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

a. Promoted;

b. Demoted;

c. Reassigned;

d. Converted from career-conditional to career tenure;

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

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

3.6.3. Reemployments.

3.6.3.1. Reemployments are not one of the general exceptions to the subject to investigation rule. When individuals are reemployed in Federal service, they must complete a new Declaration for Federal Employment (OF 306). They must also complete new investigative questionnaires (or update their prior form if the public trust or sensitivity level of their new position is the same as the old one). If suitability issues are admitted on the OF 306 or investigative questionnaire, or if they are otherwise developed, they must be investigated and adjudicated.

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

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

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

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

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

3.6.6. Change in Position Risk Level. All employees moving to a new position at a higher risk level than the risk level

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

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

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

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

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

3.7 Coding of Position Risk Level on Personnel Documents

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

The codes are:

RISK LEVEL	CODE
High	6
Moderate	5
Low	1

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

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

ACTION	LOW RISK POSITION	MODERATE RISK POSITION	HIGH RISK POSITION	PRP POSITION

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

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

3.9 Suitability Determination Procedures for NASA Federal Employees

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

3.9.2. As required by 5 CFR, Part 731, EO 10450, and FIPS 201, each prospective Federal employee must undergo an initial entry on duty (EOD) personnel security investigation to determine suitability for employment with the Federal Government. This investigation shall take place before appointment to a Government position or no later than 14 days after appointment.

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

in some instances, make them ineligible for Government employment.

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

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

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

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

3.9.6. Pre-appointment Checks for High Risk Positions.

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

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

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

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

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

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

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

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

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

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

Follow the requirements outlined in subparagraph 3.9.7.2.

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

3.10 Adverse Information

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

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

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

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

3.10.2. Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center counterintelligence office or the NASA Office of Security and Program Protection.

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

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

3.11 Reinvestigation Requirements

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

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

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

3.11.4. Positions involving participation in the MCSSPRP outlined in paragraph 3.5.6. shall be reinvestigated every 10 years or sooner for cause.

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

3.12 Recordkeeping

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

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

4.1 General

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

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

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

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

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

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

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

c. Upon expiration of the additional 5 working days, all issued temporary badges/passes and approved accesses will be terminated pending submittal of completed forms. Centers must establish the necessary procedures to ensure abuse of the visitor/temporary badging system does not occur.

4.2 Applicability

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

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

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

4.2.1.3. Require remote access to unclassified NASA IT Systems.

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

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

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

4.3 Responsibilities

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

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

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

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

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

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

c. Exercising appropriate risk management authority when investigative results have not been received in a timely fashion (normally within 90 - 120 days) requiring the need to make a decision to deny access, or grant interim or final access, as appropriate.

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

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

f. Making appropriate notifications for:

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

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

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

(1) Copies of all investigative results,

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

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

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

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

4.4 Designation of Security Risk Levels

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

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

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

4.4.3. The security risk level is determined by evaluating the sensitivity and risk of the work being performed and accesses required by the contractor and the potential for damage to NASA's mission and operations if performed inefficiently, ineffectively, or in an unsafe or unethical manner. Included in this is the requirement to properly identify and assign risk level designations for those individual positions directly involved in IT systems and/or application software development commensurate with the risk level that will ultimately be applied to the system and/or application when deployed. Section 4.6.2 and 4.6.5.1 is applicable.

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

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

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

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

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

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

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

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

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

4.5.5. All access factors (i.e., Center, facility, information, and IT systems) must be considered concurrently, as part of the overall risk designation process. This procedure serves to avoid duplication of effort by eliminating the possibility that a single individual could be assessed numerous times for different accesses. The intended result will be that the highest risk level designation (e.g., IT-6C = High Risk designated position compared against that same individual's need to access uncontrolled areas of the Center = Low Risk) is the designation for which the appropriate investigation will be conducted.

4.5.6. Position risk level determinations are inclusive of many factors. Generally, they are represented in the categories below:

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) Privileged access to IT systems whose misuse can cause "significant adverse impact" to NASA missions. These systems include those that interconnect with a NASA network in such a way as to enable the user to bypass firewalls or systems operated by a NASA contractor whose function and data has substantial value, even if these systems are not interconnected to a NASA network. (NOTE: Foreign Nationals (FN) are not authorized to have "Privileged" access to NASA IT Systems. The only exception is an FN who is involved in an international program or project under an International Space Act Agreement (ISAA). IT System Line Managers contemplating the granting of such access shall

consult with their Center Export Administrator and Center International Visit Coordinator (IVC) to ensure that an ISAA is in place, that the ISAA includes such a requirement, and that the international program or project involved certifies the need for such access.)

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

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

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

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

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

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

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

(1) Proprietary data:

(2) Privacy Act protected information:

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

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

(3) **Low Risk or 1C** positions are all IT system positions that do not fall in the categories above and includes all non-sensitive positions and all other positions involving IT Systems whose misuse has limited potential for adverse impact or sensitive data is protected with password and encryption. Low risk IT positions may involve:

(a) General word processing;

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

(c) Positions that provide for no privileged or limited privileged access or do not afford IT-1 or IT-2 access. Includes: Systems that contain Sensitive But Unclassified (SBU) as described in chapter 5, section 5.24. These requirements do not apply to NASA web-pages established for general public access. These web-pages are prohibited from containing classified information or NASA Sensitive But Unclassified (SBU), or providing unprotected links to NASA "Private" domains.

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

(2) NASA Mission Critical Space System Personnel Reliability Program (MCSSPRP)

(a) The MCSSPRP is mandated by 14 CFR Subpart 1214.5. The PRP, managed by the OSPP, is a tailored element of the overarching NASA personnel security program established to meet specific reliability requirements for persons whose principle duties, regardless of final risk level designation, fall within the following categories:

(b) Contractor personnel (including foreign nationals) occupying positions that involve unescorted access to mission-critical space systems areas, mission data, or mission-specific IT systems including those activities related to access to and/or manipulation of command and control systems of all NASA space-assets (e.g., shuttle, ISS, NASA satellites, other exploration vehicles, etc.), where inappropriate actions could result in damage and/or loss of the asset and/or critical data, or result in the loss of life and/or serious injury.

(c) Persons requiring unescorted access to Mission Essential Infrastructure (MEI) assets will be certified under the

MCSSPRP.

(d) Reliability determinations will consists of the following:

(1) Conduct of a personal background investigation consisting of a National Agency Check with inquiries (NACI), and local records checks (LRC), as appropriate.

(2) A review of personnel employment records.

(3) Completion and submittal of NASA Form 1734, "NASA PRP Investigative and Qualification Data Request" and review of the completed form, examination and certification by a NASA designated medical/psychiatric authority as to the individual's physical, mental, and emotional stability, and subsequent evaluations for cause only.

(4) Appropriate entry-on-duty screening, and subsequent entry into the contractor's random testing program, related to illegal drug abuse in accordance with EO 12564, "Drug Free Federal Workplace," and NPR 3792.1A, NASA Plan for a Drug-Free Workplace.

(5) Upon completion and submittal of NASA Form 1734, "NASA PRP Investigative and Qualification Data Request" contractor personnel (U.S. Citizen only) processed for a security clearance for access to classified national security information under Chapter 6, and whose investigation is within scope, are deemed qualified for PRP positions without additional investigation.

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

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

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

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

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

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

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

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

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

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

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

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

a. Non-U.S. citizens (including lawful permanent residents (LPR)) are eligible for placement in **Low** and **Moderate** risk positions, but are not normally eligible for employment in positions designated as **High Risk** . Under specific

situations the AA/OSPP may authorize the placement of a non-U.S. citizen for a specific **High Risk** position when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization shall submit a written request to the AA/OSPP via the CCS. The request shall:

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

(2) Define the individual's special expertise.

(3) Define the compelling reasons for the request.

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

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

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

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

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

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

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

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

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

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

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

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

4.7 Contractor Personnel Security Background Investigations Conducted by NASA

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

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

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

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

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

4.7.3. The timing of security form submittal and the estab , , lished risk level may d , ictate whether a proposed , NASA contractor employee can begin work prior to a final access de , , term ination. Based on the specifics of the situation

and a preliminary review of the submitted forms, the CCS shall advise the COTR whether the individual can commence working prior to the receipt of the completed investigation and final access determination.

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

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

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

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

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

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

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

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

4.8 Forms Required to Request an Investigation

ACTION	LOW RISK POSITION	MODERATE RISK POSITION	HIGH RISK POSITION	PRP POSITION
NON-NASA PERSONNEL	NACI/No Access SF 85 - e-QIP OFI Form 79B, FC 258	NACI/No Access SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization and Release of Credit Reports)	BI SF 85P - e-QIP FC 258, OFI Form 79B, NASA Form 1684 (Authorization and Release of Credit Reports)	NACI/No Access SF 85P-e-QIP FC 258, OFI Form 79B, NASA Form 1734, NASA Form 1684 (Authorization and Release of Credit Reports)

4.9 Adjudication Process for Access

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

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

4.9.1.2. In cases other than the Personnel Reliability Program (PRP), the CCS, or designee, shall make the final determination based on the results of the DSS investigation

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

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

? Voluntarily reported the information;

? Was cooperative, truthful, and complete during the investigation;

? Sought assistance and followed professional guidance;

? Resolved or appears likely to favorably resolve the concern;

? Has demonstrated positive changes in behavior and employment.

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

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

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

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

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

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

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

4.10 Escort Requirements in Lieu of Completed Favorable Background Investigations

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

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

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

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

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

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

(1) FN visitors, representatives, or FN contractor employees (including PRA's) from a non-designated country shall not be granted unescorted access privileges to NASA Centers after normal working hours unless specifically justified and

included in the Security/Technology Control Plan. See Appendix K for a Security/Technology Control Plan Template.

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

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

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

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

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

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

4.11 Adverse Information

4.11.1. When adverse information is developed or received in the course of any personnel security investigation or subsequent to such investigation and initial favorable determination, the scope of inquiry shall be expanded to the extent necessary to obtain sufficient information to make a determination that the contractor shall or shall not be (or continue to be) granted access to NASA facilities or IT systems.

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

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

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

4.11.2. Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center counterintelligence office or the NASA Office of Security and Program Protection.

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

4.12 Tenant Organization Employee and Contractor Reliability

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

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

4.13 Reinvestigation Requirements

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

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

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

4.13.4. Positions involving participation in the MCSSPRP will be reinvestigated every 10 years or sooner for cause.

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

4.14 Recordkeeping

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

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

5.1 General

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

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

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

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

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

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

5.2 Responsibilities

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

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

5.2.2.1. Establish Agency-wide procedures pertaining to the management of CNSI and material, and ACI generated by or in the custody of NASA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3 Agency Information Security Program Data Report, SF-311

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

5.4 Classifying, Marking, and Declassifying CNSI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.3. Marking for Original Classification.

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

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

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

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

5.4.4. Marking for Derivative Classification.

5.4.4.1. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a

classification guide issued by an original classification authority. Persons who apply derivative classification markings shall observe and respect original classification decisions, carry forward to any newly created documents the pertinent classification and declassification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward, the date or event for declassification that corresponds to the longest period of classification among the sources and a listing of the sources on or attached to the official file or record copy. Users can also use classification guides for derivative classifying. Center Security Office will be prepared to provide assistance as requested. The CCS will ensure they have access to the ISOO Marking Classified National Security Information Pamphlet www.archives.gov/isoo/ and other guidance.

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

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

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

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

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

5.4.7. Declassification and Downgrading.

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

5.4.7.2. The DSMD has developed the NASA Declassification Management Plan which provides the framework for NASA compliance with Section 3.3 through 3.7 of E.O. 12958, as amended. The NASA Declassification Plan will cover the following: Purpose, Legal Basis and Authority, 25 year Automatic Declassification, Systematic Declassification Review, Mandatory Declassification Review, Declassification Review Technique, RD/FRD review, Special Media Records, TS, TS/SCI, SAP Material review, Classification and Declassification Guides, Foreign Government Information, Declassification vs. Release, NASA Records Retention Schedule, NASA Handbook for Preparing Security Classification Guides, NASA Security Classification Guides, NASA Original Classification Authority, NASA Declassification Authority, Major Subject Matter/Equity Headings, Classification/Declassification Glossary, 25 year Automatic Declassification Exemptions, NASA Declassification Review and Referral Handbook, Review and Referral procedures, Declassification Authorities and NASA Staff contacts. NASA DCAs may only declassify NASA-originated classified national security information (CNSI).

5.4.7.3 An agency head may exempt from automatic declassification classified national security information, a group or file series "EXEMPT FILE SERIES" (A "file series" is also described in Information Security Oversight (ISOO) guidance as an "integral file block.") of records if the release of a substantial portion of the records within the file series

would be expected to remain exempt based on the provisions of E.O. 12958, as amended, Section 3.3. (b) and (c). E.O. 12958, as amended, Section 3.3. (d) states: At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) E.O. 12958, as amended, Section 3.3., that the agency proposes to exempt from automatic declassification. File series exemptions were approved by ISOO in 1996 pursuant to the E.O.12958, signed in April 1995, and did not have to be re-approved under E.O. 12958, as amended, signed in March 2003. File series exemption criteria include the following:

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

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

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

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

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

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

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

5.5 Access to CNSI

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

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

5.5.1.2. Have a justified need-to-know.

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

5.6 Accountability and Control of CNSI

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

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

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

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

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

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

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

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

5.6.4. Accountability records.

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

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

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

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

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

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

5.6.5. Top Secret disclosure records.

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

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

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

5.6.6. Exceptions from accountability.

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

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

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

5.6.7. Receipt of classified material.

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

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

5.6.8. Record of destruction.

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

5.6.8.2. A record of destruction is required for all CNSI material. The destruction record shall indicate the date the material was actually destroyed, the control number, the short title or a description of the material destroyed consistent with the description indicated in the control log, and the printed names and signatures of the official actually performing the destruction and a witness. Both individuals must have personal knowledge of the actual material destroyed. If applicable, the official authorizing the destruction shall also sign the record. Either the control log or a separate destruction report may be used for this purpose.

5.6.9. Inventory requirements.

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

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

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

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

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

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

5.6.10. Changes and corrections

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

5.7 Page Checks

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

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

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

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

Initial receipt	Yes
Page change	Yes

Change residue	Yes
Change of custodian	Yes
Inventory	No
Destruction	Yes

5.7.4. No page checks are required for Confidential material.

5.8 Working Papers

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

5.8.1.1. Dated when created.

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

5.8.1.3. Protected in accordance with the classification assigned.

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

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

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

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

5.8.2.3. Filed permanently.

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

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

5.9.2. Each Center shall apply the following:

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

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

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

5.9.2.4. Agency heads or any designee may prescribe special provisions for the dissemination, transmission,

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

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

b. Limit the number of individuals who receive it

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

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

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

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

1. A description of the disclosed information

2. Who authorized the disclosure

3. .To whom the information was disclosed

4. How the information was disclosed and transmitted

5. Reason for the emergency release

6. How the information is being safeguarded

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

5.10 Reproduction of CNSI

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

5.10.1.1. Protect classified information during reproduction.

5.10.1.2. Adequately clear equipment after reproduction.

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

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

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

5.11 Hand Carrying and Receipting of Classified Material

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

5.11.2. Methods of Transportation within a Center.

5.11.2.1. The TSCO, custodian, or other employee having a Top Secret clearance and designated by either TSCO or the

CCS, shall personally hand-carry Top Secret information within a Center. A Top Secret Cover Sheet (Form SF 703) shall be attached to all Top Secret information in document form.

5.11.2.2. When traveling within a building or between buildings on a Center, classified material shall be hand carried covered with the appropriate coversheet and enclosed in a single envelope or other suitable package marked with the highest classification or carried in a briefcase or other container. When hand carrying classified material, the individual shall proceed directly to the intended destination. Restroom breaks, coffee breaks, etc., are not permitted when hand carrying classified material.

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

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

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

5.11.3. Hand Carrying Outside a Center.

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

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

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

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

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

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

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

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

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

5.12 Transmission of Classified Material

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

5.12.1.1. Classified material shall be transmitted either in the custody of an appropriately cleared individual, by an

approved system or courier, or otherwise in accordance with the provisions of this chapter.

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

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

5.12.2.1. Defense Courier Service (DCS).

5.12.2.2. Department of State Courier System.

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

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

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

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

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

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

5.12.3.5. When an urgent requirement exists for overnight delivery within the 50 United States and its Territories, the Center Director may authorize the CCS to use Federal Express (FedEX) for overnight delivery of material for the Executive Branch. The sender is responsible for ensuring that an authorized person shall be available to receive the delivery. The package may only be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of street-side collection boxes is prohibited. COMSEC, NATO, and foreign government information (FGI) shall not be transmitted in this manner.

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

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

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

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

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

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

5.12.4.2. USPS registered mail for:

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

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

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

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

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

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

5.13 Release of Classified Information to Foreign Governments

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

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

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

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

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

5.14 Receipt System

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

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

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

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

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

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

5.15 Managing and Handling COMSEC Material

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

5.16 Defense Courier Service Reimbursement Program

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

5.17 Disposition or Destruction of Classified Material

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

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

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

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

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

5.17.6. Unclassified material, including formerly classified material that has been declassified, unclassified messages,

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

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

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

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

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

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

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

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

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

5.18 Destruction Procedures

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

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

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

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

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

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

5.18.2.5. Completing and signing all appropriate records of destruction.

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

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

5.19 Security Violations and Compromise of CNSI

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

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

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

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

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

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

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

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

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

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

1. Type of report:

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

2. Type of incident:

a. Compromise or Possible compromise;

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

b. Administrative Discrepancy;

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

3. Complete identification of all material involved including;

a. Unclassified title
b. Classification
c. Originator

4. Identity of all personnel involved including;

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

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

a. Fiscal year
b. Sequential number

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

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

5.20 CNSI Meetings and Symposia

5.20.1. General

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

5.20.2. Responsibilities

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

the Office of External Relations regarding the attendance of any foreign nationals or representatives at a CNSI symposium or meeting.

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

5.20.3. Minimum Standards

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

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

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

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

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

5.21 Security Container, Vault, and Strong Room Management

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

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

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

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

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

c. Custodian/Alternate custodian.

d. Highest classification level of information stored.

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

5.21.1.4. Ensure high value items that are targets of theft such as funds, weapons, and precious metal are not to be stored in the same drawer as classified materials.

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

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

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

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

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

b. When the locking system requires replacement.

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

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

5.22 Classified Material is NOT Personal Property

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

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

5.23 Security Classification Reviews for NASA Programs and Projects

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

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

b. Complete NASA Form 1733 **,** **"** Information and Technology Classification and/or Sensitivity Level Determination Checklist."

c. Include the Form 1733 as permanent program documentation and in any procurement related documentation.

5.23.2. Upon the conclusion of the security review, if the information surrounding or concerning the program of project, or portions thereof, meet one or more of the categories of information presented in the executive order, a Subject Matter Expert (SME) must develop an appropriate Security Classification Guide (SCG). The SME and project officials shall consider the level of classification needed for specific information. NOTE: See chapter 10 for a definition of an SME. There are three levels of classified national security information: Top Secret, Secret, and Confidential. Chapter 10 provides a definition of each. Subject matter experts (SME) must be able to specifically identify what particular information is under consideration for classification. The SME, weighing the information being protected against the definitions in chapter 10, shall provide a recommendation to the Office of Security and Program Protection (OSPP) as to what level the information must be classified (Top Secret, Secret or Confidential) and how long the information must be kept classified. Duration of classification shall be considered within the following guidelines:

a. The SME shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity and shall assign such date or event as the declassification instruction.

b. If unable to determine a date or event of less than 10 years, the SME shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

c. If unable to determine a date or event of 10 years, the SME shall assign the declassification date not to exceed 25 years from the date of the original classification decision.

5.23.2.1. All SCGs must be approved by the OSPP. The DSMD shall assist program and project managers in the development of SCGs.

5.23.2.2. The OSPP will establish and maintain a central repository for all NASA originated SCGs and declassification guides, and shall provide a sequential numbering schema for all SCGs and declassification guides both classified and unclassified. The OSPP will also obtain and maintain SCGs and declassification guides from other agency programs in which NASA is working or supporting.

5.23.2.3. The SCG must be reviewed for updating every 5 years.

5.23.2.4. Upon completion, termination, or cancellation of a program or project, a declassification guide must be produced to provide the necessary requirements for declassifying the project information. The declassification guide must be approved by the OSPP.

5.23.2.5. The " *NASA Handbook for Writing Security Classification Guides* " provides requirements and guidance for the creation of a SCG.

5.23.3. If information surrounding or concerning the program or project is considered to be unclassified, a letter of transmittal shall be produced that reflects this determination. The original letter shall be maintained by the Project Office, with copies sent to the Mission Directorate Office having responsibility for the project or Center and to the DSMD.

5.23.4. If information surrounding or concerning the program or project is considered to be SBU, the information shall be managed as prescribed in section 5.24 of this NPR.

5.23.5. All CNSI and SBU information should be reviewed by a Record Manager, the responsible Program Manager or head of the office and a Declassification Authority (DCA), if the information is classified, to determine the disposition of the records before they are sent to the Federal Records Center (FRC) or the National Archives and Record Administration (NARA) for temporary or permanent storage.

5.24 Sensitive But Unclassified (SBU) Controlled Information

The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

5.24.1. With the exception of certain types of information protected by statute, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency. Therefore, NASA has determined that official information and material of a sensitive but unclassified (SBU) nature that does not contain national security information (and therefore cannot be classified) shall be protected against inappropriate disclosure by designating and handling such information as SBU in accordance with the procedures set forth in this NPR. See also the definition of Sensitive Information/Material in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

5.24.1.1. Information, regardless of its form (digital, hard-copy, magnetic tape, etc.), the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests is designated as SBU to control or restrict its access. Information designated as SBU shall be afforded appropriate protection sufficient to safeguard it from unauthorized disclosure.

5.24.1.2. Within NASA and the Federal Government, such information had previously been designated "FOR OFFICIAL USE ONLY." This designation was changed at NASA to "Administratively Controlled Information" for clarity and to more accurately describe the status of information to be protected. However, recent efforts to apply consistent terminology across multiple federal agencies have prompted NASA to change the designation to "Sensitive but Unclassified." Therefore the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)" will be used to identify sensitive

but unclassified information within the NASA community when that information is not otherwise specifically described and governed by statute or regulation. The use of caveats other than SBU will be governed by the statutes and regulations issued for the applicable category of information.

5.24.1.3. The SBU designation and procedures set forth herein do not apply to the information, reports, or analysis by members of other agencies or departments who are members of the National Intelligence Board (NIB), who are on loan to NASA, and whose authorities are derived from other sources. However, SBU designation and procedures shall be applied when such information, or portions thereof, is copied for dissemination within NASA.

5.24.2. Identification of SBU Information. The failure to sufficiently identify information that requires protection from disclosure may result in increased risk to life or mission essential assets, damage to official relationships, monetary or other loss to individuals or firms, or embarrassment to NASA.

5.24.2.1. The originator of information, or the official approving its dissemination, must review the information for possible designation as SBU prior to its use. In general, information to be designated as SBU falls into one of the 3 categories described below. The criteria of at least one of the following subparagraphs must be met to designate the information as SBU:

a. Information originated within or furnished to NASA that falls under one or more of the exemption criteria of the Freedom of Information Act (5 U.S.C. §552). However, designating information as SBU does not represent that the information has been determined to be exempt from disclosure under FOIA. Requests under FOIA, for information designated as SBU, will be reviewed and processed in the same manner as any other FOIA request.

b. Information exempt or restricted from disclosure by statute, regulation, contract, or agreement. The following are examples of such information.

(1) Information subject to export control under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR)

(2) Information disclosing a new invention in which the Federal Government owns or may own a right, title, or interest.

(3) Proprietary information of others provided to NASA under a nondisclosure or confidentiality agreement.

(4) Source selection and bid and proposal information.

(5) Small Business Innovative Research Data, Limited Rights Data, and Restricted Computer Software received in performance of NASA contracts.

(6) Information developed by NASA under a Space Act agreement and subject to section 303(b) of the Space Act (42 U.S.C. 2454(b)).

(7) Information concerning or relating to private entity trade secrets or confidential commercial or financial information received by a NASA employee in the course of government employment or official duties.

(8) Information subject to the Privacy Act of 1974 (5 U.S.C. §552a)

c. Information that is determined by a designated NASA official to be unusually sensitive (refer to paragraph 5.22.5. for decontrol provisions). The following are examples of such information.

(1) Predecisional materials such as national space policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries

(2) Geological and geophysical information and data, including maps, concerning wells.

(3) Center maps and/or plain text documents describing locations/directions (e.g., latitude, longitude, depth, etc.) of underground utility conduits (e.g., sewers, gas, data, communications, etc.).

(4) Drawings and specifications that identify existing or proposed security measures for mission essential infrastructure designated assets or other key resources

(5) Mission specific security plans that identify protective measures and procedures for assets that are sensitive in nature but are not classified. (Example: Payloads that utilize special nuclear materials, payloads that contain certain animal experiments, and STS missions, as determined by the CCS, etc.)

(6) Emergency contingency or continuity of operations plans that provide detailed information regarding emergency response processes and procedures that, if publicized, could give a potential adversary vital information with which to

thwart or compromise emergency response efforts.

(7) Sensitive scientific and technical information (STI) (See NPD 2200.1 and NPR 2200.2 for requirements for documentation, approval, and dissemination of NASA STI).

(8) Information that could result in physical risk to personnel.

(9) NASA information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models.

(10) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.

(11) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(12) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

(13) Developing or current technology, the release of which could hinder the objectives of NASA, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

5.24.2.2. Information identified in paragraphs a. and b. below that has designation and protection criteria established by other statutes, regulations, NASA directives, etc., shall be protected and marked in accordance with those applicable directives.

a. Information or material that may already have individual, officially designated identification, protection, or management requirements (e.g., FAR, FOUO, Export Control, FOIA, STI), and/or established markings on the sheet(s) will be controlled in accordance with their respective requirements. However, for the purpose of uniformity and consistency, physical protection and disclosure requirements established for the broader spectrum of SBU will still apply.

b. Information exempted from disclosure by treaty, statute (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulation (ITAR), and Section 303(b) of the Space Act), or other agreements.

5.24.2.3. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to SBU. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for SBU as provided in this document. Should the additional guidance be less restrictive than in this document, the information will be safeguarded in accordance with this NPR.

5.24.2.4. Information shall not be marked or designated as SBU if it does not meet the criteria in paragraph 5.24.2.1.

5.24.2.5. New material derived from documents marked SBU shall carry forward the control marking, if any, from the source documents.

5.24.3. Marking for SBU

Information designated as SBU will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of SBU markings on information known by the holder to be SBU does not relieve the holder from safeguarding responsibilities. Where the SBU marking is not present on information known by the holder to be SBU, the holder of the information will protect it as SBU. Information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with such guidance need not be additionally marked SBU. If there is no specific guidance or marking requirements, information designated SBU will be marked as follows:

a. Prominently mark the top and bottom of the front cover, first page, title page, back cover and each individual page containing SBU information with the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)."

b. Materials containing specific types of SBU information may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It is to be controlled, stored, handled, transmitted, distributed, and disposed* of *in accordance with NASA policy relating to SBU information. This information shall not be distributed beyond the original addressees without prior authorization* of *the originator.*

c. SBU information being transmitted to recipients outside of NASA, for example, other federal agencies, state or local officials, NASA contractors, etc., shall include the following additional notice:

WARNING: *This document is SENSITIVE BUT UNCLASSIFIED (SBU) . It contains information that may be exempt from public release under the Freedom of Information Act* (5 *U.S.C.* 552) or other applicable laws or restricted from disclosure based on NASA policy. *It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have* a *valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).*

d. Computer storage media, i.e., disks, tapes, removable drives, memory sticks, etc. containing SBU information will be marked "SENSITIVE BUT UNCLASSIFIED."

e. Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only SBU information will be marked with the abbreviation (SBU).

f. Individual portion markings on a document that contains no other designation are not required.

5.24.4. Responsibilities.

5.24.4.1 Officers and employees designating information or materials as SBU and those receiving materials so marked shall be responsible for properly safeguarding the information contained therein. These individuals will:

a. Comply with the safeguarding requirements for SBU information as outlined in this document.

b. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding SBU and other sensitive information and the penalties that could result in unauthorized disclosure of SBU information.

c. Keep the number of copies of SBU information to a minimum.

d. Require that all individuals performing work for NASA (contractors, consultants and other persons not employed directly by NASA) execute a NASA Form (TBD), "Sensitive But Unclassified Information Non- Disclosure Agreement (NDA)," as a condition of access to SBU information. Other individuals not assigned to, employed by or performing work for NASA, but to whom access to SBU information will be granted, may be required to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

5.24.4.2. Supervisors and managers will:

a. Ensure that an adequate level of education and awareness is established and maintained to emphasize safeguarding and preventing unauthorized disclosure of SBU information.

b. Ensure that an adequate level of education and awareness is established and maintained to emphasize that disclosing SBU information without proper authority could result in administrative or disciplinary action, fines and/or imprisonment.

c. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when unauthorized disclosures of SBU information occur.

5.24.5. Decontrol Provisions. Officers and employees designating information or materials as SBU shall be held responsible for their continued review and the prompt removal of such designations and restrictive markings when the necessity no longer exists. Authority to decontrol such material and any copies is limited to the official who initially designated the material as SBU, a successor or superior, or an official of an office having primary interest in the material. The following procedures apply:

5.24.5.1. The control status of any information or material designated as SBUshall be reviewed upon request by an

individual or individuals to whom disclosure has been restricted. Such material shall be decontrolled and disclosed unless the office of origin or the office of primary interest determines, within a reasonable period of time after the request and after consultation with legal counsel, that the information must remain protected against disclosure. The existence of an SBU marking does not necessarily make information exempt from disclosure. A determination that information is exempt from disclosure must be based on the applicability of some legal authority. Consultation with the Office of the General Counsel at Headquarters or Center Office of Chief Counsel is required.

5.24.5.2. The restrictive marking on information designated as SBU in accordance with paragraph 5.24.2.1. shall be immediately removed when the need for protection no longer exists, (e.g., imminent public release, transfer to records archives, implementation of organization plan, or conclusion of sensitive travel).

5.24.6. Storage, Access, Disclosure, Protection, Transmittal, and Destruction of SBU. The minimum requirements for storage, access, protection, transmittal, and destruction of SBU information is provided in section 5.24.6.1 through 5.24.6.5, respectively. However, some types of SBU information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this NPR. For example, certain types of information may be considered extremely sensitive based on the consequences of an unauthorized release. Such consequences could be increased risk to life or mission essential assets, damage to official relationships, or embarrassment to NASA. Additional control requirements may be added as necessary to afford appropriate protection to such information. NASA employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

5.24.6.1. Storage. Employees who handle information or material designated SBU shall ensure the proper safeguarding of such information by limiting its access to authorized persons only and by storing it in cabinets, desks, or other containers, or securing it within an individual office area when not in use. Access to SBU information is on a "need to Know" basis in accordance with section 5.24.6.2.

a. When unattended, SBU information will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. SBU information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

b. SBU information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When SBU information is stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

c. IT systems that store SBU information will be certified and accredited for operation in accordance with federal and NASA standards. Consult the NPR 2810.1, Security Information Technology, for more detailed information.

d. Laptop computers and other media containing SBU information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with NPR 2810.1.

5.24.6.2. Access and Disclosure. SBU information of which NASA or a NASA contractor is the originator may disclosed to any Federal Government employee or contractor who has a demonstrated "need-to-know" in connection with official duties. When NASA is not the originating agency, SBU information may be disclosed only with authorization from the originating or designated action agency. Whenever SBU information is disclosed, the recipient must be made aware of the following restrictions on access and disclosure:

a. In no case shall SBU information be disclosed - orally, visually, or electronically - unless the disclosure is clearly in accordance with existing law and Agency regulations or policy directives and is in the best interest of NASA.

b. Access to SBU information is based on "need-to-know" as determined by the holder of the information. When discussing with or transferring SBU information to another individual(s), the holder of the information must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, or from observing or otherwise obtaining the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his/her next-level supervisor or the information's originator.

c. A security clearance is not required for access to SBU information.

d. SBU information may be shared with other agencies, federal, state, tribal, or local government and law enforcement

officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where SBU information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable NASA program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The NASA program office shall then determine if it is appropriate to release the information to the other a , gency official. (See section 5.24.3 for marking requirements)

e. When NASA is not the originating agency, further dissemination of SBU information by the holder of the information may be made only with authorization from the originating or designated action agency. When information requested or to be discussed originated with another agency, the holder of the information must comply with that originating agency's policy concerning third party discussion and dissemination.

,

f. The holder of the SBU information will comply with any access and dissemination restrictions cited on the material, provided with the material, or verbally communicated by the originator. Sensitive information protected by statute or regulation, i.e., Privacy Act, Critical Infrastructure Information, etc., will be controlled and disseminated in accordance with applicable guidance for that type of information. Where no guidance is provided, handle SBU information in accordance with the requirements of this NPR

g. NASA IT Systems containing SBU shall be appropriately protected from unauthorized access. Access shall be granted only after the requisite security investigation, as outlined in chapters 3 or 4 of this NPR, has been accomplished. In addition, access provisions for FIPS 199 Security Category Moderate shall apply.

h. When discussing SBU information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

5.24.6.3. Protection. When materials marked SBU are prepared for dissemination or forwarded to any locations/persons (within or outside a NASA Center), they must be protected using NASA Form 1686, "SENSITIVE BUT UNCLASSIFIED" (SBU) cover sheet. Users shall check appropriate boxes on the form to signify what type of SBU information is contained in the document.

a. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal SBU information to unauthorized persons, a SBU cover sheet (NASA Form 1686) will be used to prevent unauthorized or inadvertent disclosure.

b. When disclosing, disseminating, or transmitting SBU information, a SBU cover sheet, (NASA Form 1686), should be placed on top of the transmittal letter, memorandum, or material.

c. When receiving SBU equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this NPR.

5.24.6.4. Transmittal. Transmission of SBU information may be made via first class mail, courier, encrypted e-mail, encrypted FTP, encrypted HTTP, or secure fax to known recipients. All transmissions of SBU information require a SBU cover sheet (NASA Form 1686) be transmitted with the information. Additionally, the holder of the SBU information will comply with any access, dissemination, and transmittal restrictions cited on the material, provided with the material, or verbally communicated by the originator.

a. Transmission of hard copy SBU information within the U.S. and its Territories:

(1) Material containing SBU information will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(2) Material containing SBU information may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(3) Material containing SBU information may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

b. Transmission of hard copy SBU information to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, SBU may be transmitted directly to the office. Where the overseas office is not serviced

by a military postal facility, the SBU information will be sent through the Department of State, Diplomatic Courier.

c. Electronic Transmission.

(1) Transmittal via fax. The use of a secure fax machine is highly encouraged. However, unless otherwise restricted by the originator, SBU information may be sent via nonsecure fax. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the SBU information faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

(2) Transmittal via E-Mail, FTP, and HTTP (Web)

(i) SBU information transmitted via email, FTP, web, etc., should be protected by encryption or transmitted within secure communications systems. If it is not possible to transmit SBU via appropriately encrypted channels, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of SBU information will comply with any email or other electronic transmission restrictions imposed by the originator.

(ii) Due to inherent vulnerabilities, SBU information shall not be sent to personal email accounts.

(3) NASA Internet/Intranet

(i) SBU information will not be posted on a public NASA website or any other public website.

(ii) SBU information may be posted on the NASA Intranet or other government controlled or sponsored protected encrypted data networks. However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular Intranet site. The official must determine the nature of the information is such that need-to-know applies to all such personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as SENSITIVE BUT UNCLASSIFIED; and information posted does not violate any provisions of the Privacy Act or other applicable laws.

5.24.6.5. Destruction. SBU information or material that cannot be decontrolled per paragraph 5.24.5 or which is no longer needed shall be removed from IT systems, shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure. Destruction may be accomplished by:

a. "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing, or non-recoverable encrypted deletion. Contact local IT security personnel for additional guidance.

c. Paper products containing SBU information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

5.24.6.6. Disposal of IT Systems Containing SBU. Refer to NPR 2810.1 for procedural requirements regarding clearing of hard drives, blackberries, personal digital assistant (PDA's), and other storage mediums, prior to disposal or recycling.

5.24.7. Incident Reporting. The loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will be reported. Incidents involving SBU in NASA IT systems will be reported to the center IT Security Manager in accordance with IT incident reporting requirements in NPR 2810.1.

5.24.7.1. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the NASA Center Chief of Security.

5.24.7.2. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information will report it immediately, but not later than the next duty day, to the originator and the Center Chief of Security.

5.24.7.3. Additional notifications to appropriate NASA management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5.24.7.4. At the request of the originator, an inquiry will be conducted by the center security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender

5.24.8. Administrative Violations and Sanctions.

5.24.8.1. All NASA employees, as well as non-employees, who have access to SBU are responsible individually for complying with the provisions of this NPR and may be subject to administrative sanctions if they disclose information designated SBU without proper authorization.

5.24.8.2. Sanctions include, but are not limited to warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, and/or discharge.

5.24.8.3. Such sanctions may be imposed, as appropriate, upon any person determined to be responsible for a violation of disclosure restrictions in accordance with applicable law and regulations, regardless of office or level of employment.

5.25 Use, Protection, and Accountability of Department of Energy (DoE) Unclassified Controlled Nuclear Information (UCNI)

5.25.1. Use.

5.25.1.1. UCNI is sensitive unclassified Government information concerning nuclear material, weapons, and components, whose dissemination is controlled under section 148 of the Atomic Energy Act.

5.25.1.2. It is to be accessed only by personnel with a need-to-know.

5.25.1.3. Foreign Nationals are not authorized access without approval of DoE.

5.25.2. Protection.

5.25.2.1. UNCI must be stored to prevent unauthorized disclosure. Securing in a locked room, file cabinet, or desk drawer is the minimum requirement.

5.25.2.2. UCNI may be reproduced.

5.25.2.3. Use of encryption is mandatory for electronic transmission.

5.25.2.4. Use of a Secure Telephone Unit (STU III) or Secure Telephone Equipment (STE) is mandatory whenever conversations involving UCNI are necessary.

5.25.3. Accountability.

5.25.3.1. Organizations using UCNI shall designate in writing a Reviewing Official responsible for reviewing created NASA correspondence, reports, and related materials for the presence of UCNI and ensuring the appropriate marking per DoE policy.

5.25.3.2. All copies of UCNI must be periodically inventoried to ensure appropriate accountability.

5.25.3.3. Unneeded copies shall be destroyed by burning or shredding.

Chapter 6. Industrial Security

6.1 General

6.1.1. This chapter provides procedural requirements for implementation of industrial security requirements in accordance with the National Industrial Security Program Operating Manual (NISPOM) and the NISPOM Supplement.

6.1.2. It pertains to, but is not limited to, the requirement to review all programs/projects in accordance with Chapter 5, subparagraph 5.25.1, classified contract administration and the processing and control of classified visits for cleared Government and contractor employees.

6.1.3. The processing and control of classified and unclassified visits to a Center in relation to classified contracts is the responsibility of the CCS and shall be covered in written local security procedures tailored to that Center.

6.2 Department of Defense (DoD) Support

6.2.1. Currently, the DoD, through the Defense Security Service (DSS), acts on behalf of NASA in providing industrial security services for most NASA classified contracts.

6.2.2. The standard security provisions of NASA classified contracts require the contractor to obtain a facility security clearance and be assigned a Cage Code, execute a DoD Security Agreement (DD Form 254), and complete other applicable industrial security forms that require the contractor to comply with the NISPOM for industrial security matters.

6.2.3. NASA exercises the right to inspect contractor operations located on NASA property that are involved in access to and safeguarding classified information.

6.3 Scope

This chapter pertains to contracts, grants, cooperative agreements, and other binding transactions in which performance shall require access to CNSI by the contractor, supplier, grantee, or its employees. It does not apply to agreements with other Federal agencies.

6.4 Responsibilities

6.4.1. NASA program or project management personnel contemplating offers or quotations for a classified contract, negotiating or awarding a classified contract, or bearing responsibility for the performance of a classified contract will:

6.4.1.1. Ensure the CCS is fully engaged in supporting the development of security requirements for the contract.

6.4.1.2. Ensure adequate resources are provided to the CCS for program security oversight, as required.

6.4.1.3. Per the NISPOM, ensure the contractor provides a "Classified Visit Request" to the CCS and updates the list, as appropriate.

6.4.2. The Director of Procurement of each Center is responsible for the following:

6.4.2.1. Ensuring that the request for proposals or offers includes a statement that the contractor or prospective contractor shall or shall not require access to classified information and shall or shall not generate classified information in the performance of such contract. If the contract shall involve access to classified information or cause the generation of classified information, a letter as discussed in paragraph 2305.1 of the NISPOM shall be attached to the material submitted to the individual negotiating the contract.

6.4.2.2. Ensuring that each classified contract contains the standard security clauses prescribed by Section 4.404(a) of the Federal Acquisition Regulation, and NASA Supplement 1804.404-70.

6.4.2.3. Ensuring that any proposed deviation in this standard security provision (e.g., elimination, addition, or substitution) is forwarded to the Office of Procurement for approval by the Assistant Administrator for Procurement, with concurrence by the AA/OSPP and the OGC.

6.4.3. The CCS shall ensure that NASA recommendations affecting the contractor's security program are made primarily through the cognizant security office (Defense Security Service) for the contractor concerned, since that office is primarily responsible for ensuring that the contractor complies with all security recommendations. When it becomes apparent that full and satisfactory action on a specific NASA recommendation has not been taken by the cognizant security office or by the contractor, a detailed report of the circumstances shall be forwarded to the AA/OSPP for appropriate action with a copy to the contracting officer (CO).

6.4.4. All changes to a contractor's security program that may affect the cost, performance, or delivery of the contract must go through the contracting officer (CO) for the processing of a contract modification.

6.4.5. Through coordination with the CO and Contracting Officer's Technical Representative (COTR), the CCS shall develop local written security procedures to ensure that the following requirements are met:

6.4.5.1. All DD Form 254s, Contract Security Classification Specification, shall be completed by the procurement officer with the assistance of the security office. The completed form shall then be signed by the CCS or designated security representative. Additionally, the following is applicable to a DD Form 254 for NASA contracts:

6.4.5.2. In item 12 of the DD Form 254, delete the words: "To the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review in accordance with the Industrial Security Manual," and insert the words: "To the Office of Public Affairs, National Aeronautics and Space Administration, Washington, DC 20546, for review."

6.4.5.3. In the case of prime contracts, the Public Information Office of the NASA contracting Center shall also be specified in item 12 to indicate that proposed publicity releases shall be submitted through that office to the Office of Public Affairs, NASA, Washington, DC 20546.

6.4.5.4. In the case of subcontracts, the publicity office of the prime contractor shall be specified, in addition to the Public Information Office of the NASA Contracting Center, to indicate that proposed publicity releases shall be submitted through those two offices to the Office of Public Affairs, NASA, Washington, DC 20546.

6.4.5.5. The Chief, Headquarters Security Office shall perform these responsibilities for Headquarters contracts.

6.4.5.6. A signed copy of each DD Form 254 shall be forwarded to the DSMD.

6.4.6. The CCS shall ensure contractors operating under a DD Form 254 provide the appropriate "Classified Visit" documentation, per the NISPOM, on all "cleared" contractor personnel working under the DD Form 254 and ensure updates are provided on an as need basis. Classified Visit Requests are mandatory for all NASA Classified Contracts.

6.5 Suspension, Revocation, and Denial of Access to Classified Information

6.5.1. Occasionally, Center security offices may find it necessary to take action to suspend, revoke, or deny a NASA contract employee access to CNSI or to suspend operation of the entire contract. To ensure uniformity and consistency, the following shall apply:

6.5.2.. Only the AA/OSPP or designee may deny or revoke a cleared contractor's access to classified information.

6.5.3. The AA/OSPP, DSMD, or CCS may grant interim and final access or suspend access for cleared contractor personnel, as necessary.

6.5.4. The AA/OSPP, Center Director, CCS, or the DSMD shall suspend a contractor's access for cause.

6.5.4.1. Each action shall be fully documented. Information developed during the security inquiry shall not be shared with the Contracting Officer or contractor management while the inquiry is ongoing. The DSMD or CCS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, or is a threat to a critical mission, or may otherwise be ineligible for continued access to classified information.

6.5.4.2. Center security officials shall ensure coordination is effected with the local or regional Industrial Security investigative organization (OPM, DSS, DIS) to obtain direction and to ensure information is provided to enable them to properly adjudicate for continued clearance eligibility.

6.5.4.3. During the investigative and adjudicative process, all reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

6.5.5. The CCS shall propose denials and revocations of contractor access to the AA/OSPP. The AA/OSPP shall make final denial or revocation determinations after consultation with the NASA CAF and the OGC.

6.5.6. Subjects of adjudication must be allowed to review and refute any information developed during the investigation process which shall make him or her ineligible for access to NASA CNSI, unless release of that information jeopardizes national security.

6.6 Periodic Review of DD Form 254

6.6.1. Each approved DD Form 254, Contract Security Classification Specification, or other written notification, issued in lieu thereof, shall be reviewed at least annually by CCS with the assistance of the procurement office.

6.6.2. The individual(s) responsible for this review shall be identified by the CCS in local written security procedures.

6.6.3. When a change is made in a security classification specification pertaining to a prime contract, that change shall be reflected in all applicable Form DD 254s, or other classification documents pertaining to subcontractors.

Chapter 7: Physical Security Program

7.1 Security Control at NASA Centers

7.1.1. Each Center shall apply and maintain appropriate physical security measures necessary to provide for protection of persons and property.

7.1.2. Positive entry controls shall be implemented at all entry points to the Center and individually designated security areas and facilities, as deemed necessary, to preclude unauthorized access to critical areas, information, or personnel.

7.1.3. Procedures shall be established to ensure only authorized personnel are admitted to NASA Headquarters and field Centers.

7.2 NASA Photo-Identification (Photo-ID) Badge Program

7.2.1. NASA currently employs an Agency-specific employee photo-ID badge or Center-specific visitor pass to ensure only properly authorized personnel are granted access to NASA Centers, facilities, and other resources.

7.2.2. The CCS shall develop and monitor local procedures pertaining to the issuance, utilization, control, and accountability of the NASA Photo-ID badge and any Center-specific visitor passes.

7.2.2. NASA photo-ID badges are color-coded to designate the following categories of personnel, as specified in Appendix I, NASA Photo-Identification Standards. These photo-ID badges are required as official identification for entry to NASA facilities:

7.2.2.1. NASA civil service

7.2.2.2. NASA non-appropriated fund employees

7.2.2.3. Consultants/contractors

7.2.2.4. Other Federal agency employees and military personnel detailed to NASA

7.2.2.5. COOP students, summer students

7.2.2.6. Appropriately accredited members of the press

7.2.2.7. Foreign national visitors and contractor employees from designated and non-designated countries. Includes lawful permanent residents (LPR).

7.2.3. Security clearance status shall not be designated by any device, color, or code on any NASA photo-ID.

7.2.4. The NASA photo-ID issued to NASA civil service employees and other Federal agency and military detailees shall be honored for access to NASA Headquarters and all NASA Centers.

7.2.5. NASA photo-ID badge system databases shall be designated "sensitive unclassified information" and protected as ACI.

7.2.6. At a minimum, a favorable review; conducted by center security personnel, of submitted investigative documentation (e.g., SF 85, SF 85P, SF 86, NASA Form 531, etc.) is required for issuance of the NASA photo-ID to authorized NASA civil service, NASA contractor, and tenant organization personnel. See chapters 2, 3 & 4 for specific investigative requirements.

7.2.7. Issued NASA photo-ID badges or visitor passes shall be properly displayed and worn at all times while bearer is on a NASA Center or Component Facility. They shall be worn:

7.2.7.1. Above the waist on the outermost garment.

7.2.7.2. Photo-side visible.

7.2.8. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, etc.) on the NASA photo-ID (or any alteration or modification thereof) is not authorized.

7.2.9. The NASA photo-ID is not personal property. It is the property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued NASA photo-ID's; immediately reporting the loss or false use of a NASA photo-ID; challenging unbadged personnel; notifying the CCS of a name change; properly displaying the badge when on Center; and surrendering the NASA photo-ID upon resignation or retirement, or upon the direction of the issuing authority.

7.2.10. NASA Retiree ID Card. The Center HR Office shall initiate the request for the NASA Retiree ID Card only for those NASA Civil Service employees who have retired under favorable conditions (e.g., instances other than retired in lieu of termination for cause, etc.). The issuance and use of the NASA Retiree Card is a privilege that may be denied or revoked at any time for cause.

7.2.10.1. The NASA Retiree photo-ID Card is valid at any NASA Center and when presented along with another appropriate form of photo-identification shall be used to obtain a visitor pass to enter the Center.

7.2.10.2. Access shall normally be restricted to business hours only, unless after hours access is "sponsored" and monitored by a Center employee.

7.2.10.3. All Center procedures and controls for visitor pass and visitor access, to include escorting, shall be observed as appropriate.

7.2.11. Forging, falsifying, or allowing misuse of a NASA Photo-ID or other forms of NASA identification in order to gain unauthorized access to NASA facilities is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than 1 year, or both, and may further result in termination of employment and access to NASA facilities.

7.2.12. To deter duplication, falsification, and misuse, the NASA photo-ID shall be redesigned and reissued, at a minimum, every 6 years.

7.3 NASA Photo-ID Issuance Criteria

7.3.1. NASA Civil Service personnel photo-ID: NASA civil service personnel are issued Agency-unique color-coded photo-identification that clearly identifies the individual as a NASA employee. The NASA Photo-ID design, color, and other characteristics are established in Appendix J, NASA Photo Identification Card Standards.

7.3.1.1. Issuance of the NASA civil service personnel NASA photo-ID is restricted to U.S. Citizens only, with the following exception:

7.3.1.2. The NASA civil service personnel photo-ID may be issued to non-Federal employees (e.g., consultants, IPA's, Foreign Nationals) including foreign members of the Astronaut Corps, employed under an IPA when:

a. a. Such issuance is deemed to be in the best interest of the Agency.
b. b. The individual is nominated by a Center Director, in writing with sufficient justification for consideration and approval by the AA/OSPP.

7.3.1.3. As a reminder, when issued, the permanent NASA photo-ID provides an individual with official NASA civil service personnel identification resulting in the assumption on the part of NASA employees, Center management, and Center Security Officials, that they are dealing with a U.S. citizen. Therefore, care must be taken to:

a. Ensure these personnel are appropriately screened and restrictions imposed where appropriate to preclude inadvertent access to areas, meeting, conferences, and information (e.g., export controlled information, other forms of SBU, etc.) not authorized through the implementing hiring agreement.

b. Ensure appropriate notification, to all Center security offices when issuance of this photo-ID occurs so that restrictions outlined in subparagraph a above are implemented. .

7.3.1.4. As a reminder, when issued, the NASA photo-ID provides an individual with official NASA civil service personnel identification; therefore, care must be taken to ensure appropriate awareness and due consideration of the risk involved.

7.3.2. Non-NASA Employee NASA Photo-ID. Contractor employees, consultant, military or other Government agency detailees, students, interns, and accredited press shall be issued a unique color-coded NASA photo-ID, per design specifications established in Appendix I. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3. Foreign National (FN) NASA Photo-ID. All Foreign Nationals, except Astronauts, visiting or assigned to work at NASA Installations shall be issued a unique color-coded NASA photo-ID unless the exception established in subparagraph 7.3.1.2 above is granted. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3.1. Specific and prominent lettering on the front of all FN NASA photo-ID will be placed identifying the bearer as a Foreign National and whether the FN is from a non-designated or designated country. This shall be accomplished with the placement of the letters "FN" for non-designated and "FND" for designated countries on the front of the NASA photo-ID.

7.3.3.2. An expiration date that is the earlier of the expiration of the individual's foreign passport, the expiration of the U.S. visa, or such earlier date as determined through review and approval pursuant to NPR 1371.2A, "Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. citizens who are Representatives of Foreign Entities."

7.3.3.3. If the Foreign National is deemed to require an escort per chapter 4, section 4.13, the issued photo-ID shall be so labeled with the words "Escort Required" on the face of the badge, and procedures shall be developed to ensure the escort requirement is appropriately implemented and monitored to ensure compliance.

7.3.3.4. Access and movement restrictions, if any, shall be placed on the back of the FN NASA photo-ID and recorded on a Security/Technology Control plan as required in chapter 4, paragraph 4.13.9.

7.3.3.5. The term foreign national applies to all non-U.S. citizens.

7.3.4. Center Security Offices, in coordination with Center Chief Information Officers, will establish the procedures necessary to ensure the NASA photo-ID and necessary access privileges to controlled facilities and/or IT Systems are properly activated at the time of badge issuance. Procedures must include necessary guidance to facility managers and IT System owners for identifying and requesting activation of specific privileges.

7.4 NASA Photo-ID Color-Coding

7.4.1. Gold NASA Photo-ID - NASA civil service personnel, and all active members of the NASA Astronaut Corps. Accepted for access to all NASA Centers, as appropriate.

7.4.1.1. Foreign National members of the Astronaut Corps shall have a representation of their National Flag superimposed on the badge for further designation as a FN.

7.4.2. Blue NASA Photo-ID - NASA consultants and contract employees (U.S. Citizen) who require access to a NASA Center or controlled facility.

7.4.3. Green NASA Photo-ID - Military and other U.S. Government agency detailees. Accepted for access to all NASA Centers, as appropriate.

7.4.4. Violet NASA Photo-ID - Any intern/student (U.S. citizen) who requires access to a NASA Center to perform their duties.

7.4.5. Orange NASA Photo-ID - Any foreign national (FN) contractor personnel from non-designated countries who require access to a NASA Center, or NASA controlled facility to perform their work.

7.4.6. Red NASA Photo-ID - Any Foreign National (FND) contractor personnel from designated countries who require access to NASA IT systems or shall have a need to work at a NASA controlled facility to perform their work.

7.4.7. Brown NASA Photo-ID - Any accredited member of the media (U.S. only) who may require access to "public" areas only of a NASA Center.

7.4.8. Silver NASA Photo-ID - Employees of the Jet Propulsion Laboratory (JPL).

7.4.9. If an individual does not require access to controlled Center assets, a local Center specific photo-ID may be issued in lieu of the NASA photo-ID.

7.4.10. Foreign national visitors shall be issued a visitor's pass, specifically identifying them as a foreign national, and escorted at all times.

7.5 Inspection of Persons and Property

7.5.1. General.

7.5.1.1. In the interest of national security and general employee safety, NASA shall provide appropriate and adequate protection or security for personnel, property, installations (including NASA Headquarters, Center, and Component Facilities), and information in its possession or custody.

7.5.1.2. In furtherance of this policy, NASA reserves the right to conduct an inspection of any person and property in their possession as a condition of admission to, or continued presences on, or upon exit from, any NASA Installation. Requirements, policy, and procedures for all aspects of this program are contained in 14 CFR part 1204, subpart 10.

7.5.1.3. All NASA entities must adhere to these requirements in the implementation of this program.

7.5.2. Requirements.

7.5.2.1. Per 14 CFR, Section 1204.1003 all entrances to Centers shall be conspicuously posted with the following notices:

1. " CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from, this installation is contingent upon your consent to inspection of person and property.
2. UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you shall not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

7.5.2.2. Only properly trained members of the Center's security organization shall conduct inspections pursuant to this NPR and the CFR. Personnel may be supplemented with detection devices (mirrors, x-ray, other sensing devices) and/or canines as the situation dictates.

7.5.2.3. Training shall include:

a. Appropriate search techniques for the type of vehicle being searched.
b. Key locations where devices or other contraband may be secreted.
c. Procedures for confiscating illegal or dangerous items, detaining of individuals and referring incidents to appropriate external law enforcement.

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

a. Consent to inspection notices covering NASA employees, contractors, and visitors to NASA Centers shall be issued in accordance with the authority contained under Section 304(a) of the National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. 2455(a), and 14 CFR section 1204.1003.
b. A consent to the inspection must be obtained from the person to be inspected giving permission for a general exploratory inspection while that person is about to enter or is on the grounds of, or is about to depart from a NASA Center. The person may change their mind at any time, and inspection shall not be pursued further. If an individual does not consent to an inspection, it shall not be carried out, and the individual shall be denied admission to, or be escorted from, the Center.
c. Inspecting personnel must exercise good judgment at all times prior to or while conducting an inspection. They must avoid exceeding their authority or exercising their authority with undue severity.
d. Security personnel shall present appropriate NASA credentials to the subject of the inspection.
e. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., weapons, drugs, explosives), the items may be confiscated, the individual shall be denied admission to, or be escorted from, the Center; or detained at the scene while the appropriate investigation is conducted by NASA investigators. The NASA Office of Inspector General or

appropriate law enforcement authorities shall be notified to assume jurisdiction over the matter.

f. The Office of the General Counsel shall approve Agency procedures based upon the requirements of this section.

7.6 Security Areas

7.6.1. Types of Security Areas.

7.6.1.1. Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource shall be "Restricted" areas (as a minimum designation).

7.6.1.2. Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors shall be escorted or other internal restrictions implemented, as determined by the CCS.

7.6.1.3. Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

7.6.1.4. Temporary Secure Work Area (TSWA). An area in which security measures are needed for 30 days or less. Shall be of a "restricted," "limited," or "closed" nature. A TSWA shall also be established if approval as a permanent security area is pending.

7.6.2. Establishment, Maintenance, and Revocation.

7.6.2.1. Establishment. Center Directors; Director, Headquarters Operations; the AA/OSPP; and the CCS shall establish, maintain, and protect such areas designated as restricted, limited, or closed depending on the rationale for the establishment of the area and the area's vulnerability to unauthorized access.

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

a. Post appropriate signs at entrances and at intervals along the perimeter of the designated area, as appropriate for the facility, to provide reasonable notice to persons that the area is a security area.
b. Signs must read as shown in Appendix G; however, the AA/OSPP may approve existing signs now used pursuant to a State statute.
c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

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

7.6.3. Access. Only those NASA employees, contractors, and visitors who need access and who meet the following criteria shall enter a security area unescorted. All other individuals must be escorted. Escorts must be authorized NASA employees or NASA contractors (U.S. Citizens).

7.6.3.1. To enter a Restricted Area unescorted, individuals must undergo the appropriate investigation required for that area as established by the individual Center; the investigation shall be, at a minimum, a NACI for civil service employees and a NAC for non-NASA personnel.

7.6.3.2. To enter a Limited Area, individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a NACI for unclassified but sensitive information and material.

7.6.3.3. To enter a Closed Area, individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

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

7.6.4. Cellular phones and other devices with digital camera capability. When introduced into security areas and/or areas of a sensitive nature, these items pose an unacceptable security risk to NASA. This risk encompasses numerous facets of the NASA security program. These risks include, but are not limited to: the protection of information (both

classified and unclassified but sensitive (SBU) such as ACI and ITAR information); contract proceedings and information; investigative information; and employee right to privacy. The Center CCS will implement and enforce the following:

a. No cell phones or other devices with photographic capabilities may be introduced into a NASA area housing the processing, display, or open storage of classified information.
b. Each Center Security Office shall conduct a continuing review of their facilities to ascertain the locations of other sensitive functions requiring protection from an overt or inadvertent compromise utilizing such devices.
c. Centers must have written security plans to accomplish the protection of those areas. Copies of those plans shall be maintained in the Center Security Office, and a copy must be available within the protected area at all times. Plans must include, as a minimum, the following items:

1. The method used to alert and educate affected employees.
2. Details on how the policy shall be enforced, including how the devices shall be physically denied entry or otherwise controlled.
3. Spot-check procedures.

7.6.5. Two-way pagers and other communications devices capable of recording and sending text messaging are also not authorized in security risk areas.

7.7 Facility Security

7.7.1. NASA Buildings and Facilities.

7.7.1.1. NASA buildings and facilities come in varying types and sizes, are used for varying purposes, and require implementation of varying levels of security to ensure adequate protection of NASA personnel and assets.

7.7.1.2. Facilities and buildings shall be provided the level of security commensurate with the level of risk as determined by conducting a vulnerability risk assessment:

a. Physical security enhancements for existing facilities shall be established based on an assessment of the type of vulnerability(ies) identified during a security vulnerability risk assessment, development of strategies to address identified vulnerabilities, and implementation of selected security measures, both physical and procedural.
b. Minimum physical security requirements shall be incorporated into construction of facilities projects in accordance with the requirements established by the CCS, Facility Engineering, and the Interagency Security Committee (IASC).
c. Procedural security measures shall be developed, implemented, and properly disseminated to ensure awareness, adherence, and compatibility with implemented physical security measures.

7.7.2. Security Fencing.

7.7.2.1. When used properly and in conjunction with other physical and procedural security measures, fencing provides for a cost-effective method of delineating U.S. Government property boundaries, establishing clearly visible protected borders, and serving as a deterrent to most would-be intruders.

7.7.2.2. Selection and placement of security fencing shall be in accordance with the requirements established in Chapter 6, NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

7.7.3. Keys, Locks, Locking Devices (hasps and chains), and Protective Seals.

7.7.3.1. Despite the growth and sophistication of IT-based access control systems, traditional keys, locks, and seals continue to play a significant role in the implementation and management of facility and asset protection.

7.7.3.2. Center Security Officials shall establish key and lock control policies and procedures in accordance with Chapter 5, NPR 1620.3, Physical Security Standards for NASA Facilities and Property.

7.7.4. Minimum Protection Considerations for MEI Facilities or areas housing MEI assets.

7.7.4.1. A Facility Security Manager (FSM) shall be designated for each facility. The FSM shall ensure that security training is provided to employees with access to the MEI asset and that program management implements and enforces the security requirements developed for the asset.

7.7.4.2. An access control system shall be employed at all times.

7.7.4.3. Intrusion Detection Systems (IDS) and other surveillance systems (e.g., video surveillance), when required, shall be appropriately monitored and shall receive appropriate response by armed mobile security personnel capable of responding within locally established time limits, but shall not exceed 5 minutes. Unannounced response tests shall be performed at a minimum of twice in a calendar year. ,

7.7.4.4. Security fencing shall be installed when the need is identified during the conduct of security vulnerability risk assessments.

7.7.4.5. Security lighting shall be installed at key areas around the facility to facilitate, to the extent possible, detection of intruders.

7.7.4.6. All personnel requiring unescorted access to the MEI shall have been investigated per chapters 3 or 4. All personnel not meeting investigative requirements shall be escorted.

7.7.4.7. Personnel shall properly display issued photo-ID.

7.7.4.8. NASA MEI shall be designated and properly posted as a NASA "Restricted" area, at a minimum. See Section 7.6 for criteria regarding designation of NASA Security Areas.

7.7.4.9. After completion of an initial security vulnerability risk assessment upon designation as an MEI asset, reassessments shall be conducted every 2 years at a minimum, or more frequently as circumstances warrant.

7.7.5. Childcare Centers

7.7.5.1. Childcare centers established under the auspices of NASA sponsorship shall, with coordination and approval of the CCS:

a. Establish positive measures to ensure the proper identification of authorized personnel, to include parents and others, authorized to pick up children.
b. Establish physical and procedural security measures necessary to separate and control child areas from visitor reception areas.
c. Install duress system buttons at key locations per Security Office specifications.
d. Install video surveillance capability in key locations per Security Office specifications.
e. Ensure adequate mechanisms are in place for emergency notification and response.
f. Ensure appropriate security lighting is installed at key areas around the facility to enable detection of would-be intruders.

7.7.5.2. Minimum physical security and antiterrorism construction standards for new NASA Childcare Centers shall be incorporated into construction of facilities projects in accordance with the requirements established in NPR 8820.2E, NASA Facility Project Implementation Guide, and the Interagency Security Committee (IASC).

7.7.6. Visitor Centers and Outdoor Displays

7.7.6.1. NASA Visitor Center and outdoor displays traditionally house one-of-a-kind, irreplaceable items of historical significance.

7.7.6.2. Such items are generally considered invaluable because they are irreplaceable and must be considered sensitive property. They must be reasonably protected.

7.7.6.3. The degree of protection necessary must be determined locally and in partnership between the Visitor Center curator, CCS, and supporting facility engineers.

7.7.6.3. Visitor Center buildings and apertures providing access to the building must be modified or constructed so as to delay a determined intruder long enough for a security force to respond.

7.7.6.4. Interior and exterior security lighting shall be provided in all Visitor Center buildings in which sensitive property is located.

7.7.6.5. Viewing surfaces of exhibit or display cases shall be constructed of materials resistant to breakage and must be securely fastened into frames or into the container.

7.7.6.6. Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.

7.7.6.7. Pilferable component parts shall be secured to the display or removed at the close of each business day.

7.7.7. Minimum Strongroom Physical Security Standards.

7.7.7.1. While generally considered sufficient for their intended purpose, the use of strongrooms to protect CNSI must be kept to the absolute minimum.

7.7.7.2. Any room designated for use as a strongroom must be modified in accordance with the following:

a. Doors shall be solid core metal clad and installed with the appropriate "X" Series tumbler lock.
b. Doors frames shall be steel.
c. Construction shall be a minimum of true floor to ceiling wood stud framing covered by 3/4" plywood and 1/2" wallboard. If necessary, plywood and new wallboard shall be installed directly over existing framing and wallboard.
d. Use of Intrusion Detection Systems (IDS) shall be determined by the CCS on a case-by-case basis and shall be evaluated on the basis of existing threats, overall building security program, and establishment of periodic security checks of facility.

7.7.8. IDS, Video Surveillance, and Electronic Access Control System Minimum Standards and Integration.

7.7.8.1. Security systems intended to protect people, property, or information are the responsibility of the CCS.

7.7.8.2. IDS, Video Surveillance, and Electronic Access Systems provide an effective means to enhance any organization's physical security program. If employed correctly and managed appropriately, these systems offer a wide range of coverage options.

7.7.8.3. The CCS shall:

a. Determine, in coordination with facilities engineering personnel with the appropriate expertise in security systems design, integration, and operation overall performance requirements for IDS, video surveillance, and Electronic Access Control Systems.
b. Establish and operate a 24-hour monitoring site where emergency response can be dispatched upon need.

7.7.8.4. Individual, stand alone systems offering no centralized monitoring oversight and alarm response capability (including internally-monitored systems) are not authorized.

7.7.9. For those facilities protected under the National Preservation Act of 1966, implementation of security measures shall be those measures allowable under the Act, to the extent necessary and practical.

7.8 Airfield and Aircraft Security

7.8.1. The cost and criticality of aircraft assets require protection at the home port, at intermediate landing locations, and at destinations. The CCS, in concert with Center Airfield Operations Management personnel, shall:

7.8.1.1. Ensure that a physical security survey and security vulnerability risk assessment are conducted on resident aircraft, hangars, ramps, and airfields.

a. The security vulnerability risk assessment shall help to determine the level of criticality and vulnerability of NASA flight assets to theft, sabotage, terrorism, vandalism, and air piracy.

b. The survey shall be used to establish a requisite level of protection that is reasonable and sustainable.

7.8.1.2. Ensure that specific physical and procedural security measures for the protection of NASA aircraft, are implemented, as appropriate.

7.8.1.3. At a minimum, designate and post airfield and associated support facilities as "Restricted Areas," and establish appropriate access control measures.

7.8.1.4. With the assistance of aircraft commanders, develop physical security requirements tailored to the configuration of specific aircraft to be included in the Pilot's Aircraft Checklist.

7.8.1.5. Develop a procedure for reporting and responding to the unauthorized movement or taxiing of aircraft.

7.8.1.6. Develop an alerting system that promptly advises the tower, fire department, security force, and other appropriate authorities of unauthorized activity.

7.8.1.7. Develop a response procedure in the event of the unauthorized movement of an aircraft.

7.8.2. Aircraft Commanders shall:

7.8.1.1. Ensure security of their aircraft at transient domestic and international locations.

7.8.1.2. Prohibit unauthorized access to aircraft under NASA control.

7.8.1.3. Ensure that passengers are properly identified and that baggage and packages are either associated with passengers or are authorized NASA cargo.

7.8.1.4. Reject unaccompanied or unidentifiable luggage or cargo and release to the custody of Center or other Airfield security forces for appropriate disposition.

7.8.1.5. Conduct appropriate security inspections of any NASA aircraft before placing it in service and after it has been left unattended.

7.9 Control and Issuance of Arms, Ammunition, & Explosives (AA&E)

7.9.1. Authority.

7.9.1.1. The AA/OSPP shall direct or grant approval for the following security officers and employees to carry firearms on official duty:

a. The DSMD and designated HQ security personnel.

b. The CCS of each Center and designated security personnel.

c. NASA employees, contractors, and subcontractors, while engaged in the performance of their official security duties such as couriers, investigators, or protective operations and details. This does not include the OIG, whose authority is derived from other sources.

d. NASA contractors and subcontractors engaged in the protection of property owned by the United States and located on NASA Centers or component facilities.

7.9.2. Responsibilities.

7.9.2.1. NASA certifying officials, described in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms," shall ensure compliance with the requirements of this section.

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

7.9.2.3. NASA security personnel and contractors shall not carry firearms outside the 50 States, the District of Columbia , and U.S. territories (Puerto Rico, Guam , U.S. Virgin Islands, American Samoa , et al.) without the advance approval of the AA/OSPP.

7.9.3. Certification to Carry Firearms.

7.9.3.1. The certifying official shall issue a NASA Form 699A or 699B, Certificate of Authority to Carry Firearms. The following items define the forms and their use and procedures for certification:

a. NASA Form 699A is a certification to carry concealed firearms when necessary in the performance of official duties.

b. The form shall be issued to NASA Civil Service employees and select contractor security officers (requires AA/OSPP approval) only. Uniformed contractor personnel shall not carry concealed weapons.

c. The NASA Form 699A is prepared in triplicate and indicates an expiration date (not to exceed 2 years from date of issue).

d. Upon termination of employment or assignment to duties not requiring carrying concealed weapons in the course of official duties, the certificate must be returned to the issuing officer within 15 days.

e. Exceptions to these requirements shall be made (in writing) only by the DSMD.

7.9.3.2. NASA Form 699B is a certification to carry unconcealed firearms that shall be issued only to NASA contractor employees serving as uniformed guards.

a. This form shall be prepared in duplicate and shall indicate the date of expiration (not to exceed the term of any applicable guard service contract; otherwise, not to exceed 5 years).

b. The form shall also identify the specific nature and location of official duties that require the carrying of firearms.

c. The original certificates shall be issued to the employee and shall be retained in the employee's possession while on official duty.

d. One copy of the certificate shall be retained by the NASA certifying official.

e. All losses of certificates shall be reported immediately to the certifying official.

f. Upon termination of employment or assignment to duty no longer needing certification to carry firearms, the original certificate shall be returned to the certifying official.

g. Only the certifying official may make exceptions to these requirements.

7.9.3.3. NASA Forms 699A and 699B are serialized for control and accountability purposes. Certifying officials shall maintain appropriate accountability records, including certification of destruction, for all forms in their custody and ensure that all unused forms are kept in a secure storage container other than the one in which the accountability records are stored.

7.9.3.4. Certifying officials shall not sign their own certificates. The Center Director or the AA/OSPP shall sign certificates authorizing the issue of a weapon to a certifying official.

7.9.4. Conditions Under Which Firearms May be Carried by Center Security Personnel. Including shoulder-fired weapons (e.g., rifles, machine guns, shotguns):

7.9.4.1. Firearms may be carried only when all of the following criteria are met:

a. The individual has successfully completed the appropriate suitability background investigation and has been favorably evaluated by a qualified physician to be physically fit as well as emotionally stable.

b. The individual is in immediate physical possession of a valid NASA certification to carry firearms.

c. The individual has successfully completed a qualification course for the firearm being carried, and the qualification is current. (Refer to Appendix E and paragraph 7.9.8)

d. It is necessary in the performance of official NASA duties and with the knowledge and approval of a certifying official.

e. There is no use of intoxicants (e.g., illegal drugs, alcohol) during duty and prior to 12 hours of reporting to duty.

f. Appropriate annual criminal hsitory check for recertification under the Lautenberg Amendment to the Gun Control Act of 1968, effective 30 September 1996.

7.9.4.2. The wide range of circumstances under which it shall be necessary to carry firearms requires consideration of all pertinent factors, augmented by common sense and good judgment.

7.9.5. Conditions Under Which Firearms and Explosives May be Used, Stored, and Maintained by Non-Security Personnel:

7.9.5.1. Researchers and scientists frequently use firearms and explosives during testing and experimentation. The safe operation, storage, and accountability of firearms and explosives used under testing and experimentation are required to ensure the safety and security of Center personnel.

a. NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics, are the governing documents for establishing the safe storage and handling of firearms and explosives.

b. This chapter is the governing document for issue, use, secure storage, and accountability for firearms and explosives.

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

a. NASA program and project personnel contemplating the of use firearms or explosives in testing or experimentation

programs must submit a written request to the CCS outlining the program or project need for introducing firearms, ammunition, and explosives onto a NASA facility.

b. An inventory of the type of weapons and explosives with serial numbers, type and amount of ammunition, and type and amount of explosives shall be maintained and updated on a quarterly basis. The inventory shall be made available for review by security and safety personnel, as requested.

c. Identify location of stored/secured and names of personnel having access.

d. In coordination with the Center Security and Safety personnel, establish appropriate secure storage for AA&E.

7.9.6. Weapons Aboard Commercial Aircraft.

7.9.6.1. Armed NASA Special Agents (SA) may only carry firearms on commercial aircraft after completion of required Federal Aviation Administration certification in accordance with 14 CFR 108.219, and then only in conjunction with "Official" Government travel requiring the SA to be armed.

a. Refresher Federal Aviation Administration certification training, for carrying firearms on a commercial aircraft, shall be required every 2 years and shall be integrated with required firearms qualification to ensure appropriate awareness.

b. The DSMD or designee shall be notified in advance of all official air travel of armed NASA Civil Service SA. NASA security services contractor personnel are not authorized to fly armed.

7.9.6.2. In addition to the Federal Aviation Administration requirement, the SA must be currently qualified to carry a firearm.

7.9.6.3. The SA must be in possession of a current NASA Form 699A (concealed weapons permit) and NASA badge and credentials.

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

7.9.6.5. The SA shall always carry the weapon on his/her person and never in carry-on baggage.

7.9.6.6. The SA shall always carry handcuffs.

7.9.6.7. The SA shall never carry Oleoresin Capsicum spray or other chemical intermediate weapon while on-board a commercial flight.

7.9.7. Firearms Instruction.

7.9.7.1. The certifying official shall designate a firearms instructor, who shall inform the certifying official in writing of an individual's knowledge of the rules of firearm safety and the content of this NPR.

7.9.7.2. In cases involving a contractor guard force, the firearms instructor may be appointed from the guard force complement.

7.9.7.3. Minimum standards shall be met before a firearms instructor or certifying official shall consider an individual qualified to carry firearms.

7.9.7.4. Recent firearms training and experience during prior employment, such as the FBI, Secret Service, police, military, or other significant and qualifying experience, shall meet NASA standards if the individual has qualified under all provisions of this chapter within the past 30 days.

7.9.7.5. These qualifications shall be verified by a review of employment and training history either through an interview with previous management or visual inspection of documented training history.

7.9.7.6. Appropriate NASA training, including firearm safety procedures and use of deadly force, followed by obtaining a qualifying score on a recognized course as specified in paragraph 7.9.8 below, shall also be required.

7.9.8. Training.

7.9.8.1. Personnel shall be trained and qualified on professional firearm ranges established and maintained by NASA, or other federal, state, or municipal authorities.

7.9.8.2. Personnel shall be certified for carrying firearms after firing a qualifying score under the NASA certified firearm course. (See Appendix E of this NPR.)

7.9.8.3. The AA/OSPP shall establish firearms course of fire standards for all Center armed security personnel, to

include standards for shoulder-fired weapons (e.g., rifles, submachine guns, shotguns).

7.9.8.4. As soon as possible after certification, personnel shall receive testing and training in judgmental shooting (whether to shoot or not to shoot) through NASA's current firearms training simulator or other approved methods of judgmental shooting.

7.9.9. Maintenance of Proficiency.

7.9.9.1. Personnel authorized to carry firearms shall be required to fire a qualifying score on the NASA course of fire at least once every 6 months.

7.9.9.2. All personnel authorized to carry firearms must successfully complete testing and training on the simulator or other approved methods of judgmental shooting annually, if possible, or as often as the system is available at that Center.

7.9.10. Records.

7.9.10.1. The certifying official or firearms instructor shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data.

7.9.10.2. Records shall be maintained for 2 years.

7.9.11. Firearms Standards.

7.9.11.1. CCS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm their Civil Service and contractor security staff.

7.9.11.2. The AFL is approved by the Office of Security and Program Protection (OSPP) and maintained by the NASA Federal Arrest Authority Training Academy (NFAATA) at Kennedy Space Center .

7.9.11.3. The AFL may be waived or modified only by the AA/OSPP.

7.9.11.4. Training, qualifications, and certification for all approved firearms shall be documented per paragraph 7.9.8.

7.9.11.5. Modifications.

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

b. Center armorers shall modify grips, sights, and control levers to best suit individual users.

7.9.11.6. Handguns.

a. NASA approved handguns are semi-automatic pistols in calibers 9mm, .40, or .357.

b. Uniformed contractors at each Center must be armed with the same make and model handgun.

c. Emergency response teams/SWAT teams may carry a different make and model.

d. NASA Civil Service personnel shall carry the same make but may vary the model to suit individual users.

e. Handguns must always be worn in standard, commercially available holsters; uniformed officers must use holsters with a retention device.

7.9.11.7. Patrol Rifles.

a. At the discretion of the CCS, contractors shall be armed with semi-automatic or select fire patrol rifles.

b. Only iron or optical sights shall be installed on these weapons.

7.9.11.8. Patrol Shotguns.

a. At the discretion of the CCS, contractors and Civil Service personnel shall be armed with semi-automatic or pump action 12 gauge shotguns.

b. These weapons shall also be used to employ "less-lethal" ammunition.

7.9.11.9. Submachine guns.

At the discretion of the CCS, contractor security force may be armed with submachine guns.

7.9.12. Other approved firearms.

At the discretion of the CCS, and with the consent of the AA/OSPP, other firearms may be utilized to meet Center security requirements.

7.9.13. The user of any NASA approved firearm must meet the training and certification requirements of paragraph 7.9.8.

7.9.14. Personal weapons.

The use or carrying of personal weapons is prohibited.

7.9.15. Ammunition.

7.9.15.1. Only premium, commercially manufactured, "law enforcement only" duty ammunition shall be issued.

7.9.15.2. Duty ammunition shall be expended at training sessions at least once every 18 months to ensure use of fresh duty ammunition.

7.9.15.3. Normal training ammunition shall be commercially manufactured "lead-free" training ammunition designed for range use.

7.9.16. Firearm maintenance.

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

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

7.9.17. Accountability of Arms, Ammunition, and Explosives (AA&E).

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

7.9.17.2. The CCS shall appoint a custodian for all AA&E within the Center Security Office, within each contractor guard force, and within each non-security organization using AA&E (e.g., explosives, propellants, etc.) for research or testing purposes.

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

a. The date and method of acquisition of all firearms and ammunition.

b. Full identifying data, e.g., the caliber, make, and serial number of each firearm.

c. Amounts of basic load and training ammunition on-hand.

d. Types and amounts of explosives, (e.g., fragmentary, flash-bang grenades, C/S, pepper spray, etc.).

7.9.17.4. The CCS shall report all Center AA&E data to the AA/OSPP on an annual basis the third week after the end of the fourth quarter of each fiscal year.

7.9.17.5. Current contractor firearm data shall be maintained in the Center Security Office.

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

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

b. Serial numbers of firearms.

c. Numbers and types of assigned explosives.

d. Types and numbers of ammunition on-hand.

e. Signatures of recipients.

f. Signatures of custodians upon return of the firearms and explosives.

(NOTE: Both NASA personnel and contractor receipts shall be retained by each Center for 1 year.)

7.9.18. Lost, stolen, or missing AA&E shall be reported immediately, but no later than 24 hours after discovery, to the DSMD:

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

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

c. A description of the lost, stolen, or missing AA&E shall also be entered into the National Criminal Information Center (NCIC) database.

7.9.19. Security Services contract personnel issued AA&E may only be armed on NASA property to perform their mission, if approved by the CCS.

7.9.20. Non-security personnel having NASA mission related uses for AA&E items (e.g., researcher, scientists, etc.) shall:

7.9.20.1. Ensure control, storage and accountability of authorized AA&E are in accordance with the provisions in paragraph 7.9.21 of this chapter and the requirements established in the NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics.

7.9.20.2. Maintain appropriate and current inventories of issued and maintained AA&E per paragraph 7.9.17 and provide a copy of the inventories to the CCS as changes occur.

7.9.21. Storage and Exchange of AA&E.

7.9.21.1. Issued firearms for NAS security and law enforcement personnel may be stored loaded or unloaded under secure means, per local policy.

7.9.21.2. When not in use, all issued firearms and ammunition shall be securely stored per local policy.

a. Non-issued firearms and shoulder-fired weapons shall be stored in an arms room or a security container with a built-in 3-position combination lock and issued only as required.

b. Non-issued ammunition shall be stored in either a suitable lockable container or an arms room.

7.9.21.3. Explosives shall be stored in separate secure containers, specifically designed for the purpose of storing explosive materials.

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

7.9.21.5. NASA HQ and each Center shall adopt procedures for the maintenance of records with respect to the issuance of AA&E and access to firearms and ammunition storage areas and containers.

7.9.21.6. Weapons shall not be exchanged on a guard post. Any exchange or inspection of firearms shall be done only in an area where a "clearing barrel" is available and under proper supervision.

7.9.21.7. Firearms shall always be considered loaded. Armed NASA security personnel shall not point the firearm at anything that they do not intend to shoot.

7.10 Standards for Secure Conference Rooms

7.10.1. When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities."

7.10.2. The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with DCID 6/9.

7.10.2.1. Meetings shall be limited to collateral Secret or below.

7.10.2.2. Positive access control shall be implemented.

7.10.2.3. A Technical Surveillance Countermeasures (TSCM) Specialist, if available, or Security Officer shall conduct

a visual inspection and establish security procedures for the meeting.

7.10.3. Special Cases.

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

7.10.3.2. For these areas, guidance on additional requirements will be provided by the CCS on a case-by-case basis.

7.10.3.3. The DSMD or CCS shall be contacted for any interpretation of these specifications.

7.11 Threat Assessment

7.11.1. Reliability.

7.11.1.1. NASA personnel, facilities, and programs are subject to a wide range of internal and external threats.

7.11.1.2. Such threats may be presented by natural forces, workplace violence, the technological sophistication of NASA Research and Development (R&D) and test facilities and programs, and the inherent risk of component and system failure by both internal and external attempts to disrupt Agency operations or to compromise National security.

7.11.2. Threat Assessments.

7.11.2.1. The DSMD, after consultation and input from various sources, shall publish an annual NASA Postulated Threat Statement.

7.11.2.2. Of significant importance are the Agency's resources identified under the Critical infrastructure and key resources protection program. However, threat assessments must transcend formally designated critical resources and assets and cover the full realm of NASA personnel and physical resources, assets, and program/project information.

7.11.2.3. The CCS shall use the NASA Threat Statement in developing a localized threat statement for their Center.

7.11.3. Countermeasures.

7.11.3.1. NASA shall employ a sound and comprehensive security program that includes security awareness training and the development and implementation of Center security plans to counter these threats.

7.11.3.2. To ensure an Agencywide standard for reacting to periods of increased security threats, the threat conditions established in section 7.17 below shall be employed as directed by NASA Headquarters or as determined by local events.

7.12 Threat and Incident Reporting

7.12.1. General.

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

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

7.12.1.3. Reports shall be forwarded to the DSMD. Refer to appendix F for a sample of the Serious Incident Report format.

7.12.2. Responsibilities.

7.12.2.1. The CCS ensures that incidents are reported to the DSMD and followed up with a fax that describes the incident.

7.12.2.2. The DSMD shall report information from the CCS (or designated representative) to the AA/OSPP, if available.

7.12.2.3. The AA for Security and Program Protection shall then decide whether it is appropriate to brief either the NASA Administrator, Deputy Administrator, or Chief of Staff.

7.12.2.4. If a principal or designated representative is unavailable at any of the cited levels, the information shall be automatically passed to the next level.

7.13 Reportable Incidents

7.13.1. Any type of incident that might have security implications shall be reported to the AA/OSPP in a timely manner, including the following:

7.13.1.1. All crimes committed at a Center requiring notification of NASA OIG, or, as appropriate, the FBI, DEA, ATF, or local law enforcement.

7.13.1.2. Possible Espionage (Reported through Center CI channels via the NASA Secure Network (NSN)).

7.13.1.3. Possible Sabotage (Reported through Center CI channels via the NSN).

7.13.1.4. Suspected terrorist activity (e.g. surveillance, photography, attempted penetrations, unusual requests for information). (Reported through Center CI channels via the NSN).

7.13.1.5. Bombing incidents, including bomb threats that severely impact Center activities.

7.13.1.6. Actual or planned demonstrations or strikes.

7.13.1.7. Shootings or other violent acts.

7.13.1.8. All incidents which involve the need for professional medical attention or damage to NASA facilities or equipment exceeding $25,000 shall also be reported in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Record Keeping.

7.13.1.9. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on NASA property may also require reporting to and through the NASA Safety Program channels in accordance with NPR 8621.1.)

7.13.1.10. A security-related incident in which the media has become involved and publicity is anticipated.

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

7.13.1.12. Threats against NASA property.

7.13.1.13. Threats that affect NASA missions.

7.13.1.14. Threats against NASA personnel.

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

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

7.14 NASA Security Office Special Agent Badges and Credentials (B&C)

7.14.1. Control.

B&C's are sequentially numbered and accountable security items. Their issue, use, and accountability shall be monitored by both the AA/OSPP and the CCS.

7.14.2. Issuance, Use, and Return.

7.14.2.1. B&C's identify NASA Special Agents authorized, under NASA Federal Arrest Authority, to conduct investigations and inspections and to perform other duties that shall be assigned by virtue of the National Aeronautics

and Space Act of 1958, as amended. [NOTE: This does not include the Office of Inspector General (OIG), whose authority is derived from other legal sources].

7.14.2.2. The AA/OSPP shall create, authenticate, and issue credentials and procure metallic badges at the request of the CCS.

7.14.2.3. The CCS shall nominate civil service personnel to receive B&C's.

7.14.2.4. Security specialists whose official duties do not require routine investigative work and/or frequent liaison with Federal, State, or local law enforcement authorities shall only be issued credentials appropriate for the position occupied.

7.14.2.5. The CCS shall ensure that B&C's or credentials no longer required for official duties are returned to the AA/OSPP. B&C's shall be surrendered to the CCS when replacements are issued.

7.14.2.6. The CCS shall ensure that B&C's are not misused and shall withdraw them immediately upon any report of misuse, pending investigation of the allegation:

a. A report outlining the circumstances of any withdrawal of B&C's shall be forwarded to the DSMD within 72 hours.

b. A report on the final disposition of the incident, including the results of a Return To Duty (RTD) assessment and recommendation, shall also be furnished to the DSMD for review and final determination.

7.14.2.7. Lost or stolen B&C's must be reported immediately. The appropriate CCS shall forward a report outlining all pertinent facts to the DSMD no later than 2 days after the loss.

7.14.2.8. Security specialists must surrender B&C's when requested by the issuing authority or when relieved of security duties by transfer, termination, or retirement. Upon termination of security duties, requests to keep B&C's shall be addressed as follows:

a. Employee must have been employed by NASA as a Security Official for a minimum of 10 years.

b. Credentials shall be sent, along with a letter requesting retention of "voided" credential, for the individual concerned.

c. Retirement and presentation of the NASA metal badge shall be considered based on the following prerequisites:

(1) Employee must be retiring from Federal service under honorable circumstances.

(2) Employee must have served NASA in an agent capacity for a minimum of 10 years.

(3) Badges must be mounted in a Lucite award block, which shall be funded by the either the individual or requesting office and procured by the OSPP.

(a) Individuals or organizations shall submit to the OSPP a written request containing the individuals name, position, and length of service with NASA, along with a personal check in the amount required at that time, made out to the OSPP selected vendor.

(b) The OSPP shall arrange fabrication of the award. Delivery time shall normally be within 4 weeks from submission of order.

7.14.2.9. B&C's may be returned to the AA/OSPP by NASA Pouch Mail, double wrapped, or they may be hand-carried.

7.14.3. B&C's for Contractors.

a. The CCS shall issue Center-unique B&C's to contractor security personnel as deemed appropriate. The B&C must identify the individual as a NASA Contract employee, authorized under the Space Act to perform specified duties (e.g., investigations, inspections, etc.).

b. All provisions of section 7.14 also apply to NASA contract security services personnel.

7.14.4. Acceptance of B&C's for Access to NASA Centers.

B & C's (Federal, State, or NASA) shall not be accepted for access to NASA Centers unless accompanied by a NASA photo-ID or issued NASA visitors pass.

7.15 Technical Surveillance Countermeasures (TSCM)

7.15.1. TSCM Program.

The AA/OSPP is responsible for the NASA TSCM program. The program shall be consistent with national policy issued by the U.S. Security Policy Board (USSPB). All matters pertaining to the conduct of TSCM activities throughout the Agency shall be directed and coordinated through the DSMD.

7.15.1.1. The AA/OSPP shall ensure that a NASA TSCM capability exists which can:

a. Conduct physical, electronic, and visual search techniques to identify and protect Agency persons, facilities, information, or activities that are vulnerable, through design or circumstance, to hostile technical surveillance activities.

b. Ensure that TSCM operations are conducted in a manner consistent with U.S. Security Policy Board guidelines.

c. Acquire and employ TSCM technologies, techniques, and methods to identify and neutralize hostile technical surveillance activities that are consistent with accepted national TSCM policies.

d. Collect, analyze, and disseminate data regarding the technical surveillance threat to the Agency.

e. Provide support by ensuring that all NASA TSCM personnel are accredited through U.S. Government TSCM training and that individuals receive continuing, advanced training necessary to maintain the level of technical expertise as prescribed by TSCM USSPB Procedural Guides 1 through 3.

f. Develop, with input by the DSMD; Director, Safeguards Division; and Center Security Chiefs, a listing of facilities that require a TSCM service.

g. Coordinate TSCM efforts with Centers that have organic TSCM assets.

7.15.1.2 Conduct of TSCM Services

a. TSCM services shall be conducted in accordance with USSPB TSCM Procedural Guides, following the four distinct phases.

b. TSCM services shall be coordinated through the DSMD for the purpose of tracking TSCM efforts.

7.15.1.3 Facilities Requiring TSCM Support

a. A TSCM service shall be performed for initial accreditation purposes for any Sensitive Compartmented Information Facility (SCIF) within the Agency. Follow-on TSCM support shall be coordinated through the Agency SSO when threat conditions warrant, when there has been a modification to the SCIF, when uncleared personnel have not been continually escorted while in the SCIF, or when new equipment or furnishing have been introduced to the SCIF.

b. A TSCM service shall be conducted in all offices in which Top Secret discussions routinely occur.

c. A TSCM service shall be conducted in offices or areas that are routinely used to process information or to discuss information that addresses sensitive aspects of controlled U.S. technology or controlled Agency technology.

d. TSCM services shall be conducted in NASA senior executive office spaces.

e. TSCM services shall be conducted in contractor facilities that process and discuss NASA classified national security information as annotated in the DD-254, DOD Contract Security Classification Specification.

f. TSCM in-conference monitoring support shall be scheduled if the conference is conducted in an area not usually associated with classified discussions and the area has not been under continuous control by cleared employees.

7.15.1.4 TSCM Request Procedures

All requests for TSCM support shall be addressed in writing to the DMSO, Security Management Division and classified at the Secret level at a minimum. Advanced coordination may be done telephonically, but only via secure means. When requesting or coordinating a TSCM service, requestors shall not use any communication medium located within the area that is to be the subject of the TSCM service. At a minimum, the request must identify:

a. Complete identification of the area requiring TSCM support, to include: name of area, room number, building number, address, location, and brief mission description of the area/facility.

b. Brief justification why a TSCM service is necessary.

c. Square footage of each space identified.

d. The name of the point of contact and an alternate, with telephone numbers for both secure and nonsecure telephones.

e. Clearance requirements for TSCM personnel.

f. The time frame the service is required.

7.15.1.5 TSCM Reports

1. Upon completion of a TSCM survey, a complete report shall be provided for the requestor. At a minimum the report shall include:

a. Complete identification of the facility receiving the TSCM support.

b. Who requested the survey.

c. When the survey was accomplished and by whom.

d. Description of the support provided.

e. Findings/Observations if security vulnerabilities or hazards were discovered.

f. Recommendations that either mitigate or eliminate the security vulnerabilities.

g. Name of local person who received the out-brief.

2. Reports shall be signed by the responsible senior security official who has operational oversight of the TSCM team. Copies of TSCM reports shall be provided to the DSMD.

7.15.1.6 Discovery of a Device

Upon discovery of a suspected eavesdropping device, the following actions shall be taken:

a. The area shall be secured and placed under continuous surveillance.

b. A report, classified Secret, shall be submitted, without delay, to the DSMD. At a minimum, the report shall contain the following.

(1) Date and time of the discovery.

(2) Facility and area where found.

(3) Specific location of the suspected find.

(4) Description of suspected device (e.g., wired microphone, modified telephone, RF transmitter, etc.).

(5) Method of discovery.

(6) Name(s) and any additional information of personnel who discovered the suspected device.

(7) Best estimate as to whether any foreign intelligence service was alerted to the discovery.

b. Only the responsible official at the facility shall be notified of the discovery and the actions taken. Information of the suspected discovery shall not be released to other persons, until such release has been coordinated with and approved by the DSMD.

c. No effort shall be made to test the specific device or to attempt to remove the suspected device, until such actions have been authorized by the DSMD.

7.15.1.7 Classification Requirements

a. NASA TSCM Security Classification Guide SCG-17, dated August 1992 is hereby rescinded.

b. The following is classification requirements for NASA TSCM operations as outlined in USSPB Procedural Guide 1 and shall serve as the TSCM classification Guide for the Agency:

á

Information that Reveals	Shall be Classified