elements. Plans should be reviewed/vetted through all key stakeholder organizations.

3.2.4 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. 3.2.5 Project and program managers are responsible for reporting incidents or perceived incidents involving loss of sensitive mission information to the Center Protective Services Office.

3.3 OPSEC

3.3.1 NSDD 298: National Operations Security Program establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program. 3.3.2 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.

3.3.3 The NASA minimum security standard is to employ OPSEC measures on all classified programs.

3.3.4 If OPSEC planning is warranted, program and project managers, in coordination with the Center Protective Services Office, shall develop and implement a project OPSEC plan that will identify critical information or activity, analyze threat(s) and vulnerability(ies), assess risk, and apply appropriate countermeasures.

3.4 Risk Management Process

3.4.1 The AA, OPS in coordination with the concerned directories, programs, projects, and Centers shall establish and implement an Enterprise Security Risk Management Program that enhances operational readiness and mission success by providing security support to program/projects throughout the life cycle of a system or activity that is commensurate with the risk and helps ensure mission critical information, technologies, and/or assets are appropriately protected.

3.4.2 NASA has adopted a risk management approach, using requirements established in NPR 8000.4A, Agency Risk Management Procedural Requirements, NPR 1620.2, Facility Security Assessments, and NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, in which the risk must be weighed against the cost and operational impact of implementing established minimum-security standards.

3.4.3 Risk management provides a mechanism that allows security and program/project managers to recommend waivers to security standards based upon a threat and vulnerability assessment and the resulting risk determination.

3.4.4 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.

3.4.5 The CCPS/CCS shall ensure that security and program standards, established in this and other NPRs are met or that appropriate requests for exception or waivers are submitted and approved by the AA, MSD.

3.5 Special Security Programs

3.5.1 All NASA security activity associated with Special Security Programs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG). Furthermore, NPD 1600.4, National Security Programs, establishes policy for Special Access Programs (SAP).

3.5.2 Sensitive Compartmented Information (SCI) Programs.

3.5.2.1 SCI programs shall only be created within NASA upon specific written approval of the AA, OPS or his designated representative to ensure required security protocols are implemented and maintained. Furthermore, NPD 1600.4, National Security Programs, establishes policy for SCI programs.

3.5.2.2 All requests for NASA personnel, including NASA contractors, to participate in SCI programs external to NASA must be coordinated with the AA, OPS or his/her designated representative to ensure accountability of NASA equities.

3.5.2.3 Failure to comply with the requirements of this section shall result in denial or revocation of security clearance and suspension of SCI activity.

3.6 NASA Critical Infrastructure (NCI) and Key Resources Identification, Prioritization, and Protection

3.6.1 PPD-21 "Critical Infrastructure Security and Resilience" 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 NCI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

3.6.2 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.

3.6.3 Designated NCI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate physical security risk vulnerability assessment. At a minimum, NCI will be designated Facility Security Level III as defined in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

3.6.4 NCI may include IT resources; critical components, communication, command, and control capability, Government-owned flight or experimental flight vehicles, International Space Station and apparatus, and one-of-a-kind irreplaceable facilities.

3.6.5 Supporting infrastructure called "interdependencies" shall not be designated as NCI.

3.6.5.1 "Interdependencies" includes those external and internal commercial elements that the Center NCI depends on to operate, including electrical power, gas, communications hubs, local area networks, and telephone systems.

3.6.5.2 "Interdependencies" nevertheless shall 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" will also take the "single point of failure" aspect into account when developing their mitigation plans.

3.6.6 Policy and procedures shall be developed and implemented at each Center that accurately reflect Agency requirements for assessing NCI as outlined in this and other Agency-wide requirements. This ensures Agency-wide uniformity and consistency in the approach to performing the appropriate security risk assessments for each identified NCI.

3.6.7 Criteria and procedures NASA Centers shall use in identifying NCI are contained in Appendix F, Identifying and Nominating NASA Assets for the NASA Critical Infrastructure Protection Program (NCIPP).

3.6.8 Minimum security requirements for NCI facilities or facilities housing NCI assets are provided in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

Chapter 4. Control, Issuance, and Storage of Arms, Ammunition, and Explosives (AA&E)

4.1 Authority

4.1.1 The AA, OPS is the approval authority for the CCPS/CCS to carry firearms. Authority for NASA OIG personnel to carry firearms is not affected by this chapter and is instead governed entirely by OIG regulation. The AA, OPS may withdraw weapons-carry authority for any NASA Special Agent, Security Specialist, or Armed SPO/SO if deemed in the best interest of the Agency. Persons whose weapons-carry permission is withdrawn may submit a response in writing within ten working days as to why the permission should be reinstated or otherwise mitigated. Via CCPS/CCS, the AA, OPS will consider any such response and his weapons-carry determination is final.

4.1.2 Under authority delegated from AA, OPS, CCPS/CCS shall direct or grant approval for their Center's NASA Special Agents and designated NASA Security Specialists and contractor security personnel to carry firearms. The CCPS/CCS will withdraw weapons-carry authority for any NASA Special Agent, Security Specialist, or Armed SPO/SO if deemed in the best interest of the Agency, but must seek ratification or approval of that decision from the AA, OPS as soon as practicable, by submitting the action taken and the basis for it to OPS. Paragraph 4.4.1 pertains in permitting the affected individual to submit a response to the AA, OPS via CCPS/CCS for final determination.

4.2 Responsibilities

4.2.1 NASA certifying officials, described in Appendix A. Definitions, shall ensure compliance with the requirements of this section.

4.2.2 The CCPS/CCS shall ensure compliance with Appendix H of this NPR when a NASA officer uses, or attempts to use, deadly force against another or a security police activity results in life-threatening injury or the death of another.

4.2.3 NASA employees and contractors to whom firearms are issued are responsible for strict compliance with all the conditions regarding the carrying and use of firearms as established herein and set forth at 14 C.F.R. Part 1203b, Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

4.2.4 NASA security personnel and contractors shall not carry firearms outside the 50 States, the District of Columbia, and U.S. territories (Puerto Rico, Guam, U.S. Virgin Islands, American Samoa, Northern Mariana Islands) without the advance approval of the AA, OPS.

4.3 Authorization to Carry Firearms

4.3.1 The CCPS/CCS or their designated official will ensure that all civil service and contractor employees' weapons training and qualifications records are current.

a. The CCPS/CCS will determine the need for civil service and contractor employees to carry concealed firearms when necessary in the performance of official duties. Firearms shall be

concealed when Special Agents or other armed non-uniformed security personnel are in public places.

4.3.2 NASA Special Agents, Security Specialists, and contract SPOs/SOs may carry firearms, including shoulder-fired weapons (e.g., rifles, machine guns, and shotguns), only if the following requirements are met:

a. The individual has successfully completed a qualification course for the firearm being carried and the qualification is current.

b. NASA Security Specialists required to carry weapons off Center in the performance of official duties must be under direct operational control of a NASA Special Agent and with the prior knowledge and approval of the CCPS/CCS.

c. An initial and annual criminal history check for recertification under 18 U.S.C. § 922 (d) (9) (formerly the Lautenberg Amendment) has been conducted.

d. The individual has satisfactorily completed NASA Protective Services Training Academy (NPSTA) Federal Arrest Authority (FAA) or Security Officer Fundamentals Certification Course (SOFCC) training and is current with all requirements of the training.

e. The individual is physically fit, emotionally stable, and not under the influence of alcohol or drugs that could impair judgment or motor skills.

f. Personnel are prohibited from consuming intoxicants during duty and for eight hours prior to reporting to duty.

g. NASA Special Agents, Security Specialists, and designated contractor personnel authorized to carry concealed weapons shall have their weapon concealed at all times while outside of their immediate office area. Exception: Handguns may be displayed openly if the armed person(s) has on a CCPS/CCS approved outer garment that identifies the armed person as a member of NASA Security.

4.3.3 Conditions Under Which Firearms, Explosives and Pyrotechnics may be Used, Stored, and Maintained by Non-Security Personnel.

4.3.3.1 Researchers and scientists who use firearms, explosives, and pyrotechnics during testing and experimentation shall ensure the safe operation, storage, and accountability of firearms, explosives, and pyrotechnics used.

4.3.3.2 NPR 8715.3, NASA General Safety Program Requirements, and NASA Technical Standard (NASA-STD) 8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics, are the governing documents for establishing the safe storage and handling of explosives, propellants, and pyrotechnics.

4.3.3.3 The following procedures are required for the use, storage, and accountability of firearms, explosives, and pyrotechnics by non-security personnel:

a. NASA program and project personnel contemplating the use of firearms and ammunition must submit a written request to the CCPS/CCS outlining the program or project need for introducing firearms and ammunition onto a NASA facility.

b. An inventory of the type of weapons, explosives, and pyrotechnics with serial numbers, type and

amount of ammunition, and type and amount of explosives or pyrotechnics shall be maintained and updated annually. The inventory will be made available for review by security and safety personnel, as requested.

c. Identify the location of stored/secured firearms, ammunition, explosives, and pyrotechnics and the names of personnel having access.

d. Establish appropriate secure storage for firearms, ammunition, explosives, and pyrotechnics in coordination with the Center Security and Safety personnel and in accordance with NASA-STD 8719.12.

4.4 Carrying Weapons On Commercial Aircraft

4.4.1 Armed NASA Special Agents shall carry firearms on commercial aircraft only after completion of required Federal Aviation Administration certification in accordance with 14 C.F.R. 108.219, when authorized by the AA, OPS or designee (which may not be below SES level), as set forth below, and then only in conjunction with official Government travel. NASA Protective Services contractor personnel are not authorized to fly armed.

4.4.2 Refresher Federal Aviation Administration certification training for carrying firearms on a commercial aircraft shall be required every two years and will be integrated with required firearms qualification to ensure appropriate awareness.

4.4.3 The Special Agent must be currently qualified to carry a firearm.

4.4.4 The Special Agent must be in possession of a current NASA badge and credentials.

4.4.5 The Special Agent shall not display his/her weapon or make known to passengers that he/she is carrying a weapon.

4.4.6 The Special Agent shall always carry the weapon on his/her person and never in carry-on baggage. When practicable, the Special Agent should carry the weapon upon which they actually last qualified. 4.4.7 The Special Agent shall always carry handcuffs when flying armed.

4.4.8 The Special Agent shall never carry Oleoresin Capsicum (OC) spray or other chemical intermediate weapons while on-board a commercial flight.

4.4.9 The Special Agent shall be dressed in appropriate attire and must ensure the firearm remains concealed at all times.

4.5 Firearms Instruction

4.5.1 The certifying official (the AA, OPS or the CCPS/CCS when so delegated) shall designate a firearms instructor, who will inform the certifying official in writing of an individual's knowledge of the rules of firearm safety and the content of this NPR. The firearms instructor will have:

4.5.1.1 Recent firearms training and experience during prior employment, such as the FBI, Secret Service, police, military, or other significant and qualifying experience, shall meet NASA standards if the individual has qualified under all provisions of this chapter within the past 180 days.

4.5.1.2 These qualifications shall be verified by a review of employment and training history either

through an interview with previous management or visual inspection of documented training history.

4.5.1.3 Appropriate NASA training, including firearm safety procedures and use of deadly force, followed by obtaining a qualifying score on a recognized course, as specified in paragraph 4.6 below, shall also be required.

4.5.2 In cases involving the Protective Services contractor force, the firearms instructor may be appointed from the Protective Services contract security force.

4.6 Training

4.6.1 The AA, OPS shall establish through the NPSTA a firearms course with standards for all Center armed security personnel, to include standards for shoulder-fired weapons.

4.6.2 Personnel shall be trained and qualified on professional firearm ranges established and maintained by NASA, or other Federal, state, or municipal authorities. The use of private or commercial weapons ranges will be approved in advance by the CCPS/CCS.

4.6.3 Personnel shall only be certified for carrying firearms after firing a qualifying score under the NASA certified firearm course established by the NPSTA.

4.6.4 Annual training and testing in judgmental shooting using an approved firearms training simulator are required after certification. Personnel shall receive testing and training in judgmental shooting through NASA's current firearms training simulator or other approved methods of judgmental shooting.

4.7 Maintenance of Proficiency

4.7.1 NASA Special Agents, Security Specialists, and security contractors authorized to carry firearms shall be required to fire a qualifying score on the NASA course of fire at least once every six months.

4.7.2 NASA Special Agents, Security Specialists, and security contractors authorized to carry firearms must successfully complete annual testing and training on the simulator, non-lethal training ammunition (e.g., "Simunition") or other approved methods of judgmental shooting.

4.8 Records

4.8.1 The law enforcement training originator shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data.

4.8.2 Records shall be destroyed five years after employee separation.

4.9 Firearms Standards

4.9.1 CCPS/CCS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm their civil service and contractor security staff.

4.9.2 The AFL is approved by the AA, OPS and maintained by the NPSTA. The AFL may be waived or modified only by the AA, OPS.

4.9.3 The user of any NASA-approved firearm must meet the training and certification requirements of the NPSTA programs.

4.9.4 Training, qualifications, and certification for all approved firearms shall be documented per paragraph 4.6.

4.9.5 The use or carrying of a firearm is limited to the approved weapons with which the individual is currently qualified.

4.10 Weapons

4.10.1 Handguns.

4.10.1.1 NASA Protective Services uniformed SPOs/SOs and civil service personnel shall only carry NASA-issued semi-automatic pistols in 9mm or .40 calibers.

4.10.1.2 NASA Protective Services uniformed SPOs/SOs at each Center must be armed with the same make and model handgun. 4.10.1.3 NASA civil service personnel may vary the model to suit individual users.

4.10.1.4 Special Response Teams (SRT) may carry a different make and model upon approval of the CCPS/CCS and AA, OPS.

4.10.1.5 Handguns must always be worn in standard, commercially available holsters; NASA Protective Services uniformed SPOs/SOs must use holsters with a minimum of a Level II retention device.

4.10.2 Patrol Rifles.

At the discretion of the CCPS/CCS, NASA Protective Services uniformed SOs and civil service personnel may be armed with semi-automatic or select fire patrol rifles.

4.10.3 Patrol Shotguns.

4.10.3.1 At the discretion of the CCPS/CCS, NASA Protective Services uniformed SPOs/SOs and civil service personnel may be armed with semi-automatic or pump action 12-gauge shotguns.

4.10.3.2 Shotguns used to employ "less-lethal" ammunition shall be solely dedicated for this use and be clearly identified as less-than-lethal weapons.

4.10.4 Submachine Guns.

At the discretion of the CCPS/CCS, NASA Protective Services uniformed SPOs/SOs and civil service personnel may be armed with submachine guns.

4.10.5 Other Approved Firearms.

At the discretion of the CCPS/CCS, and with the consent of the AA, OPS, other firearms, including those mounted on mobile platforms, may be utilized to meet Center security requirements.

4.10.6 Modifications.

4.10.6.1 No modifications to the operating system, firing mechanism, and/or trigger groups shall be made to any NASA-approved firearms.

4.10.6.2 Only Center armorers will modify or repair grips, sights, and control levers.

4.11 Exchange of Weapons

4.11.1 Weapons shall not be exchanged on a security post.

4.11.2 Any exchange or inspection of firearms shall be accomplished only in an area where a "clearing barrel" is available, if unavailable, then only under proper supervision.

4.12 Firearm Maintenance

4.12.1 All firearms shall be periodically inspected and kept in good working order by a qualified gunsmith/armorer.

4.12.2 Ammunition, holsters, and related equipment shall be periodically inspected for deterioration and kept in good working order.

4.13 Ammunition

4.13.1 Only premium, commercially manufactured, duty ammunition shall be issued.

4.13.2 Duty ammunition shall be expended at training sessions at least once every 12 months to ensure use of fresh duty ammunition.

4.13.3 Normal training ammunition shall be commercially manufactured.

4.13.4 No reloaded or remanufactured ammunition shall be utilized.

4.13.5 Only ammunition with brass cartridge cases (to include brass cases with chrome or nickel plating) shall be used. The use of ammunition with aluminum cartridge cases is prohibited.

4.14 Accountability of Arms, Ammunition, & Explosives (AA&E)

4.14.1 The control and custody of all AA&E within a Center shall be under strict accountability at all times and is the ultimate responsibility of the custodian.

4.14.2 The CCPS/CCS shall appoint a custodian(s) for all AA&E within Center Protective Services and within each NASA Protective Services contractor security force. Programs/projects will appoint a custodian(s) for all explosives, propellants, or ammunition for research or testing purposes. The custodian will:

a. Ensure control, storage, and accountability of authorized AA&E are in accordance with the provisions of this NPR, the requirements established in NPR 8715.3C, NASA General Safety

Program Requirements, NPR 4200.1, NASA Equipment Management Procedural Requirements, and NASA-STD-8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics.

4.14.3 Each custodian shall maintain an ongoing inventory of all AA&E. The inventory will indicate:

a. The date and method of acquisition of all firearms and ammunition. b. Full identifying data, the caliber, make, and serial number of each firearm.

c. Amounts of duty and training ammunition on hand.

d. Types and amounts of explosives (e.g., fragmentary, flash-bang grenades, chemical compunds, and pepper spray grenades).

4.14.5 Current NASA Protective Services contractor firearm data shall be maintained and made available to Center Protective Service Office upon request.

4.14.6 A receipt system for recording the issuance, transfer, and return of all firearms, ammunition, and explosives shall be maintained by the custodian. Receipts will include the following details:

a. Dates of issuance, transfer, or return to custody.

b. Serial numbers of firearms.

c. Numbers and types of assigned explosives.

d. Types and numbers of ammunition on hand.

e. Signatures and legible printed names of recipients.

f. Signatures and legible printed names of custodians or armory issuance personnel upon return of the firearms and explosives. (NOTE: Both NASA personnel and contractor receipts shall be retained by each Center for one year.)

4.14.7 Lost, stolen, or missing AA&E shall be reported immediately to the AA, OPS.

4.14.7.1 This preliminary report shall include all available details concerning the event with a complete description of the weapon or other lost AA&E item(s).

4.14.7.2 This preliminary report shall not be delayed pending a complete report of the circumstances.

4.14.7.3 A description of the lost, stolen, or missing AA&E shall also be entered into the National Criminal Information Center (NCIC) database by local or Federal law enforcement personnel.

4.14.8 Non-security personnel having NASA mission-related uses for AA&E items shall:

a. Ensure control, storage, and accountability of authorized AA&E are in accordance with the provisions of this NPR, the requirements established in NPR 8715.3C, NASA General Safety Program Requirements, and NASA-STD-8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics. b. Maintain appropriate and current inventories of issued and maintained AA&E pursuant to paragraph 4.14 of this NPR and provide a copy of the inventories to the CCPS/CCS upon request.

4.15 Storage of AA&E

4.15.1 Firearms and ammunition shall be stored in accordance with NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, Section 3.17.

4.15.2 Firearms or ammunition shall not be stored in containers with money, drugs, precious materials, evidence, or CNSI. They will be stored separately.

4.15.3 NASA Headquarters and Centers shall adopt procedures for the maintenance of records with respect to the issuance of AA&E and access to firearms and ammunition storage areas and containers.

Chapter 5. NASA Protective Services Office Special Agent and Security Specialist Badges and Credentials (B&C)

5.1 Badge and Credential Use

5.1.1 NASA Credentials will be issued only to those civil service protective services employees who are required to present proof of their authority in the performance of their official duties.

5.1.2 Credentials identifying NASA Special Agents will be issued to those that require FAA or perform counterintelligence/counterterrorism duties. NASA Special Agents must maintain their qualifications within the NASA training programs.

5.1.3 At the request of the CCPS/CCS, credentials identifying Security Specialists may be issued to those whose official duties do not require FAA, but do conduct routine investigative work and/or frequent liaison with Federal, state, or local law enforcement authorities.

5.2 Badge and Credential Issuance

5.2.1The AA, OPS shall create, authenticate, and issue credentials and procure metallic badges at the request of the CCPS/CCS.

5.2.2 Credentials are sequentially numbered and are accountable security items. Their issue, use, and accountability shall be monitored by the AA, OPS and the CCPS/CCS.

5.2.3 The CCPS/CCS shall ensure that Special Agent credentials or Security Specialist credentials no longer required for official duties will be returned to the AA, OPS.

5.3 Badge and Credential Return

5.3.1 The CCPS/CCS shall ensure that credentials are not misused and will withdraw them immediately upon any report of misuse, pending investigation of the allegation.

5.3.2 A report outlining the circumstances of any withdrawal of credentials shall be forwarded to the AA, OPS within 72 hours of the credentials being withdrawn.

5.3.3 A report on the final disposition of the incident, including the results of a Return To Duty assessment and recommendation, shall also be furnished to the AA, OPS for review and final determination.

5.3.4 Lost or stolen credentials must be reported immediately. The CCPS/CCS shall forward a report outlining all pertinent facts to the AA, OPS no later than two days after the loss.

5.3.5 Special Agents and Security Specialists must surrender credentials when requested by the issuing authority or when relieved of security duties by transfer, termination, or retirement.

5.4 Retired Law Enforcement Credentials

5.4.1 In accordance with the Law Enforcement Officers Safety Act Improvements Act of 2010, as amended, the AA, OPS may issue retired law enforcement credentials to NASA Special Agents that had arrest authority status at the time of separation from performance of Special Agent duties.

5.4.2 Upon cessation of Special Agent duties, requests by separating personnel to be issued retirement credentials shall be addressed as follows:

a. The CCPS/CCS shall forward the request for retired credentials from the individual concerned with concurrence/non-concurrence to the AA, OPS for approval and issuance.

b. The employee must have separated from NASA with a satisfactory performance record after completing at least ten years of security services at NASA.

5.4.3 Retirement and presentation of the NASA metal Special Agent Badge may be considered by the CCPS/CCS with concurrence of the AA, OPS based on the following prerequisites:

a. The CCPS/CCS shall submit a written request to the OPS containing the Special Agent's name and length of service with NASA.

b. The Special Agent must be retiring from NASA and leaving the Agency with a satisfactory performance record after completing at least ten years of Special Agent duties at NASA.

c. Special Agent Badges for retirees must be mounted in a Lucite award block.

d. CCPS/CCS shall obtain funding and procure the award once approved.

Chapter 6. NASA Armed Personnel Training, Certification, and Authority

6.1 General

6.1.1 51 U.S.C. § 20133 authorizes the NASA Administrator to prescribe security regulations in support of these regulations and as approved by the Attorney General of the United States. The NASA Administrator also prescribes statutory FAA. Those regulations are set forth in 14 C.F.R. Part 1203b. This chapter identifies the requirements for granting FAA. All NASA contract SPOs/SOs are required to be trained and certified to the standards described in this chapter.

6.2 Applicability

6.2.1 This chapter applies to all NASA Special Agents, Security Specialists, and contractors assigned as NASA SPOs and NASA SOs.

6.3 Responsibilities

6.3.1 The AA, OPS is the designated Senior Agency Official and Program Manager for the NASA security and law enforcement training, which includes NASA Federal Arrest Authority Training and NASA Security Officer Fundamentals Certification Course (SOFCC). These responsibilities include:

a. Directing the FAA Training Program in accordance with applicable laws, Federal Law Enforcement Training Academy (FLETA) requirements, NASA regulations, and directives.

b. Reviewing and approving nominations of all civil service employees to be NASA Special Agents and issuing credentials.

c. Determining any areas of interest in which FAA requirements are lacking and any other matters likely to impede NASA objectives in meeting FAA requirements.

d. Periodically reviewing the FAA Training Program and recommending to the Senior Official any changes necessary.

e. Reviewing and approving all internal safeguards and management procedures.

f. Reviewing and approving all NPSTA training curriculum and courses.

g. Coordinating matters pertaining to the FAA program with the OGC and/or Department of Justice.

h. Approving the NASA curriculum and certification procedures for SOFCC training, which is required for all NASA Security Specialists and contract SOs who are armed but do not require FAA.

6.3.2 Center Directors have the following responsibilities:

a. Consistent with this NPR, and as advised by the Center Chief Counsel and CCPS/CCS, implement

and maintain the NASA FAA program at their respective Center.

b. Ensure that adequate numbers of qualified civil service personnel and contract security force personnel are identified, selected, and properly trained under NASA FAA requirements pursuant to NPSTA FAA and Use of Force Qualifications and Training.

c. Upon notification, immediately suspend from duty with pay or reassign to duties not requiring FAA, any person with FAA alleged to have or suspected of violating FAA procedures or instructions. This suspension will remain in effect until completion of an internal investigation. Suspensions will be immediately reported to AA, OPS.

d. Establish as determined by Center security requirements the need for Special Response Teams (SRT), K-9 teams or other security/law enforcement emergency response teams.

(1) Centers that utilize specialized contractor security teams, such as SRT and K-9, shall utilize standardized selection criteria that will include a physical fitness test, an oral interview, a job-specific physical skills test, a written examination, and a review of employment files (to ensure the SPOs/SOs has completed probationary periods and to confirm that the officer is not under any disciplinary action).

6.3.3 The CCPS/CCS shall have the following responsibilities:

a. Determine and establish operational procedures and arrangements for providing essential, timely, consistent, and effective security and law enforcement response capability.

b. Implement the NASA FAA program after evaluating types of Center jurisdiction; availability and capability of Federal, state, and local law enforcement; and other factors that may impact Center security.

c. Prior to implementation of FAA, coordinate with their Office of Chief Counsel for appropriate consultation (including with the cognizant U.S. Attorney), regarding procedures for the appropriate and timely transfer of arrested persons.

d. In consultation with the Center Office of Chief Counsel, develop appropriate chain of custody procedures and establish the necessary relationships with local law enforcement and Federal law enforcement and prosecutorial agencies to ensure issuance and execution of necessary arrest warrants. The Center OIG may be kept informed of these arrangements.

e. Nominate, as appropriate, civil service and contractor employees for FAA to the AA, OPS.

6.4 Security Equipment Approval and Use

6.4.1 Center protective service operations are unique and often require different types and methods of deployment of specialized equipment to accomplish the Center's protection needs. Many Centers require or authorize the use of specialized firearms, Electronic Control Devices (ECD), K9 Explosive Ordnance Detection (EOD) services, vehicle inspection equipment, narcotics identification and detection equipment, OC spray, batons, and other special control equipment or duty gear that require use of force application and training considerations.

6.4.2 The CCPS/CCS shall ensure that prior to the issuance or the mandated use of any security equipment that the following has occurred:

a. The equipment has been evaluated by the NPSTA for compliance and application within the use of force training requirements.

b. The equipment has been reviewed by the NPSTA for any specialized deployment or utilization training needs.

c. The use of the equipment has been coordinated with the Center Director and Center OCC/OGC.

d. All identified NPSTA and vendor required specialized training has been provided to any approved users.

e. Appropriate accountability measures for the equipment have been implemented.

f. The AA, OPS has been informed of the issuance of any special control equipment or duty gear, and concurs on its use.

Appendix A. Definitions

Access — The ability, opportunity, and authority to gain knowledge of information or gain authorized entry onto a NASA property, leased facilities, and IT resources.

Adjudication — The evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: suitable for Government employment; eligible for logical and physical access; eligible for access to classified information; eligible to hold a sensitive position; or fit to perform work for or on behalf of the Government as a contractor employee.

Arrest — Seizure of the person without warrant based on probable cause he/she has committed a felony or a misdemeanor in the presence of the officer. Subjecting the person to the will and control of the officer; circumstances that would lead a reasonable person to believe that he/she was not free to leave the presence of the officer. Brief detention for purposes of ascertaining a person's identity and/or activities, without more, is not an arrest.

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, as defined in 14 C.F.R. 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.

Center Chief of Protective Services/Center Chief of Security (CCPS/CCS) — The senior Center security official responsible for technical management and day-to-day operations of the Center's security program.

Certification — A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Certifying Authority (CA) — Individual responsible for ensuring and certifying to the Designated Approving Authority, that requisite security measures are implemented for IT systems identified for processing of classified information.

Certifying Officials — The AA, OPS or the CCPS/CCS when so delegated, who are, by virtue of this NPR, authorized to certify that an individual has met established requirements (training, firearms qualification), 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.

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:

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

b. Secret Information — The unauthorized disclosure of which reasonably could be expected to

cause serious damage to national security that the OCA is able to identify or describe.

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

Classified information — Information that has been determined pursuant to Executive Order 13526, or a successor or predecessor order, or the Atomic energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

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

Classified National Security Information (CNSI) — Information that must be protected against unauthorized disclosure IAW Executive Order 13526, "Classified National Security Information," and is marked to indicate its classified status when in documentary form. See definition for "Classification Category" above.

Compromise — The improper or unauthorized disclosure of or access to CNSI.

Contractor — An expert or consultant (not appointed under Section 5 USC § 3109) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of NASA (but not a Federal employee).

Counterintelligence (CI) — 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.

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))

Debarment — Official determination made in writing by OPM or the Center OCHCO that bars, for cause, an individual from accessing NASA property.

Denial of Security Clearance — The adjudication decision that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in Executive Order 12968 have been exercised. Designated Approving Authority (DAA) — Official who formally assumes responsibility for operating an Information Technology Systems or network at an acceptable level of risk.

Director, Security Management Division (DSMD) — Official assigned to OPS responsible for Agency management of physical security, personnel security, industrial security, and program security.

Electronic Access Control System — Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

Electronic Control Device (ECD) — Designed to disrupt a subject's central nervous system by means of deploying battery-powered electrical energy sufficient to cause uncontrolled muscle contractions and interrupt an individual's voluntary motor responses.

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, and authorized topics of discussion.

Exception — A request for a one-time exemption for compliance with a specific procedural requirement for a single event granted by the Associate Administrator, Mission Support Directorate (AA, MSD). Exceptions are for a specified period of time, normally not exceeding one year, and are granted after appropriate justification to allow a Center, organization, or program time to achieve compliance.

Executive Order (E.O.) — Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Federal Arrest Authority (FAA) — The arrest authority granted under 14 C.F.R., Section 1203b.103 to NASA security personnel.

Infrastructure — A collection of assets. See definitions for asset and system.

Involved Member — A Protective Services contractor SPO/SO or civil service employee that has discharged a firearm while performing official duties.

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 Amendment — 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" (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.

NASA 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.

NASA Critical Infrastructure (NCI) — Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations.

NASA Critical Infrastructure Protection Program (NCIPP) — The planning and implementation of an enhanced protection level for Agency key resources identified by a 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.

NASA Controlled 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.

NASA Employees — NASA civil service personnel.

NASA Exclusion 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.

NASA PHOTO-ID — Refers to the NASA photo-ID that has any number of embedded and external technologies 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 Policy Directive (NPD) — NPDs are policy statements that describe what is required by NASA management to achieve NASA's vision, mission, and external mandates and who is responsible for carrying out those requirements.

NASA Procedural Requirements (NPR) — NPRs provide Agency requirements to implement NASA policy as delineated in an associated NPD.

National Agency Check (NAC) — The NAC is a search of the following four indices:

a. 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. b. FBI Identification Division contains a fingerprint index and name file.

c. FBI Records Management Division contains files and records of all other investigations (background, criminal, loyalty, intelligence).

d. Defense Clearance and Investigations Index contains investigations, including criminal investigations, conducted on civilian and military personnel in the DoD. (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 minimum level of background investigation conducted by the OPM required for a civil service or contractor employee to be issued a Personal Identity Verification (PIV) card.

Non-disclosure Agreement (NDA) — SF 312 is a non-disclosure agreement required under Executive Order 13526 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the Information Security Oversight Office of the National Archives and Records Administration and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. SF 312 replaces the earlier forms SF 189 or SF 189-A. Enforcement of SF-312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion, or removal, in addition to the likely loss of the security clearance."

Non-NASA Employee — Any paid worker who is not a NASA civil service employee.

Open Storage — Storage of CNSI in a security container or vault that does not incorporate secondary level storage in security containers.

Original Classification Authority (OCA) — An individual authorized in writing, either by the President, agency heads, or other senior Government officials designated by the President to classify information in the first instance.

Personally Identifiable Information (PII) — Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Reasonable Grounds or Probable Cause — Circumstances which would lead a reasonably prudent person to believe a party committed a crime; more evidence that the person is guilty than evidence the person is not but with room for doubt.

Reasonable Suspicion — Circumstances which induce a reasonable person to believe criminal activity is at hand; it justifies a SO or SPO in stopping a person and inquiring into his activities and/or identity.

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

Risk Assessment (RA) — The process of identifying internal and external threats and security vulnerabilities, identifying the likelihood of an event arising from the combination of such threats and vulnerabilities. Further, the RA defines the critical security countermeasures necessary to continue an organization's operations, defines the controls in place or necessary to reduce risk, and evaluates the cost for such controls.

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

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 Special Access Program information.

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 Officer (SO) — An armed officer, who has successfully completed the required NASA training, but who is not to exercise NASA arrest authority, whose duties may include but are not limited to: first response to emergencies, mobile patrols, temporarily detain or seize with reasonable suspicion, inspections, perimeter and internal access control, contingency posts, and crowd control. An SO may request an SPO effect an arrest when he either has directly observed any Federal offense or has reasonable grounds to believe that a felony has been committed.

Security Police Officer (SPO) — An armed officer, who has successfully completed the required NASA training, with NASA Federal arrest authority, whose duties may include but are not limited to: first response to emergencies, enforces Federal law, mobile patrols, inspections and searches, traffic enforcement, investigations, and other duties as required. An SPO may effect an arrest on

request of an SO, as stated above.

Security Specialist — A qualified and trained NASA civil service employee assigned to perform certain security duties such as physical, personnel, and program security functions.

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 (including the loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; and security area violations). (NOTE: Does not include incidents of criminal activity, such as theft, assault, or DUI).

Sensitive But Unclassified (SBU) Information — 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.

Special Access Program (SAP) — Any program established and approved under Executive Order 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Special Agent — A qualified and credentialed NASA civil service employee assigned to perform specialized security, investigative, or law enforcement duties authorized by statute and this NPR.

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 Federal employment. 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. See 5 C.F.R. Part 731.

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

Technical Surveillance — Covert installation or modification of equipment to monitor (visually or audibly) activities within target areas or to acquire information by specialized means.

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. Used in conjunction with a Vulnerability Assessment to prepare an RA.

Unauthorized disclosure (Executive Order 13526) — A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access or may also be the result of inadvertent disclosure.

Waiver — The approved request for a permanent or extended exemption (more than one year) for compliance with a specific procedural requirement granted by the AA, MSD.

Appendix B. Acronyms

AA	Assistant Administrator or Associate Administrator
AA&E	Arms, Ammunition, and Explosives
AFL	Approved Firearms List
ATF	Bureau of Alcohol Tobacco, Firearms, and Explosive
CAD	Call and Dispatch
CA	Certifying Authority
CFATS	Chemical Facility Antiterrorism Standards
CCPS/CCS	Center Chief of Protective Services/Center Chief of Security
CI	Counterintelligence
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIPP	Critical Infrastructure Protection Program
CISD	Critical Incident Stress Debriefing
CNSI	Classified National Security Information
CO	Contracting Officer
CUI	Controlled Unclassified Information
CSO	Center Security Office
DAA	Designated Approving Authority
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DO	Designating Official
DoD	Department of Defense
DSMD	Director of Security Management Division
EAP	Employee Assistance Program
ECD	Electronic Control Devise
ECP	Entry Control Point
EEO	Equal Employment Opportunity
E.O.	Executive Order
EOD	Explosive Ordnance Disposal
EOC	Emergency Operations Center
ESF	Emergency Support Function
FAA	Federal Arrest Authority
FBI	Federal Bureau of Investigation
FLETA	Federal Law Enforcement Training Academy
FLETC	Federal Law Enforcement Training Center

FRS	Force Related Shooting
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICD	Intelligence Community Directive
ITS	Information Technology Security
IVC	International Visit Coordinator
MSD	Mission Support Directorate
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NASA-STD	NASA Technical Standard
NCI	NASA Critical Infrastructure
NCIPP	NASA Critical Infrastructure Protection Program
ND	Negligent Discharge
NDA	Non-disclosure Agreement
NFS	Non-Force Shooting
NPSTA	NASA Protective Services Training Academy
NISPOM	National Industrial Security Program Operating Manual
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSDD	National Security Decision Directive
NTAS	National Terrorism Advisory System
OCA	Original Classification Authority
OGC	Office of the General Counsel
OCHCO	Office of the Chief Human Capital Officer
OIG	Office of Inspector General
OPSEC	Operations Security
PPD	Presidential Policy Directive
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PSCC	Protective Services Communications Center
RA	Risk Assessment
RAA	Risk Acceptance Authority
SA	Special Agent
SAP	Special Access Program
SAPF	Special Access Program Facility
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information

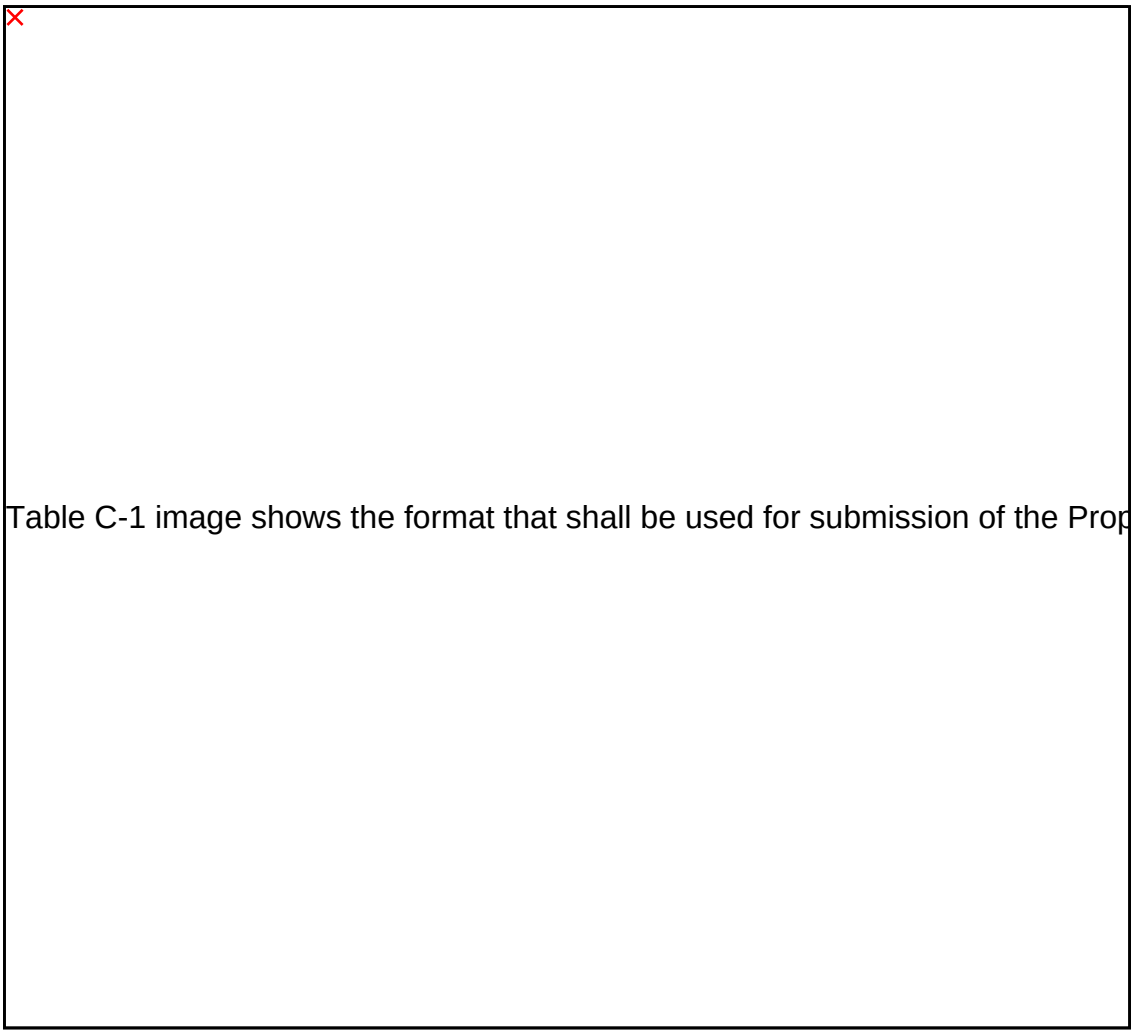
SCIF	Sensitive Compartmented Information Facility
SETA	Security Education, Training, and Awareness
SO	Security Officer
SPO	Security Police Officer
SOFC	Security Officer Fundamentals Certification
SOFCC	Security Officer Fundamentals Certification Course
SPB	Security Policy Board
SRT	Special Response Team
TSCM	Technical Surveillance Countermeasures

Appendix C. Property Loss and Incident Details

C.1 CCPS/CCS shall provide the Property Loss and Incident Details report to the AA, OPS quarterly.

C.2 The format provided in Table C.1 shall be utilized for submission. The CCPS/CCS can contact the AA, OPS for an electronic version.

TABLE C.1



Appendix D. NASA National Terrorism Advisory System (NTAS) Actions

D.1 The National Terrorism Advisory System (NTAS) replaces the color-coded Homeland Security Advisory System (HSAS). This new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, Government agencies, first responders, airports and other transportation hubs, and the private sector.

D.2 NTAS alerts are based on the nature of the threat. In some cases, alerts are sent directly to law enforcement or affected areas of the private sector, while in others, alerts are issued more broadly to the American people through both official and media channels.

D.3 NTAS alerts contain a sunset provision indicating a specific date when the alert expires; there will not be a constant NTAS alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS alert. All changes, including the announcement that cancels an NTAS alert, will be distributed the same way as the original alert.

D.4 NTAS-No Alert, Minimum Security Measures.

D.4.1 Definition: Low risk of terrorist activity against the United States or NASA facilities or personnel.

a. Threat condition (No alert) employs every day, routine security measures determined by the CCPS/CCS and endorsed by the Center Director as being appropriate for the optimum protection of NASA assets at that Center.

b. The program shall include security 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.

D.5 NTAS-Elevated Threat Alert, Minimum Security Measures.

D.5.1 Definition: Warning of a credible terrorist threat against the United States.

a. Continue all No Alert minimum threat mitigation measures.

b. Advise continuously all employees of the condition, through training, briefings, and other mediums.

c. Increase general security awareness, through training, briefings, and other mediums.

d. Secure buildings, rooms, and storage areas not in regular use.

e. Increase security inspections of packages.

f. Check all deliveries at mailrooms and shipping and receiving departments.

g. Periodically test emergency communications capability with command locations.

h. Review and update emergency response plans.

i. Keep key Center personnel updated.

j. Monitor visitors.

k. Curtail special events and visitors.

l. Increase surveillance of critical locations.

m. Coordinate with local law enforcement and emergency response agencies, as required.

n. Assess the threat characteristics for further refinement of established/planned protective measures.

o. Review and implement as necessary contingency, Continuity of Operations Plans (COOP), and emergency response plans.

D.6 NTAS-Imminent Threat Alert, Minimum Security Measures.

D.6.1 Definition: Warning of a credible, specific, and impending terrorist threat against the United States or a NASA facility.

a. Continue all Elevated Threat minimum threat mitigation measures.

b. Inspect all incoming packages at a centralized receiving point.

c. Close the Center to all visitors, admit only essential visitors under escort.

d. Establish random Center checkpoints.

e. Cancel special events.

f. Perform a consent search on all entering vehicles and conduct random searches of exiting vehicles.

g. If necessary, cancel vacations for security personnel.

h. Establish additional 24-hour patrols as necessary.

i. Coordinate with local law enforcement agencies.

j. Limit entry and exit to a single point.

k. Augment security forces as necessary to ensure adequate response capability.

l. Minimize all administrative journeys and visits.

m. Frequently check the exterior of buildings and parking areas for suspicious items and activity.

n. Activate the Emergency Operations Center (EOC).

o. Evaluate reducing NASA personnel on Center to those deemed essential for operation or consider closing the Center, implementing telework.

Appendix E. NASA Serious Incident Report Format

{Date}

TO: Assistant Administrator for the Office of Protective Services

FROM: Center Chief of Protective Services

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 Protective Services Office:
b. Center Safety Office:
c. Local, state, and Federal law enforcement:

4. ACTIONS FOR ASSISTANT ADMINISTRATOR FOR PROTECTIVE SERVICES:

5. COMMENTS/RECOMMENDATIONS:

Appendix F. Identifying and Nominating NASA Assets for NASA Critical Infrastructure Identification, Prioritization, and Protection

F.1 Introduction.

PPD-21, "Critical Infrastructure Security and Resilience," 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.

F.2 Purpose.

To establish the roles and responsibilities of key Agency and Center personnel in the implementation and support of PPD-21 and the Agency Critical Infrastructure Protection Program (CIPP).

F.3 CIPP.

The Agency CIPP implements the Agency critical infrastructure and key resources protection strategy. The CIPP shall be consulted whenever action impacting a NASA Critical Infrastructure (NCI) asset is being considered.

F.3.1 Criteria for Determining NCI.

F.3.1.1 Agency NCI 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 NCI 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 would cause significant impact on the security of the Nation — national economic security, national public health, safety, psychology, or any combination.

b. A NASA critical infrastructure where a cyber-security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

c. A NASA critical 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.

d. Using paragraphs a, b, and c 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 national

defense? Examples include:

(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. Does the loss or compromise or the asset endanger or otherwise threaten the safety and health of the general public? This refers to:

(a) NASA facilities and systems that protect the general public from hazardous materials.

(b) Situations that could be generated using materials owned by NASA to create safety and health hazards.

(c) Utilities, communications, or similar systems on which other Agencies depend to accomplish their essential missions serving the general public.

(d) 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? This 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. Does the loss or compromise of the asset enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy its essential missions? This refers to:

(a) Critical elements of the NASA Strategic Enterprises that are absolutely required for NASA's mission capability.

(b) Critical Infrastructure Interdependencies (e.g., IT resources, data, electric power, water, oil and gas, and environmental control networks) that are dependent on or support NCI and whose loss could directly impact NASA's essential mission capability. These assets need not be identified as separate NCI but shall be integrated into the Center NCI asset protection scheme, evaluated for security risk assessments, and protected accordingly.

(c) Having very high public visibility in terms of the general public's perception of NASA as a symbol of national pride.

(d) Being integral to the performance of NASA's mission, having a very large dollar value, or are difficult or impossible to replace in a reasonable period of time.

(5) Impact on Human Life. Does the loss or compromise of the asset (e.g., telecommunications, telephone system, local area networks, wide-area components, transportation, security and safety,

and buildings or facilities) endanger or otherwise threaten the life, health, or safety of personnel engaged in the performance of NASA's missions?

F.4 Appointment of Agency and Center Critical Infrastructure Assurance Officer (CIAO).

F.4.1 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.

F.4.2 The AA, OPS 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 NCIPP.

F.4.3 The Agency 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 NCIPP.

F.5 Procedures for Nominating NASA Assets for Consideration for Inclusion Under the NCIPP.

Procedures for identifying, nominating, and assessing initial Agency and Center NCI 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 NCI and met all initial milestones.

F.6 Procedures for Adding/Deleting NASA Assets to the NCI Inventory.

F.6.1 At a minimum, all proposed changes to the NCI list shall be coordinated by the Center with the responsible Headquarters Mission Directorate Associate Administrator, the Center's CIO, CCPS/CCS, and CIAO.

F.7 Using the criteria outlined in paragraph F.3.1 above, personnel responsible for the Center and/or Agency asset deemed a candidate for inclusion or deletion under the NCIPP shall follow the below procedure to determine the appropriateness of the NCI designation or deletion. F.7.1 Nominating IT Assets.

a. The system owner, in coordination with the Center CIO, Chief of Security, IT System Security Manager, and the Center CIAO, shall propose IT system inclusion or deletion on the Agency NCI inventory to the Center Director.

b. Upon final determination that the asset must be designated or deleted as an NCI, a written proposal shall be prepared for the Center Director's approval.

c. Upon the Center Director's approval, the Center CIO shall forward the fully justified proposal to the NASA Deputy CIO for ITS.

d. The NASA Deputy CIO for ITS, in consultation with the Center ITS Manager, shall recommend acceptance or rejection of the proposal to the NASA CIO.

e. 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.

f. Upon approval, the Center IT Security Manager and System Owner shall conduct an appropriate IT NCI system assessment using requirements established in NPR 2810.1.

g. Appropriate mitigation plans shall be prepared and implemented to address all vulnerabilities, or if the proposal is disapproved, the NASA CIO will coordinate with the affected Center CIO and Mission Directorate Associate Administrator to establish the appropriate appeals process, if warranted.

h. Upon approval to delete an IT asset from the NCI 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 will update/distribute the NCI list, accordingly.

F.7.2 Nominating Physical Assets.

a. Facility owner, in coordination with the CCPS/CCS and the Center CIAO, shall propose facility inclusion or deletion on the Agency NCI inventory to the Center Director.

b. Upon final determination that the asset must be designated or deleted as a NCI, a written proposal shall be prepared for the Center Director's approval.

c. Upon Center Director's approval, the CCPS/CCS shall forward the fully justified proposal to the NASA CIAO, with copies to the manager of the Mission Directorate Associate Administrator.

d. The NASA CIAO, in consultation with the CCPS/CCS and Mission Directorate Associate Administrator, shall recommend acceptance or rejection of the proposal to the NASA CIAO.

e. The NASA CIAO shall either approve or reject the proposed change.

f. If the proposal is approved, the NASA CIAO shall modify and distribute the updated NCI list, and notify the requesting Center Director; CCPS/CCS; AA, OPS; and Center CIAO of the decision.

g. Upon approval of request for designation as an NCI, the CCPS/CCS and Center CIAO shall ensure the following is accomplished.

(1) Conduct a physical security vulnerability risk assessment.

(2) Prepare and implement appropriate mitigation plans to address all vulnerabilities.

h. 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.

F.8 Upon approval to delete a physical asset from the NCI list, the NASA CIAO shall notify the requesting Center Director; CCPS/CCS; Agency CIO; AA, OPS; and Center CIAO of the decision and update and distribute the NCI list, accordingly.

Appendix G. NASA Federal Arrest Authority and Use of Force Training Curriculum

G.1 General

G.1.1 The Administrator is authorized by 51U.S.C. § 20134 and 14 C.F.R. Part 1203b-Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel to implement an Agency FAA and Use of Force policy to ensure appropriate protection for NASA employees, facilities, information, and missions.

G.1.1.2 The Agency FAA shall be managed in strict compliance with the requirements approved by the Attorney General of the United States and the direction provided in the following paragraphs.

G.1.1.3 Failure to maintain qualification, training, and certification requirements established under this NPR shall result in denial of Center authorization to arm personnel.

G.2 FAA, SOFCC, and FAA Bridge Training Programs

G.2.1 FAA Training Program.

G.2.1.1 FAA training shall not be authorized or implemented at a Center unless the CCPS/CCS has the following assurances:

a. All FAA candidates meet the physical fitness standards prescribed by the NPSTA course curriculum required to graduate.

b. NASA civil service supervisors have ensured that all civil service employees and security contractor personnel nominated for FAA are physically and emotionally stable. FAA training and authorization may be withheld or suspended pending an assessment of an FAA candidate's physical and mental health by a qualified physician.

G.2.2 Attendance at the full FAA 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 (including Federal Law Enforcement Training Center, FBI Academy, Military, or other similar programs). Under these circumstances, a waiver detailing the candidates training history will be submitted to the AA, OPS for approval. Upon approval, the candidate must only attend the FAA refresher course; and

b. The candidate must complete required in-service Use of Force Training, to include Intermediate Force to Lethal Force semiannual qualification with assigned firearm, annual judgmental shooting training, and familiarization training related to NASA regulations and Center implementing instructions for FAA; or

c. The candidate is not identified as requiring FAA training and therefore, must attend and graduate from the NASA Security Officer Fundamentals Certification Course (SOFCC).

G.2.3 Selection and Attendance at NASA FAA Training.

G.2.3.1 Attendance at FAA training is required for all civil service personnel tasked with operational control of those performing duties related to:

a. Investigations.

b. Frequent duty-related interactions with outside law enforcement.

c. VIP and special event protection details.

d. Special Response Team (SRT), K-9, and other law enforcement (LE) special response members.

G.2.3.2 Attendance at FAA training for security services contractor personnel shall be determined by the CCPS/CCS. At a minimum, those performing the following duties will attend FAA:

a. Shift Supervisors (e.g., Captain, Lieutenant, or Sergeant).

b. Those conducting investigations.

c. 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, and disturbances).

(Note: Duties with the potential for the lawful detention of a person pending release to proper law enforcement authorities does not meet criteria for attendance at FAA training.)

G.2.3.3 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, such as CNSI material management, facility security inspections, or conducting interviews and research for the purpose of adjudicating access or suitability, shall not be armed. Civil service personnel performing these functions will be armed only after the AA, OPS approval.

G.2.3.4 Contractor personnel standing static security posts are not required to attend FAA training. These personnel must complete the SOFCC.

G.2.4 SOFCC Training Program.

G.2.4.1 To ensure consistency Agency wide, the SOFCC shall be developed by the NPSTA and taught by NPSTA-certified trainers. The SOFCC will include adequate training on:

a. Use of force and intermediate use of force.

b. Lawful detaining of persons.

c. Unarmed defensive tactics.

G.2.5 SOFCC to FAA Bridge Course.

G.2.5.1 The SOs certified under the SOFCC and Use of Force Training Program may be authorized to have Federal Arrest Authority after completing the FAA Bridge Course Training program.

G.2.5.2 The SOs' eligibility to attend 80 hour SOFCC to FAA Bridge Course Training is dependent on the following:

a. The SOs applying for FAA shall have successfully completed SOFCC within the last two FAA curriculum training cycles.

b. Before participating in the bridge course, the SO shall pass the most current FAA Legal Written Exam with a minimal score of 80 percent on the first attempt.

c. The SO shall meet the criteria for FAA candidacy outlined in this NPR.

G.2.6 SOFCC and FAA Program Mandatory Standards and Testing.

G.2.6.1 SOFCC candidates may be authorized by the CCPS/CCS to carry firearms upon successfully achieving the following standards:

a. All individuals must pass all portions of the designated program with minimum 80 percent passing grade.

b. In case of a failure, candidates shall be provided the opportunity to retake the section failed only one time after initial testing. A repeat failure after retaking the course of instruction will result in the nominee being dropped from SOFCC. CCPS/CCS are NOT authorized to reduce any training standards established under this NPR.

c. An individual failing to demonstrate proficiency during a practical evaluation will be disqualified from the SOFCC.

G.2.6.2 FAA candidates may be authorized by the CCPS/CCS to carry firearms upon successfully achieving the following standards:

a. All individuals must pass all portions of the designated program with minimum 80 percent passing grade.

b. In case of a failure, candidates shall be provided the opportunity to retake the section failed only one time after initial testing. A repeat failure after retaking the course of instruction will result in the nominee being dropped from the FAA program. CCPS/CCS are NOT authorized to reduce any training standards established by the NPSTA.

c. An individual failing to demonstrate proficiency during a practical evaluation will be disqualified from the FAA course.

G.2.7 Authorized FAA individuals shall carry the appropriate Miranda Advisement of Rights cards.

G.3 Use of Force

G.3.1 SPOs/SOs and civil service personnel performing security duties may find themselves in a situation where they are required to detain, take a person into custody, or defend themselves or someone else.

G.3.2 CCPS/CCS shall ensure that NASA Use of Force training is conducted at least semiannually concurrent with required weapons qualification. Established training must include complete and current Use of Force theory and currently recognized practices to ensure an appropriate level of understanding and practical application is present among security force personnel.

G.3.2.1 The application of force during an officer/subject encounter should be based on the

perceived action(s) of the suspect within the totality of the circumstances. An officer's response to a subject's perceived actions must be guided by objective reasonableness when effecting lawful control.

G.3.2.2 If at any time a subject becomes injured while under detention or arrest, immediately request medical personnel to respond to the scene.

G.3.3 If it becomes necessary to use a firearm as authorized in 14 C.F.R. § 1203b.107, NASA CCPS/CCS shall comply with the following procedures:

a. The incident shall be reported to the CCPS/CCS, who in turn, will report it to the appropriate supporting law enforcement agency and then to the AA, OPS as expeditiously as possible with as many details supplied as are available.

b. The CCPS/CCS shall ensure compliance with Appendix H, Discharge of Firearms of this NPR.

c. 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, OPS deems appropriate, pending investigation of the incident.

d. The respective Center Director or the AA, OPS shall appoint an investigating officer to conduct a thorough investigation of the incident. Additional personnel will also be appointed as needed to assist the investigating officer. Upon conclusion of the investigation, the investigating officer will submit a written report of findings and recommendations to the appropriate Center Director or the AA, OPS.

e. Upon conclusion of the investigation, the Center Director and/or the AA, OPS, 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 will be promptly reported to the supporting law enforcement agency.

G.3.4 Prohibitions.

G.3.4.1 Unreasonable use of force is considered misconduct. Such misconduct may result in administrative, civil, and/or criminal action.

G.3.4.2 Verbal abuse, verbal threats of violence, nonphysical threats, cannot alone be the justifiable basis for the use of force.

G.4 Training Curriculum

G.4.1 The NASA Protective Services Training Academy (NPSTA) Program curriculum is developed, managed, and approved by the AA, OPS. Training shall consist of the following topics:

a. Legal studies.

b. General law enforcement studies and exercises.

c. Weapons familiarization and defensive tactics.

G.4.2 All applicants for training must be qualified with the designated handgun from the AFL prior to attendance of any NPSTA program (FAA and SOFCC).

G.4.3 Additional standards are required to qualify for SRT and K9 training and positions.

a. Selection criteria for SRT and K9:

(1) Physical fitness test.

(2) Task specific physical fitness test.

(3) Weapons qualification.

(4) Written test.

(5) Oral interview.

b. All Task Specific Physical Fitness Tests (Pass or Fail) must be approved by the NPSTA. Each demonstration must be completed consecutively within a designated time to be determined based on the course developed and to meet the objectives as designated. Demonstrations include:

(1) Demonstrate overall physical fitness (e.g., run, push-ups, pull-ups, and sit-ups).

(2) Demonstrate defensive tactics.

(3) Demonstrate the ability to maneuver on the ground.

(4) Demonstrate the ability to run stairs.

(5) Demonstrate the ability to maneuver with designated equipment (e.g., vest, gas mask, helmet).

(6) Demonstrate the ability to operate in confined space.

(7) Demonstrate the ability to reason under physical stress.

(8) Demonstrate the ability to manipulate handgun with gas mask still on and under physical stress.

(9) Conduct function check with handgun in a safe direction down range (ERT only).

(10) Complete an obstacle/agility course, including a K-9 Handler task specific test (K9 only).

c. Upon selection, all SRT candidates must attend and pass an NPSTA-approved tactical officer certification course for SRT.

d. Upon selection, all K-9 candidates must pass an NPSTA-approved canine training program.

e. Reoccurring training and certification requirements will be established by the NPSTA.

G.5 FAA and Use of Force Refresher/Certification Training

G.5.1 Personnel trained and certified under the NASA FAA and Use of Force Training Program will attend and complete a 40-hour refresher training every training cycle.

G.5.2 Training cycles start every odd calendar year, January 1 and ends on the even numbered years, December 31.

G.5.3 All applicants requesting certification or recertification must meet the standards outlined by NPSTA.

G.6 SOFCC and Use of Force Refresher/Certification Training

G.6.1 Personnel trained and certified under the NASA SOFCC and Use of Force Training Program will attend and complete 24-hour refresher training every training cycle.

G.6.2 Training cycles start every odd calendar year, January 1 and end on the even numbered years, December 31.

G.6.3 All applicants requesting certification or refresher certification must meet the standards outlined by NPSTA.

G.7 NPSTA Instructor Approval, Certification, and Training

G.7.1 Instructor Certification.

G.7.1.1 NPSTA instructor candidates shall complete a general instructor course and be certified by the Federal Law Enforcement Training Center or an NPSTA-approved equivalent.

G.7.1.2 NPSTA instructors shall successfully complete the NPSTA FAA basic course of instruction.

G.7.1.3 High liability course instructors will complete use of force, defensive tactics, and/or firearms instructor certification course (as applicable) and be certified by the Federal Law Enforcement Training Center or an NPSTA-approved equivalent.

G.7.2 Instructor Approval.

G.7.2.1 NPSTA instructor candidates shall attend a one-week instructor development course. They will participate as a student instructor.

G.7.2.2 New instructors will be evaluated by a designated instructor on their abilities as an instructor, based on the NPSTA Initial Instructor Checklist.

G.7.2.3 The NPSTA Academy Director will send recommendations for instructors to NASA OPS.

G.7.2.4 The NASA OPS shall evaluate the recommendations of the new NPSTA instructor and forward an acceptance or rejection letter to the Academy Director.

G.7.2.5 Failure to meet and maintain minimum standards will result in the instructor candidate being released from the program.

G.7.3 Instructor Annual Training.

G.7.3.1 The OPS will coordinate an annual instructor workshop. Workshops shall be used as a tool to keep instructors updated on new policies, procedures, laws, instructor techniques, etc.

G.7.3.2 Instructors shall attend and participate in annual instructor workshops.

Appendix H. Discharge of Firearms

H.1 Policy.

NASA has specific responsibilities when its security operations result in life-threatening injuries or death to another. This chapter provides procedures intended to minimize additional trauma for officers involved in these incidents and to ensure that all the facts are properly documented. This policy is applicable when a NASA SPO/SO or NASA employee assigned to perform security duties uses, or attempts to use, deadly force against another or a security activity results in life-threatening injury or the death of another.

H.2 Discharge of Firearms.

H.2.1 Internal Review — The Center Protective Services/Security Office is the office primarily responsible for criminal and internal investigations outside the purview of the OIG. Incidents involving the discharge of firearms by members, whether accidental or intentional, will be reviewed by the CCPS/CCS. Written reports are required on all discharges of firearms, noting the exceptions enumerated in this policy.

H.2.2 Exceptions — Exceptions to this policy are: firearms training and qualification and the destruction of injured, rabid, or otherwise dangerous animals. While investigations are not required, supervisory approval and written reports are required for animal destructions.

H.2.3 Criminal Investigation — The investigation conducted by Center Protective Services/Security Office will be limited to policy compliance, initial fact-finding, and evidence/crime preservation. Any further investigation, including the lead investigative authority (i.e., FBI, ATF, or OIG), will be determined and coordinated by the OIG, OCC/OGC and the OPS.

H.2.4 Involved Member's Rights — Any rights of the involved member(s), witness(es), and/or others (including injured persons) and the integrity of investigations arising from such incidents will be strictly maintained.

H.3 Non-Force Shootings (NFS) Procedures.

H.3.1 An NFS occurs when an officer/member discharges a firearm, the projectile does not strike any person, and the officer was not responding to a perceived threat.

H.3.2 A negligent discharge (ND) occurs if a member fails to use reasonable care through inadvertence, thoughtlessness, inattention, and the like. NDs are documented in accordance with applicable Agency policy.

H.3.3 Supervisor Notification — The involved member will immediately notify the Protective Services/Security Communications Center (PSCC) of any firearm discharge (other than the exceptions for training and animals above) including Force Related Shooting (FRS), ND and/or NFS. As necessary, PSCC will notify all on-duty supervisors in officer's/member's chain of command.

H.3.3.1 The Shift Supervisor will make additional notifications, via chain of command, to the CCPS/CCS and the contractor Security Program Manager/Chief.

H.3.3.2 The Center Protective Services Investigator (Duty Agent) will be called out.

H.3.4 Scene Security — The involved member's ranking supervisor (Lieutenant or above) will respond to control the scene. Once the scene is under control, no person will enter prior to arrival of Center Protective Services.

H.3.5 Supervisor Involvement — If the shooting involves a patrol supervisor, an alternate supervisor will be appointed.

H.3.6 Center Protective Services Investigations Authority — The scene will be turned over to the Center Protective Services Investigator upon arrival. The Investigator will assess the incident and determine if a criminal investigation is needed.

H.3.7 Involved Member — Member will remain available for collection of evidence, preliminary interviews, etc.

H.4 Force Related Shootings (FRS).

H.4.1 A FRS occurs when a member: (1) intentionally or unintentionally discharges a firearm at a perceived threat (2) and one or more person is in close proximity and immediate danger of being shot, even if no injury occurs, or (3) if a person is injured or killed by the fired round(s) or debris from the round(s).

H.4.2 Supervisor Notification — The involved member will immediately notify the PSCC of the incident. PSCC will notify all on duty supervisors in the member's chain of command. The Shift Supervisor will initiate notification matrix to include Center Security Office (CSO) Duty Agent.

H.4.3 Outside Agency Investigation — NASA duty agent will request an outside law enforcement agency to investigate shootings involving injury or death to another. Any further investigation, including the lead investigative authority (i.e., FBI, ATF, or OIG), will be determined and coordinated by the OIG, OCC/OGC, and the OPS. Center Protective Services will investigate shooting cases not resulting in injury to a person.

H.4.4 Scene Security — Ranking Supervisor or designee will assign a uniformed SPO/SO to secure the crime scene. A perimeter around the scene will be established and cordoned off, as large as practicable to prevent contamination. Only persons administering necessary emergency medical treatment may enter the scene. Their movements inside the perimeter will be closely monitored and documented to reduce scene contamination. Except for exigent circumstances, no person, regardless of rank, will enter the crime scene prior to the arrival of the designated investigating authority. If the shooting scene is outdoors, no vehicle within the scene, either police or citizen, will be moved prior to examination by the Crime Scene Technician.

H.4.5 Investigative Control — Scene will be turned over to the appropriate investigator upon arrival. Primary responsibility and authority over the crime scene rests with the external investigating authority.

H.4.6 Replace Weapon — The involved firearm and other involved NASA-owned or issued equipment will be secured and safeguarded, consistent with investigative requirements at least until

the external investigating authority determines the member will not be the subject of a criminal prosecution.

H.4.7 Member Available — Absent unusual circumstances which dictate otherwise (i.e., need for medical treatment, decontamination, or other exigent duties) the member will cooperate and remain available for collection of any other evidence, taking of interviews, etc. Accordingly, the member will not shower, wash, change clothes, or discard any items present during the shooting until notified to do so by CCPS/CCS and/or outside investigating authority.

H.4.8 Member's Family — The member may contact a family member to inform of injury status.

H.4.9 Collective Bargaining Representative — If required by applicable collective bargaining agreements, the contracting entity will ensure that the collective bargaining unit representative for the involved member is notified on any firearms discharge (except training or animal exceptions).

H.5 Death or Serious Injury; Not Shooting Related.

H.5.1 General — Member activities that result in the death or serious injury of a person or persons will follow similar procedures, internal review, and investigative protocol as previously outlined.

H.5.2 Traffic Related — Traffic mishaps resulting from member activities that result in death or serious injury of a person or persons will follow similar procedures, internal review, and investigative protocol for FRS.

H.6 Responsibilities of Members — FRS or Serious Injuries or Death.

H.6.1 Protective Services Communications Center (PSCC).

H.6.1.1 Dispatcher will designate a supervisor to respond, dispatch necessary additional patrol units, make contact with appropriate medical personnel, and notify the Communications Shift Supervisor.

H.6.1.2 Ensure a major incident Call and Dispatch (CAD) log is kept, notify the Communications Section Manager, and complete the notification procedure at the direction of the on-duty supervisor or commander.

H.6.1.3 Dispatcher will contact the on-duty field supervisor and on-duty Shift Supervisor. Additionally, PSCC will assist with additional notifications and call outs at the discretion of the Shift Supervisor or his/her designee.

H.6.2 Involved Member(s).

H.6.2.1 After due regard for the preservation of human life, the involved member will secure the scene. Evidence should be left undisturbed except as necessary to safeguard life, property, and secure the scene. Involved member will attempt to determine the physical condition of any injured person, request medical aid, and render first aid when safe to do so.

H.6.2.2 Any member involved in any shooting will immediately notify PSCC of the incident and will request emergency medical assistance, as appropriate.

H.6.2.3 Any members involved in a shooting incident and members who witness a shooting incident

or are involved in any incident involving the death or serious injury of another person are required to submit a detailed report to the Agency within 72 hours of the incident, unless otherwise approved by the CCPS/CCS. Providing a sworn recorded statement to an authorized person investigating the shooting incident meets this requirement.

H.6.3 First Responding Security Police/Police Officer's Responsibilities.

H.6.3.1 First responding officers will check the welfare of members involved, other people involved, provide first aid when appropriate, establish Incident Command, secure the scene and preserve visible evidence, brief the on-scene supervisor and investigative personnel, and other duties as directed.

H.6.3.2 First responding officers will secure the scene, coordinate emergent care, ensure public safety, separate witnesses and obtain preliminary information. Officers will also assist in crowd and media control, and begin an entry and exit log at the entry control point (ECP) of all personnel entering or exiting the scene.

H.6.3.3 An officer will be assigned to accompany the involved member to a medical facility if deemed necessary by the on-scene supervisor/commander and will secure evidence and protect personal property of the involved member. This may be delegated to the companion officer.

H.6.4 Companion Officer's Responsibilities.

H.6.4.1 An assigned companion officer is provided to the involved member for their welfare and safety. Companion officer will remain with them until relieved. Companion officer will transport the involved member to the appropriate security facility and maintain contact. If the involved member is at a medical facility, the companion officer will remain until relieved, as directed by supervision.

H.6.4.2 Companion officer will secure a quiet room and facilitate contacting clergy if requested by the involved member.

H.6.4.3 Companion officer will facilitate collection of evidence from involved member upon request by supervisor or crime scene personnel. In most instances, companion officer should not allow member to wash or change clothes or appearance until crime scene personnel have obtained photographs and collected other evidence.

H.6.4.3.1 In the event of exposure to biological, radiological, or other hazards, the involved member should be allowed to reduce potential health risks by washing if continued exposure increases health risks, even if the collection of evidence is delayed or impacted. Where time permits, these clean-up measures should be approved by supervisors. Where time does not permit, the companion officer should maintain a record of actions taken.

H.6.4.4 Companion officer will inform the on-duty commander of the involved member's location. In the event the involved member is moved from one location to another, the on-duty supervisor or commander will be notified of the new location.

H.6.4.5 Companion officer will not discuss the incident with the involved member. Communications with the companion officer are not privileged and disclosure of any communications may be compelled.

H.6.5 Responsibilities.

H.6.5.1 On-Scene Field Supervisor's Responsibilities.

a. On-scene field supervisor will function as the Incident Commander (IC) and ensure adequate personnel and other resources are dispatched to respond to the scene or stage at an appropriate location. Supervisor will ensure the involved member is assigned a companion officer at the scene or other appropriate location.

b. Supervisor will assign an officer to transport the involved member to the Agency. If the involved member is transported to a medical facility for treatment, the supervisor will ensure a companion officer is assigned.

c. Supervisor will maintain security of the scene until relieved by the investigating body or another supervisor.

d. Complete the Patrol Supervisor Officer Involved Death/Life Threatening Injury Checklist.

e. Complete the initial incident report.

f. Collect supplemental reports from initial responding witness officers on scene about the incident or crime that precipitated the shooting, death, or life threatening injury.

g. Provide an incident briefing to the Shift Supervisor before being relieved as the IC.

H.6.5.2 Shift Supervisor.

a. The Shift Supervisor shall promptly respond and assume responsibility as the IC. If the shooting involves a field supervisor, the Shift Supervisor will designate who will assume the field supervisor's duties. The scene will be secured; including the scene perimeter, which will be marked by ribbon or rope, as appropriate. Shift Supervisor will ensure that the Patrol Supervisor checklist is being followed.

b. Make an initial determination as to whether the shooting is a force-related shooting. If it is, the Shift Supervisor will establish security until arrival of outside Criminal Investigation Agency. If the shooting is a non-force shooting, the CCPS/CCS will conduct the investigation. Incidents concerning death or serious injury to a person, but other than an officer-involved shooting, should be treated with similar investigative protocol as contained herein. Furthermore, the Shift Supervisor will be responsible for the following activities:

(1) Confirm all appropriate investigative and NASA personnel are notified and responding as required. Ensure the scene is secured consistent with public health and safety.

(2) Monitor the actions and demeanor of the involved member for signs of stress-related reactions.

(3) Separate all witnesses, including any involved members, before taking any statements. An attempt will be made to contact and identify all persons in areas deemed to be appropriate by the Shift Supervisor.

(4) Appoint officers to conduct a thorough search if all firearms rounds are not accounted for.

(5) Complete Shift Supervisor Officer Involved Death/Life Threatening Injury Checklist making all appropriate notifications.

H.6.5.3 Center Protective Services Civil Servant Investigator.

a. Responds to the scene.

b. Obtains briefing from on-scene commander.

c. Coordinates the needs of the crime scene security with the appropriate field supervisor.

d. If an injury or fatality occurred, assigns investigator or supervisor to act as liaison between the CCPS/CCS and outside Agency, if applicable. This assigned investigator's responsibilities are to coordinate and facilitate efforts with the outside Agency and to provide timely information to the CCPS/CCS.

e. If no injury occurred, assigns an investigator to investigate the incident.

f. Confirms or makes all required notifications.

H.6.5.4 CCPS/CCS and contractor Security Program Manager/Chief — Head of involved member(s) duty assignment (e.g., patrol, SRT, or investigations).

a. Coordinates activation of the Critical Incident Stress Debriefing (CISD) with Employee Assistance Program (EAP).

b. Schedules EAP psychological appointment before involved member(s) return to duty and completes Division Commander Employee Involved Death/Life Threatening Injury Checklist.

c. Verifies attendance — Upon receipt of written EAP clearance for duty, completes Return to Duty Memorandum.

d. Monitors the actions and demeanor of the involved member for signs of stress-related reactions.

H.7 Internal Review.

H.7.1 Review Mandatory — CSO will conduct an administrative investigation of all shooting incidents, regardless of whether a criminal case is established against the officer.

H.7.2 Non-Use of Force Investigation — If the incident is not handled as a criminal investigation, that is, if it is a no force shooting or an accidental discharge, CIU will have control of the scene and all other aspects of the case.

H.7.3 Information Release Prohibited — Center Protective Services will not release information from the administrative investigation to the criminal investigators.

H.8 Post-shooting Stress.

H.8.1 Debriefing — Critical Incident Stress Debriefing (CISD) will be mandatory for any involved officer who: (1) discharges a firearm resulting in any injury or death of a person, (2) receives any injury as a result of an assault with a firearm, or (3) is referred by a supervisor following any shooting incident. This debriefing is facilitated by NASA EAP.

H.8.2 Critical Incident Stress Management member (Peer Support) must attend the debriefing for support.

H.8.3 Three Days — CISD will be completed within three calendar days after the incident. No officer will be returned from administrative leave until this debriefing has occurred.

H.8.4 EAP — The officer's Division Commander will coordinate the scheduling of the psychological appointment with EAP.

H.9. Status.

H.9.1 Assignment — Member will be placed on administrative leave immediately by the CCPS/CCS, without loss of pay or benefits, pending the results of the investigation.

H.9.2 Limited Discussion — Member should not discuss the case with anyone except his attorney, union representative, state attorney, or other persons as authorized by the CCPS/CCS.

H.9.3 Criminal Charges — If the Office of the State/District Attorney or any other prosecutor files criminal charges or a grand jury indicts the member, the member will be relieved of duty in accordance with the current collective bargaining agreement and SOP.

H.10 Assistance by Agency.

H.10.1 NASA OPS and its contract partners will provide any assistance requested by the investigative body

.