Langley Research Center

Directive: LPR 1620.1

Effective Date: May 23, 2005

Expiration Date: April 30, 2009

Information Security Program Management Procedures and Guidelines

National Aeronautics and Space Administration

TABLE OF CONTENTS

Responsible Office: Security Management and Safeguards Team,
Center Operations Directorate

PREFACE

P.1 PURPOSE

This directive establishes a Center wide program management system to ensure the protection of LaRC controlled Classified National Security Information (CNSI). It prescribes responsibilities, and supplemental procedures and guidance to those established in listed references. CNSI designated as Sensitive Compartmented Information (SCI) or Special Access Required (SAR) shall be exempt from the requirements set forth in this directive.

P.2 APPLICABILITY

These procedural requirements are applicable to all LaRC personnel with a security clearance and access to Classified National Security Information (CNSI).

P.3 AUTHORITY

a. Executive Order 12958, "Classified National Security Information," Part 5

b. 32 CFR Part 2001, "Information Security Oversight Office, Classified National Security Information, Directive Number 1."

P.4 REFERENCES

a. NPD 1440.6, "NASA Records Management."

b. NPD 1600.2, “NASA Security Policy.”

c. NPR 1441.1, "NASA Records Retention Schedules."

d. NPR 1620.1, “Security Procedural Requirements.”

e. LAPD 1440.6, "Records Management."

f. LAPD 1600.3, “Langley Research Center (LaRC) Security Policy.”

g. LMS-CP-2707, "Records Management.”

h. NASA Langley Form 68, "Delivery Ticket."

i. NASA Langley Form 186, "Request to Hand Carry Classified Materials Outside the Boundary of NASA Langley Research Center."

j. NASA Langley Form 187, "NASA Langley Research Center Courier Briefing Statement."

k. NASA Langley Form 454, "Classified Material Destruction Verification Record."

P.5 CANCELLATION

LPR 1620.1, dated November 24, 2004

Lana M. Couch
Associate Director for
Business Management

CHAPTER 1. PROGRAM MANAGEMENT AND SELF-INSPECTION

1.1 Management Infrastructure

1.1.1. The Center Chief of Security (CCS) shall designate an Information Security Program Manager. The LaRC Information Security Program Manager (ISPM) shall provide assistance to Organizational Unit Managers (OUM) and their personnel in information security and security education matters.

1.1.2. Each OUM, with employees who handle and store CNSI, shall appoint a primary information security representative to serve as the point of contact between the LaRC ISPM and Organizational Unit (OU) personnel and to administer the unit's information security program. OUMs for large activities with many sub-units and significant classified material involvement shall consider appointing alternate information security representatives at subordinate branch levels. Classified information security representatives must be government employees.

1.1.3 The LaRC Records Manager shall serve as the determining agent regarding the retention of classified materials in permanent archives.

1.2 Self-Inspection

1.2.1 The LaRC ISPM shall conduct periodic reviews of each LaRC OU that handles or stores CNSI. These reviews shall be a comprehensive evaluation of the organization's overall compliance with the information security program and a determination of the volume and type of classified material stored. During these reviews, classified custodians shall screen classified materials and destroy all materials no longer needed.

1.2.2. ISPM conducted reviews are designed to assist OUMs and their staffs in the management of CNSI. The ISPM will provide a written report of findings and recommendations to the OUM. These reports will not require an answer unless major deficiencies are noted.

CHAPTER 2. Classification and Declassification

2.1 Requests for Original Classification Determinations

2.1.1 LaRC employees who develop new information that they believe warrants protection as CNSI, which is not related to any existing classification guide or known previous classification determination, shall protect the information as classified and immediately contact the LaRC ISPM. Authors of new potentially classified information must demonstrate that the compromise of that information would reasonably be expected to cause damage to national security. There are no original classification authorities resident to LaRC. Where sufficiently supported by justification, the ISPM shall elevate requests for an original classification determination to appropriate functional managers at NASA Headquarters.

2.1.2 Project managers involved in the development and publication of classification guidance for newly developed classified programs shall coordinate those efforts with the LaRC ISPM. A designated original classification authority must approve classification guides.

2.2 Declassification

Classified custodians in possession of information developed and originally classified by LaRC officials and that appears to no longer warrant protection as CNSI, shall submit such information to the LaRC ISPM for declassification review. The Declassification Authority shall consider the affected information for declassification after a technical assessment by knowledgeable persons in the subject area and a determination that the compromise of such information would not reasonably be expected to cause damage to national security. LaRC personnel delegated declassification authority by HQ NASA may reduce the classification level or declassify all or part of the information being assessed. A declassification determination does not automatically signify that the information is releasable to the public. The Declassification Authority shall notify all known holders of the information that there has been a change in classification. Classified custodians shall not submit information for declassification review that has no retention value. Such information shall be destroyed.

2.3 ARCHIVING CLASSIFIED MATERIALS

Classified materials shall be subject to a review for declassification under the Automatic or Systematic Declassification provisions of the Executive Order prior to commitment to a permanent archive. The LaRC Records Manager shall identify all records or materials bearing classification markings and being processed for permanent storage at National Archive facilities to the LaRC ISPM for declassification consideration. Classified records determined exempt from declassification under Section 3.4b of the Executive Order shall be subject to future systematic reviews for declassification at intervals determined appropriate based on the nature of the exemption category. Exempted

classified information committed to archives shall be posted with a notice of prior declassification review, authority for continued classification and the schedule for future systematic reviews. The LaRC ISPM shall be responsible for recording systematic declassification review schedules for exempted materials in permanent archives and initiating reviews according to the established schedule.

CHAPTER 3. Marking

3.1 Classified Marking Standards

Classified materials, regardless of media type, prepared by LaRC personnel shall be properly marked with classification and associated markings. Personnel developing a classified product derived from one or more existing classified sources may use the "Guide to Marking Classified Documents," published by the LaRC Security & Program Protection Services for reference. All classified materials shall be reviewed by the LaRC ISPM for proper application of classification and associated markings prior to dissemination to any tenant activity or organization outside of the Center.

3.2 Classified Working Papers

LaRC personnel exercising derivative classification by preparing classified material using one or more existing classified sources shall NOT annotate draft documents as "Working Papers." The "Working Paper" exclusion used in marking classified material under development is not appropriate when the developer of a classified product has the source or classification guide to transfer associated and classification markings to the new product. Normally, the "Working Paper" annotation is used in the development of information that will result in an original classification determination. Classified material authors who choose to use the "Working Paper" marking exclusions must comply with the conditions and limits imposed by Executive Order 12958.

CHAPTER 4. Handling and Safeguarding

4.1 Access

NASA employees who have authorized possession, knowledge, or control of classified information may grant an individual access to that information based on verification of a valid U.S. issued security clearance at the appropriate level and an official need-to-know the information. Some categories of classified information shall require additional approval for disclosure from the responsible controlling program office. Security clearance and level of clearance eligibility shall be verified by contacting the Center Security & Program Protection Services, the Badge and Pass Office, the individual's supervisor or Organizational Unit Manager, or by receipt of a valid classified visit request. Access to classified information shall never be granted based solely on the type of identification badge the holder has been issued.

4.2 Classified Custodian Control Measures

Unless located in a controlled entry environment where only appropriately cleared personnel may enter, all classified information that has been removed from secure storage shall be covered with an appropriate classified coversheet or placed in a folder or envelope conspicuously marked front and back with the highest classification. Security container custodians shall maintain sufficient quantities of classified coversheets and marked folders and envelopes to meet work area needs. Appropriately cleared individuals shall maintain custody of classified material at all times when it is not in secure storage.

4.3 End-of-Business Day Inspections

Supervisors of work areas where classified material is handled or stored shall institute procedures that include an end-of-work-day security inspection to ensure all classified materials are properly stored. As a minimum, this check will include classified work areas such as desk tops, routing trays, reproduction equipment and other areas where classified material is handled, computers used for classified processing, secure telephone keying devices and any vaults, secure storage spaces or security containers. During end-of-work-day security container inspections, each container combination lock dial will be rotated a minimum of three full turns and the Standard Form 702, "Security Container Check Sheet," annotated in the "checked by" column. This check shall not be required if the container has not been opened since the last inspection.

4.4 Use of Reproduction Equipment

The LaRC ISPM shall evaluate all new or existing reproduction equipment to determine suitability for use with classified material. Upon approval, the LaRC ISPM will post reproduction equipment as authorized to reproduce CNSI. The ISPM shall conduct these evaluations upon OUM request or during periodic OU information security reviews. The authorizing document shall be affixed to the reproduction equipment or

posted in the immediate vicinity. It shall include the equipment property number, any specialized operating instructions, the level of CNSI that may be reproduced and the authorizing ISPM signature. The LaRC ISPM shall post equipment not approved for the reproduction of CNSI as not authorized for classified use.

4.5 Storage of Administratively Controlled Information (ACI)

Information meeting the criteria for designation as ACI, as described in NPR 1620.1, "Security Procedural Requirements," while not under the observation of the custodian or other authorized individual, shall be stored in a LOCKED space such as an office, room, file cabinet, desk or other container that affords physical protection. Locked building perimeter entrance doors do not meet the locked space requirement unless the building perimeter door is also the office entrance.

4.6 Emergency Actions

4.6.1 If time and circumstances permit, custodians of CNSI material shall return the material to proper storage during emergency situations or upon order to evacuate the work area. However, PREVENTION OF INJURY OR LOSS OF LIFE WILL TAKE PRIORITY OVER EMERGENCY EFFORTS TO PROTECT CNSI. Custodians shall immediately report to the CCS or ISPM any evacuation of buildings that result in leaving CNSI outside of proper storage. In addition, custodians will ensure senior on scene fire and security response personnel are briefed that emergency personnel entering the building may be exposed to CNSI.

4.6.2 Fire department and emergency medical personnel responding to valid emergencies shall not be delayed or denied entry to areas where CNSI is exposed. If time and circumstances allow, custodian of CNSI shall take available and reasonable actions to mitigate CNSI exposure such as covering or obscuring the viewable material with any available nearby object. In addition, custodians shall, at the first opportunity that does not interfere with the actions of the emergency response team, identify and document all individuals that have entered the area where CNSI is exposed. The CCS or ISPM shall be notified immediately.

4.6.3 The ISPM shall conduct debriefings where emergency response personnel are exposed to CNSI during emergency situations.

CHAPTER 5. Accountability and Control

5.1 Accountability Records

Unless directed by a responsible program office or through another controlling directive, a formal accountability system for classified items (itemized record of inventory of classified materials) at the Secret and Confidential level is not required. Top Secret information must be controlled through the Top Secret Control Officer (TSCO).

5.2 Technical Library Controlled Materials

Classified materials annotated with identification or tracking numbers developed through the LaRC Technical Library are Technical Library controlled materials. Library customers in possession of classified Technical Library controlled materials shall not destroy or transfer their custody. Classified Technical Library controlled materials shall be returned to the Library as soon as they have served their purpose.

CHAPTER 6. Hand Carry of Classified Material On and Off Center

6.1 Hand Carry of Classified Material Between Work Areas Within LaRC

Branch or office supervisors may approve (verbal authorization) hand carry of classified material between LaRC on-Center work areas. Personnel performing hand carry of classified material on the Center will take reasonable precautions to protect the materials being transported. As a minimum, classified materials hand carried within the Center shall have an appropriate cover sheet attached and be enclosed in an opaque container, envelope or briefcase.

6.2 Courier Authorization

In addition to branch or office supervisor approval, the LaRC ISPM shall approve all hand carry of classified material outside the perimeter of LaRC. This includes travel to and from Langley Air Force Base. LaRC employees shall provide to the LaRC ISPM a minimum of two working days prior notice of intent to hand carry classified material outside the Center. They shall request courier authorization and provide travel information using NASA Langley Form 186, "Request to Hand Carry Classified Materials Outside the Boundary of NASA Langley Research Center." Personnel requesting courier authorization may send their completed Langley Form 186 via email or facsimile to the Center Security & Program Protection Services. All personnel will execute a NASA Langley Form 187, "NASA Langley Research Center Courier Briefing Statement" prior to hand carry of classified materials off Center property. LaRC employees performing frequent hand carry of classified material off the Center property may qualify for a continuous courier authorization letter.

CHAPTER 7. Destruction

7.1 Procurement of Destruction Equipment

The LaRC ISPM shall approve all requests for procurement of equipment intended for use in the destruction of any type of classified materials. Acquisition requests shall be routed through the ISPM with a description of the destruction device, the approximate volume (per month by number of pages or cubic feet) and type of materials (e.g., paper, microfiche, data storage media) anticipated to be destroyed.

7.2 Approval of Equipment for Classified Destruction

Destruction equipment meeting specifications for the destruction of classified materials shall be posted indicating that the equipment may be used for that purpose. Classified material custodians shall identify destruction equipment, which is intended for use in the destruction of classified material, to the LaRC ISPM for approval prior to use. The LaRC ISPM shall post all destruction equipment as approved or not approved for use in the destruction of classified materials.

7.3 Destruction of Classified Material

Classified material identified for destruction shall be destroyed using equipment approved by the LaRC ISPM. For classified paper documents, crosscut shredders and the Center pulping device may be used. The Center pulping device is normally used for a large volume of classified paper products and is located in the Duplicating Facility in Building 1152. Do not use shredders or the pulping facility for the destruction of microfiche or removable data storage media. For these types of classified materials or any classified items not suitable for destruction by shredding or pulping, contact the LaRC ISPM for proper methods of destruction.

7.4 Records of Destruction

Unless classified material is controlled by a mandatory administrative accountability system, records of destruction are not required for Confidential or Secret material. Classified material custodians shall ensure two appropriately cleared individuals destroy Secret material and one appropriately cleared individual destroys Confidential material. To meet the Secret destruction criteria, classified custodians shall ensure a second person from their work area witnesses the physical destruction of the material or, if sending the material for destruction at the Center pulping facility, the sealing of the material in a box or container for transport to the destruction facility. The Classified Material Destruction Verification Record, NASA Langley Form 454, shall be used as a receipt and verification that classified materials have been transported to the Center pulping facility and properly destroyed. Contact the Center TSCO for destruction of Top Secret materials.

7.5 Procedures for Use of Bulk Pulping Destruction Facility

Only properly trained and appropriately cleared personnel tasked through the Center classified custodian contractor may use the Center pulping equipment.

7.5.1 Classified custodian responsibilities:

7.5.1.1 Classified custodians shall properly package in an opaque container, such as cardboard boxes or envelopes, all classified materials identified for destruction at the Center pulping facility. Custodians will remove all metal objects, such as paper clips, spring clips and other items that might interfere with the proper destruction of the material or cause damage to the pulping equipment. Where Secret level classified material is involved, custodians will ensure a second, properly cleared individual witnesses the identification and packaging of the materials for transport and destruction. The Center classified material destruction contractor may not be used to destroy classified material above the Secret level. Package materials shall be securely closed with reinforced tape and posted with the appropriate classified coversheet or conspicuously marked with the highest classification of the material enclosed. Packaged materials will be properly safeguarded until receipted by the Center classified contractor tasked with classified material destruction.

7.5.1.2 Custodians shall prepare and attach to the packaged material a Delivery Ticket (NASA Langley Form 68) addressed to the Center pulping facility. The tag shall be marked with the classification of the material identified for destruction. The classified custodian will also prepare and attach a completed NASA Langley Form 454, "Classified Material Destruction Verification Record," which will be used by the contractor to receipt and verify the destruction of the packaged materials. The classified custodian need only describe the package(s) that are being receipted to the contractor classified destruction personnel. For example, "One cardboard box, approximately 2'x2' containing Secret materials." The NASA Langley Form 454 will reflect the signatures of the classified custodian and the official witnessing the packaging of the materials.

7.5.1.3 The custodian shall contact Delivery Services to arrange pickup and delivery to the Center pulping facility. The classified custodian must EXPLICITLY state that the material is classified and is intended for destruction at the Center pulping facility.

7.5.1.4 Classified custodians shall verify through the Delivery Services office that those individuals that arrive to pickup the packaged classified materials are granted the appropriate level of security clearance. The packed materials will be receipted to the contractor classified destruction personnel by signature in the "Received By" block of the NASA Langley Form 68. A copy of the completed NASA Langley Form 454, describing the materials to be destroyed, will accompany the packaged materials released to the destruction contractor employees. The contractor classified destruction

personnel will certify the destruction of material by completing the appropriate block of NASA Langley Form 454 and returning the form to the requesting classified custodian.

7.5.2 Classified material destruction contractor responsibilities:

7.5.2.1 Only contractor employees granted a security clearance at the Secret level or higher and trained to operate the Center pulping equipment may be assigned classified material pickup and destruction duties.

7.5.2.2 All classified materials shall be destroyed on the day of pickup. In the event of equipment malfunction, classified materials will be returned to the owning classified custodian for safeguarding pending the availability of the pulping equipment.

7.5.2.3 Contractor employees tasked with classified material destruction responsibilities shall provide appropriate classified material safeguarding until the destruction process is complete. Once retrieved from the owning classified custodian, one appropriately cleared contractor employee will maintain constant observation of the packed materials. At no time will classified materials be left unattended. Only appropriately cleared personnel may be in the vicinity of the destruction equipment during the classified destruction process. Two appropriately cleared contractor employees will perform the classified material destruction, verify all materials have been destroyed, certify the destruction by signature in the appropriate block of the NASA Langley Form 454 and return a signed copy of the form to the owning classified material custodian.

7.5.2.4 The contractor using the Center pulping device shall follow equipment instructions to ensure proper destruction of the material and prevent damage to the pulping equipment.

7.6 Destruction of Administratively Controlled Information (ACI) and Other Sensitive, But Unclassified Information

7.6.1 Types of information applicable for protection under ACI authority are provided in NPD 1620.1. ACI and other sensitive, but unclassified information warranting safeguards from disclosure shall be destroyed as described below.

7.6.2 All such information identified for destruction shall be appropriately protected until properly destroyed. Boxed or packaged information will be under observation or secured pending destruction by the custodian or receipt by Center Delivery Services. Do not place ACI information in recycle type receptacles.

7.6.3 DO NOT destroy Federal Records. The definition of Federal records is contained in the “Introduction” section of NPR 1441.1, “NASA Records Retention Schedules.”

Refer to NPR 1441.1, NPD 1440.6, "NASA Records Management," LAPD 1440.6, "Records Management" and LMS-CP-2707, "Records Management" or check with the Center Records Management Officer.

7.6.4 ACI and other sensitive, but unclassified information shall be destroyed either by shredding using office strip-cut or cross-cut shredders or by incinerating at the Center's Trash Burning Facility. Records of destruction are not required.

7.6.5 Use the following procedures to arrange for the destruction of ACI and sensitive, but unclassified information, at the Center Trash Burning Facility:

7.6.5.1 Items identified for destruction shall be packaged in a cardboard box or envelope. The package shall be securely closed with reinforced tape, posted with the appropriate sensitive material coversheet (use NASA Form 1686, “Administratively Controlled Information (ACT),” or NASA Form 1534, “Privacy Act of 1974 Sheet”) and marked in a conspicuous manner as “SENSITIVE MATERIAL TO BE BURNED."

7.6.5.2 Attach a Delivery Ticket (NASA Langley Form 68) addressed to Trash Incinerator Facility for destruction (EXPLICITLY state in the "Material" block: SENSITIVE MATERIAL TO BE BURNED).

7.6.5.3 Contact Delivery Services to arrange for pickup and delivery to the Trash Incinerator Facility for destruction (EXPLICITLY state that the material is for destruction at the incinerator). Provide information on the number of containers that have been designated for destruction, who is the requester, telephone number and building and room where the material may be picked-up.

CHAPTER 8. Security Infractions and Violations

8.1 Philosophy

The true indicator of a healthy security environment is the prompt reporting of security infractions and violations and the identification and correction of inadequate procedures. In the case of all security violations, the most important factor is to determine if a loss or compromise occurred.

8.2 Security Infractions

Security infractions are minor deviations from proper administrative marking or classified handling procedures. They do not result in classified material being in a non-secure environment or possibly exposed to view by an unauthorized individual. Security infractions should be corrected at the work area level or through the OU classified information security representative.

8.3 Security Violations

Security violations are any incidents where classified information or material has or may have been exposed to loss or compromise. Security violations must be reported immediately to the OU classified information security representative, the OUM and the CCS. Security violations include, but are not limited to, security containers or secure storage rooms left open and unattended, classified material left unattended in any non-secure environments, classified material left in non-secure reproduction equipment or any event where classified material that is improperly handled, stored or transmitted could have been viewed by unauthorized personnel.

8.4 Inquires and Investigations

Upon receiving a report of a security violation, the CCS will appoint a qualified government employee from the Center security staff to conduct an administrative inquiry. The administrative inquiry is the initial process to determine the facts surrounding the possible loss or compromise of CNSI. The inquiry official shall gather information by evaluating the circumstances leading up to the occurrence of the violation, interview persons with information relevant to the violation, assess possible weaknesses in security practices and determine any possible opportunities that unauthorized persons may have had access to the affected CNSI. The preliminary inquiry is an administrative process and the inquiry official need not take official statements from those being interviewed. Within five business days of appointment, the inquiry official will provide a written report to the CCS with an assessment of the possibility of loss or compromise of the affected CNSI, causative practices or behavior that led to the violation, assign responsibility for identified failures to follow procedures and recommendations to prevent future violations. The CCS may direct a more comprehensive investigation where significant evidence presented in the administrative inquiry suggests CNSI was lost or compromised and that a more thorough investigation

is likely to contribute significant additional information to resolve the issue. Such investigations shall be conducted in accordance with NPD 1660.1, paragraph 5(2), and normally shall include sworn statements, collection of documentary evidence and the preparation of a report that includes findings of fact, conclusions and recommendations. Inquiry reports requiring corrective action shall be forwarded to the appropriate responsible supervisor or manager.

Where loss or compromise of CNSI is probable or confirmed, the original classification authorities for the affected information will be notified of the need for a damage assessment.