



Langley Research Center

**Directive: LPR 1620.1C**

**Effective Date: June 20, 2014**

**Expiration Date: May 31, 2019**

## **Information Security Program Management Procedures and Guidelines**

National Aeronautics and Space Administration

Verify the correct revision before use by checking the LMS Web site.

- CHAPTER 1. OVERVIEW ..... 1
- CHAPTER 2. RESPONSIBILITIES ..... 2
- CHAPTER 3. HANDLING AND SAFEGUARDING CNSI ..... 3
  - 3.1 Prerequisites to Access ..... 3
  - 3.2 CNSI Work and Storage Areas ..... 3
  - 3.3 CNSI Marking Standards ..... 3
  - 3.4 Working Papers Containing CNSI ..... 3
  - 3.5 Reproduction of CNSI ..... 4
  - 3.6 Storage of CNSI..... 5
  - 3.7 Safe Contents and Combinations..... 5
  - 3.8 End of Work Day Inspections..... 6
  - 3.9 Emergency Actions..... 6
- CHAPTER 4: DESTRUCTION OF CLASSIFIED NATIONAL SECURITY INFORMATION..... 7
  - 4.1 Procedures for Designation of CNSI Destruction Areas and Equipment..... 7
  - 4.2 Procedures for Use of the Bulk Destruction Facility..... 7
  - 4.3 Documenting the Destruction of CNSI..... 8
- CHAPTER 5: TRANSMISSION, MAILING, TRANSPORTING AND COURIER PROCEDURES FOR CNSI ..... 9
  - 5.1 Handling of Incoming Deliverable CNSI ..... 9
  - 5.2 Handling of Outgoing CNSI Mail ..... 9
  - 5.3 Authorized Mailing Modes for CNSI ..... 10
  - 5.4 Transporting CNSI with the LaRC ..... 11
  - 5.5 Transporting CNSI outside of LaRC..... 11
- CHAPTER 6: SECURITY AWARENESS TRAINING FOR ACCESS AND HANDLING OF CNSI ..... 13
  - 6.1 Initial Security Orientation Training and Indoctrination Briefing..... 13

- 6.2 Annual Security Refresher Training for Access and Handling of CNSI .....13
- 6.3 Specialized CNSI Security Training .....14
- 6.4 Security Termination Briefings from Access to CNSI.....14
- CHAPTER 7: SECURITY INCIDENT AND VIOLATION PROCEDURES INVOLVING CNSI ....15
  - 7.1 Security Incident and Violation Defined.....15
  - 7.2 Reporting Security Incidents and Violations .....15
  - 7.3 Security Incident and Violation Inquiries and Investigations .....16
- CHAPTER 8: INDUSTRIAL SECURITY ADMINISTRATIVE REQUIREMENTS AND THE DD FORM 254.....17
  - 8.1 Administration of LaRC Federal Classified Cleared Contracts .....17
  - 8.2 Administration and Management of DD Form 254 for LaRC Federal Classified Cleared Contracts.....17

## 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 local responsibilities, supplemental procedures, and guidance applicable to Langley Research Center. CNSI designated as Sensitive Compartment Information (SCI), Top Secret, or Special Access Required (SAR) shall be exempt from the requirements set forth in this directive.

## P.2 APPLICABILITY

- a. This directive is applicable to all federal employees, contractors, and tenants at Langley Research Center who access CNSI.
- b. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms: “may” or “can” denote discretionary privilege or permission, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive material.
- c. In this directive, all document citations are assumed to be the latest version, unless otherwise noted.

## P.3 AUTHORITY

- a. Executive Order 12968, “Access to Classified Information”
- b. Executive Order 13526, “Classified National Security Information”
- c. 14 CFR, Part 1203, “Information Security Program”
- d. 32 CFR, Part 2001, “Classified National Security Information, Final Rule”
- e. 32 CFR, Part 2003, “Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures”
- f. 32 CFR, Part 2004, “National Industrial Security Program Directive No. 1”

## P.4 APPLICABLE DOCUMENTS AND FORMS

- a. Information Security Oversight Office, “Marking Classified National Security Information” Guide
- b. NPD 1440.6H, “NASA Records Management”
- c. NPD 1600.2E, “NASA Security Policy”
- d. NPR 1441.1D, “NASA Records Retention Schedules”
- e. NPR 1600.1A, “NASA Security Program Procedural Requirements”
- f. NPR 1600.2, “NASA Classified National Security Information (CNSI)”
- g. Advisory Circular, “Federal Aviation Administration, Subject: Screening of Persons Carrying U.S. Classified Material, AC 108-3”
- h. DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)”

- i. NASA Declassification Management Plan
- j. NASA Handbook for Writing Security Classification Guides
- k. DD Form 254, "Department of Defense Contract Security Classification Specification"
- l. NF 387, "Classified Material Receipt"
- m. LF 186, "Classified Material Courier Request"
- n. LF 187, "NASA Langley Research Center (LaRC) Courier Briefing" Statement/Hand Carry of Classified Information Aboard Commercial Airline"
- o. LF 454, "Classified Material Destruction Verification Record"

#### P.5 MEASUREMENT/VERIFICATION

None

#### P.6 CANCELLATION

LPR 1620.1, dated May 23, 2005

*Original signed on file*

Virginia C. Wycoff  
Associate Director

#### **Distribution:**

Approved for public release via the Langley Management System; distribution is unlimited.

## **CHAPTER 1. OVERVIEW**

1.1. NASA Langley Research Center (LaRC) generates, receives, disseminates, and maintains an enormous amount of information. Much of this information is unclassified/non-sensitive in nature, with few restrictions on its use and dissemination.

1.2. NASA LaRC also generates, receives, stores, disseminates, and maintains Classified National Security Information (CNSI) under a variety of agency programs, projects, partnerships, and collaborations with other federal agencies, academia, and private enterprises.

1.3. In accordance with Executive Order 13526, 32 CFR Part 2001, and NPR 1600.2, procedures shall be established for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying CNSI generated or possessed by the Center.

## **CHAPTER 2. RESPONSIBILITIES**

2.1. The Center Director is responsible, through the Center Chief of Security (CCS) for ensuring proper planning and implementation of E.O. 13526 is accomplished through the provisions outlined in NPR 1600.1A and NPR 1600.2 for all CNSI material in the custody and control of the Center.

2.2. The CCS is responsible for ensuring that an information security program for CNSI is developed, implemented, and maintained to meet the requirements addressed in national and agency guidance and instructions.

2.3. The CCS appoints an individual from the Security Services Branch (SSB) as the Classified Material Control Officer (CMCO). The CMCO and appointed alternates are responsible for ensuring that all CNSI (SECRET/CONFIDENTIAL) received or generated by LaRC is safeguarded in accordance with all federal and agency directives and procedures.

2.4. Individuals who handle CNSI shall be trained in the requirements and procedures for accessing, handling, protecting, accounting, and safeguarding CNSI as directed by federal and agency directives and procedures.

2.5. The LaRC Records Manager shall serve as the determining agent regarding the retention of CNSI within applicable federal and agency archives.

## **CHAPTER 3. HANDLING AND SAFEGUARDING CNSI**

### **3.1 Prerequisites to Access**

3.1.1. Individuals shall meet three mandated conditions before being granted access to CNSI:

3.1.1.1. A federally conducted background investigation that results in a favorable adjudication, granting eligibility for CNSI access by a recognized federal adjudicative authority.

3.1.1.2. Authorization from a cognizant authority for a level of CNSI clearance equal to or greater than the level of classified information the individual is allowed to access, accompanied by a signed Standard Form 312, "Classified Information Non-disclosure Agreement," from the authorized individual.

3.1.1.3. A demonstrated "need to know" for the information to be accessed, based strictly on the need for the individual to complete assigned duties.

### **3.2 CNSI Work and Storage Areas**

3.2.1. CNSI shall be stored and maintained only in areas designated and certified through the CMCO. These areas will be designated either as "Limited" or "Exclusion" areas, as defined in NPR 1600.2.

### **3.3 CNSI Marking Standards**

3.3.1. CNSI that is generated, regardless of media type or form, shall be properly marked as directed by federal and agency regulations, guidance, and procedures. Marking of CNSI should be consistent with instructions as outlined in the Information Security Oversight Office reference, "Guide to Marking Classified Documents," dated December 2010.

3.3.2. Prior to dissemination to other tenant activities or organizations and agencies outside of NASA, all classified material shall be reviewed by the LaRC CMCO to ensure proper classification and associated marking are applied.

### **3.4 Working Papers Containing CNSI**

3.4.1. Working papers are defined as documents or materials, regardless of media form, that contain CNSI. These documents are generated with the expectation that they will later be revised or incorporated into a developed and finished product for dissemination or retention.

3.4.2. Working papers containing CNSI shall be dated when created; marked to the highest classification level of the material contained within them; protected in a manner commensurate to their classification level; and destroyed as appropriate for the classification level when retention is no longer required.

3.4.3. If the following conditions are present, working papers shall be controlled and maintained in the same manner as required for finalized CNSI documents or material:

3.4.3.1. When released by the originator to entities outside the originating activity.

3.4.3.2. If required to be retained for more than 180 days from the date of origin.

3.4.3.3. If situation or circumstances require originally created documents or material to be filed permanently.

### **3.5 Reproduction of CNSI**

3.5.1. Reproduction of CNSI shall be kept to a minimum. CNSI will be reproduced only on equipment that has been designated and authorized for this function by the CCS. In reproducing CNSI, the following requirements apply:

3.5.1.1. All classified material is protected and safeguarded throughout the reproduction process.

3.5.1.2. Safeguards are in place to ensure all reproduced information is recovered.

3.5.1.3. Over-runs and waste copies of classified material are safeguarded, and unneeded copies are destroyed.

3.5.1.4. Procedures are established to protect and safeguard classified material when other technical or volume reproduction processes are used.

3.5.2. The LaRC CMCO shall evaluate all equipment intended for CNSI reproduction to ensure federal standards and requirements are followed before approval and designation for use.

3.5.2.1. Equipment that has been designated for authorized CNSI reproduction shall be conspicuously marked. Authorization documentation will be affixed to the equipment and posted in the immediate vicinity where the function is conducted.

3.5.2.2. Designated reproduction equipment shall bear identification information, specify any required specialized instructions, and denote the highest level of CNSI classification authorized for reproduction.

3.5.2.3. When designated equipment is no longer authorized for CNSI reproduction, all designation signs will be removed from the machine and its immediate area. The CMCO shall ensure any memory devices or drives present are removed and electronically cleared of electronic data and/or destroyed in accordance with agency and federal directives and standards.

### **3.6 Storage of CNSI**

3.6.1. CNSI maintained by NASA shall be stored in an authorized General Services Administration-approved Classified container with an approved spin-dial combination lock.

3.6.2. CNSI shall be secured only in facilities designated as open storage or in rooms that have been approved and authorized for classified material storage.

3.6.2.1. Open storage facilities shall meet all structural, lock, and alarm requirements outlined in applicable federal and agency guidance and requirements. Such facilities will be used only when a full inspection for compliance has been accomplished by CMCO and such storage has been approved by the CCS.

3.6.3. CNSI shall be stored only in specific, designated containers or open areas that are specifically segregated for classified storage only. CNSI material must never be stored with non-classified items such as valuables, funds, weapons, or drugs.

### **3.7 Safe Contents and Combinations**

3.7.1. A Standard Form 700 is required to be placed inside each designated security container drawer being used for classified storage. The form will list the name(s), address(es), and telephone number(s) of personnel who are designated as Classified Security Container Custodians. Designated container custodians will be government personnel who are knowledgeable of the contents stored in their designated container(s). Container custodians will be contacted and are responsible for responding to assist in the event of a security incident or occurrence involving their assigned container.

3.7.2. Containers that store CNSI will have their combination changed in the following circumstances: when they are first placed into service; when an employee having knowledge of a combination is transferred, departs, or is terminated from employment and no longer has authorized access to the container; or in any situation where a compromise or potential compromise of an existing container and/or its combination is believed to have occurred.

### **3.8 End of Work Day Inspections**

3.8.1. Supervisors of areas where CNSI is handled and stored shall institute procedures for an "End-of-Work Day" area inspection to ensure all classified materials are properly secured. At a minimum, these checks will include desk tops, tables, classified fax machines, classified copying machines, and trash/recycling receptacles located where CNSI is handled, stored, or processed.

3.8.2. All security containers/safes in the area shall be physically checked to ensure they are completely secured and locked. As part of the container check, spin-dial combination locks will be rotated three full spins and each drawer of the container will be physically pulled to ensure it is completely secured and locked. These end-of-day container inspections will be recorded on Standard Form 702, "Security Container Check Sheet" when this check is completed. There is no retention requirement for SF 702.

### **3.9 Emergency Actions**

3.9.1. Current policy requires preparation of plans to assign responsibility and provide direction for the protection of CNSI in the event of local and national emergencies. Examples of emergency contingencies are bomb threats, fire, natural disasters, and any other industrial emergency situation that could be a threat to the safeguarding of CNSI. Prior planning in preparation of emergency situations is needed to establish responsibilities, requirements, and procedures applicable to all employees responsible for safeguarding CNSI.

3.9.2. In any contingency planning for securing CNSI during emergency contingencies, prevention of injury or loss of life will take precedence over any efforts to protect CNSI. If such action can be accomplished safely, personnel should attempt to cover or obscure potentially viewable CNSI.

3.9.2.1. Personnel shall report any situations to the CCS or CMCO in which evacuation of a building or area leaves CNSI in an insecure situation or environment. If at all feasible, emergency responders will be advised prior to entering a building or facility where it is determined that CNSI was not able to be secured, and where the information was left. When practical, emergency responders should be identified in post-response actions if their presence in the facility possibly led to their exposure to CNSI. If exposure is determined, the CMCO will conduct debriefings with responding personnel.

3.9.3. Additional guidance and information relevant to emergency response and contingency actions can be viewed in LPR 1046.1, Appendix I, "Bomb Threats," LPR 1046.1, Appendix H.1.3.1, "Tropical Storms and Nor'easters," and LPR 1710.11, "Fire Protection Program."

## **CHAPTER 4: DESTRUCTION OF CLASSIFIED NATIONAL SECURITY INFORMATION**

### **4.1 Procedures for Designation of CNSI Destruction Areas and Equipment**

4.1.1. The CCS shall establish annual Center-wide events to provide for all CNSI holders to review all holdings and determine if classified material is still required in support of operational and administrative needs. Material no longer needed for support will be dispositioned in accordance with NASA policy.

4.1.2. Classified materials marked as “LaRC Technical Library Controlled Material” shall not be destroyed by holders. This material will be returned to the NASA LaRC Technical Library when it is no longer required for operational needs.

4.1.3. CNSI shall be destroyed only by devices or equipment that has been approved and designated by the CCS. The LaRC should be contacted CMCO for guidance before the acquisition of any equipment or devices intended to be used for destruction of CNSI.

4.1.4. Coordination with the LaRC CMCO is required prior to using any equipment or instruments or designating any areas for the proposed destruction of CNSI. A review of safeguarding procedures, area configuration, and access considerations, as well as designation of authorized destruction equipment or devices, shall be accomplished prior to use.

### **4.2 Procedures for Use of the Bulk Destruction Facility**

4.2.1. Only properly trained and appropriately cleared personnel shall operate the Center’s bulk destruction equipment. Individuals using this equipment will be witnesses to the destruction and are responsible for observing and verifying that the destruction of the material is complete. Personnel tasked with destroying CNSI will ensure material is properly secured at all times, from the time it is removed from its secure container and/or area until it is destroyed.

4.2.2. CNSI shall be packaged in an opaque container such as a box, envelope, or other secure container for transport from its original secure environment to the bulk destruction facility. All normal on-center classified courier transport rules and requirements will be met when transporting CNSI from its secure environment to the destruction facility. Prior to transport, custodians will ensure that staples, paperclips, binder clips, or other metallic devices are removed from the material that is intended to be placed into the destruction equipment.

4.2.3. Personnel shall document all classified destruction accomplished using the Centers Pulp Destruction Equipment on NASA Form 454, Classified Material

Destruction Verification Record (available on the Langley Management System website). This completed document will be returned to the classified custodian releasing the information for destruction upon completion.

### **4.3 Documenting the Destruction of CNSI**

4.3.1. NASA Form 387, Classified Material Receipt (available on the LMS website), shall be used to record the destruction of all other CNSI destruction actions. A completed copy of the form will be provided to and maintained by the classified materials custodian.

## **CHAPTER 5: TRANSMISSION, MAILING, TRANSPORTING AND COURIER PROCEDURES FOR CNSI**

### **5.1 Handling of Incoming Deliverable CNSI**

5.1.1. When arrangements are made with outside organizations or agencies for the mailing of CNSI, or when employees of NASA LaRC are required to mail CNSI back to the Center, the Center's official classified mailing address shall be used:

NASA Langley Research Center  
Attention: Security Office  
Hampton, VA 23681

Upon receipt of such addressed items, the center mail room will contact NASA LaRC SSB designated staff to arrange pick-up or delivery.

5.1.2. Upon pick-up or delivery of packaged material to SSB, the CMCO shall inspect the material to ensure no tampering with the package has occurred. Any suspected tampering will be reported to the CCS, and appropriate inquiry will be initiated.

5.1.2.1. Inspected material will be opened and checked against the enclosed receipt. The CMCO shall determine the intended destination of the material; confirm the eligibility of the addressee to have access to the material; and, if authorization is confirmed, contact the addressee to arrange pick-up.

5.1.2.2. Prior to turning over the material to the addressed recipient, the CMCO shall verify that the individual has a proper container or area in which to secure the CNSI. If proper storage space is verified, the addressee will be provided the material and a receipt will be completed to document transfer of the material. This receipt will be maintained in SSB CMCO files. The addressee will also be provided with a copy of the mailed original receipt accompanying the packed CNSI, instructed to complete and sign the sender's receipt, and required to mail the receipt back to the sender within the next duty day. The CMCO and recipient will each retain a copy of the sender's receipt for 5 years.

### **5.2 Handling of Outgoing CNSI Mail**

5.2.1. CNSI will not be mailed from LaRC without prior coordination with the CMCO. All CNSI shall be properly packaged, marked, and accompanied by required receipts, as directed by the CMCO. CNSI will be marked in compliance with federal standards as outlined in the Information Security Oversight Office (ISOO) "Marking Classified National Security Information" guide. The proper marking of CNSI is the responsibility of the originator of the material.

5.2.2. Prior to mailing, all CNSI shall be packaged with NASA Form 387, parts 1 and 2, enclosed. Part 3 of NASA Form 387 will be maintained by the sender of the CNSI. If a receipt for the mailed material is not received by the LaRC sender within 30 days of mailing, the CMCO will be notified and tracer action will be initiated. Upon receipt of the completed NASA Form 387 from the recipient, the sender will maintain a copy on file.

5.2.2.1. United States Postal Service (USPS) Mail receipts (i.e., Postal Service Form 3811), acknowledging receipt of certified, registered, express, or insured mail, shall not be used in lieu of the NASA Form 387. These forms may be retained to indicate actual mail delivery of the material, but official verification of material receipt and acknowledged custodial change requires completion of NASA Form 387.

### **5.3 Authorized Mailing Modes for CNSI**

5.3.1. Top Secret. Transport of Top Secret material outside of LaRC shall be coordinated through the CMCO. Use of the USPS for mailing Top Secret material is not authorized. CNSI designated as Top Secret will be transported only through authorized local or federal courier procedures or providers.

5.3.2. Secret. This level of CNSI may be mailed through the USPS as registered or certified mail that requires postal service tracking and return receipt. The mailing of this level of material is restricted to the 50 states and U.S. territories.

5.3.2.1. USPS Express Mail Service may be used between NASA units and contractors who are located in the 50 states and US territories. Express Mail is authorized only when the use is the most cost-effective method or when time and/or mission constraints require its use.

5.3.2.2. The CCS may authorize the use of Federal Express delivery in situations where overnight delivery of CNSI to executive branch agencies is required under urgent situations and where delivery is to be made within the 50 states and U.S. territories. Tracking and receipt requirements are still required when such shipments are used.

5.3.3. Confidential. This level of CNSI may be mailed through the USPS by the same means as outlined for Secret-level material. Confidential material may also be mailed using USPS First Class mail between NASA Centers and other U.S. government agencies/locations within the 50 states and US territories. When using this method, the package must be marked "First Class" and must specify "Return Service Requested."

5.3.3.1. Confidential CNSI mailed to federal contractors shall be sent by USPS Registered or Certified Mail.

## **5.4 Transporting CNSI within the LaRC**

5.4.1. LaRC organizational level managers and supervisors may approve the hand carry of CNSI on LaRC between buildings, facilities, and areas.

5.4.2. CNSI hand-carried on LaRC shall, at a minimum, have the appropriate classified level cover sheet placed over the material. The covered material will then be placed into an opaque envelope or folder, container, or briefcase.

5.4.3. Personnel transporting CNSI shall maintain physical custody of the material at all times and take the most direct route from originating point of transport to intended final destination. Detours and stops along the way will be avoided.

5.4.4. Upon reaching the intended destination, personnel transporting and in possession of CNSI are responsible for validating and ensuring the authorization of any others to access or take possession of the material. CNSI transferred from one holder to another shall be properly receipted, using NASA Form 387.

5.4.5. Prior to turning CNSI over to another individual, facility, or area, the individual in possession of the material should ensure that proper security containers, rooms, or areas exist to secure the material prior to transfer.

## **5.5 Transporting CNSI outside of LaRC**

5.5.1. All CNSI requiring physical transport off LaRC shall be coordinated and approved by LaRC organizational level managers and supervisors who have cognizant authority over the material to be transported. If at all practical, alternative means of communicating CNSI should be considered over physical carry (i.e. appropriate classified electronic transmission or mail).

5.5.2. Prior to the physical transport of any CNSI across the perimeter of and outside NASA LaRC, the CMCO shall be contacted for coordination of CCS approval. This includes transport of material to Langley Air Force Base.

5.5.2.1. All requests for off-Center CNSI transport shall be submitted to the CMCO using Langley Form 186, Classified Material Courier Request. Personnel delegated to transport CNSI off-center will receive the necessary training and briefing for issue of Langley Form 187, NASA Langley Research Center (LaRC) Courier Briefing Statement/Hand Carry of Classified Information Aboard Commercial Airline. The CMCO will also provide the CCS with a signed Classified Courier Designation Letter.

5.5.2.2. The Classified Courier Designation Letter will outline the responsibilities, provisions required, and actions prohibited when taking CNSI off-Center. If the transport is to be accomplished using commercial air travel, coordination with the CMCO is

required at least three days prior to the departure date. Transporting of CNSI on commercial airlines must be coordinated with the Transportation Security Administration under guidance provided in Federal Aviation Administration Circular 108-3, Subject: Screening of Persons Carrying U.S. Classified Material.

5.5.3. LaRC employees who have a frequent need to hand-carry CNSI off-Center should contact the CMCO for issue of a long-term Courier Authorization Letter.

## **CHAPTER 6: SECURITY AWARENESS TRAINING FOR ACCESS AND HANDLING OF CNSI**

### **6.1 Initial Security Orientation Training and Indoctrination Briefing**

6.1.1. In accordance with Federal and NASA directives and guidance, the LaRC CCS is responsible for developing initial orientation training for all NASA Civil Servant personnel granted access authorization to CNSI. Prior to clearance, holders being authorized to access and handle CNSI shall attend training covering such topics as roles and responsibilities in accessing and handling CNSI, definition and management of CNSI, and requirements and processes mandated for safeguarding CNSI.

6.1.1.1. The CMCO shall schedule identified NASA Civil Servant personnel who have been granted access to CNSI for initial orientation training and, upon completion, conduct the required indoctrination briefing. When individuals have completed both the orientation training and indoctrination briefing, the CMCO will ensure completion of Standard Form 312, Classified Information Non-Disclosure Agreement/Security Debriefing Acknowledgement, by the classified clearance holder.

6.1.1.2. Initial security orientation training and indoctrination of NASA federal contractor personnel is the responsibility of the individuals' employing company in accordance with the National Industrial Security Program Operational Manual, DoD 5200.22-M.

### **6.2 Annual Security Refresher Training for Access and Handling of CNSI**

6.2.1. Federal and NASA directives and guidance require that all active, eligible personnel granted access to CNSI and holding a security clearance must complete annual refresher training covering guidance and requirements for access, managing and handling CNSI. This training also applies to all NASA-assigned federal contractors who are actively cleared for and under contractual requirements to access CNSI under NASA control to accomplish their jobs. Guidance and assistance in developing this training may be obtained by contacting the CMCO.

6.2.1.1. Annual Security Refresher Training is currently provided as an automated lesson, accessible through the NASA SATERN training site. This is the preferred method for LaRC-assigned personnel to complete the required training. Organizational managers and supervisors should contact the CMCO in situations where use of the SATERN training modules may not be feasible.

6.2.2. LaRC organizations and offices that maintain and work with CNSI within their work areas shall develop and conduct annual training with their assigned cleared personnel on the procedures, rules, and processes related to their area's operations for maintaining and handling CNSI. Such topics as area end-of-day checks, reproduction policies and procedures, and destruction procedures should be addressed.

### **6.3 Specialized CNSI Security Training**

6.3.1. Federal and NASA Guidance requires personnel who are authorized to make Derivative Classification determinations involving CNSI to be specifically trained on the rules and procedures dictated for this process, as outlined in 32 CFR, Parts 2001 and 2003. Derivative Classification determinations are defined as the extraction, summarizing and marking of CNSI derived from an originating source of the information into another separate source. Those personnel performing derivative classification determinations must receive recurring two-year training to maintain currency. The CMCO should be contacted for guidance and assistance.

6.3.2. Other commonly required specialized training includes Classified Custodian Training, Destruction Procedures for CNSI, and Use of CNSI-Authorized Transmission Equipment and Devices. The CMCO can provide guidance and assistance for any training requirements pertaining to access and handling of CNSI.

### **6.4 Security Termination Briefings from Access to CNSI**

6.4.1. When NASA Civil Servant personnel who hold access authorization to CNSI are no longer required or authorized to maintain this access, a classified security debriefing should be conducted. Personnel who are debriefed should be afforded the opportunity to ensure all classified material they may have possessed be properly transferred to an authorized classified holder. This briefing also affords NASA the opportunity to remind personnel of their continued responsibilities to ensure that CNSI they have knowledge of is protected from unauthorized release. Confirmation of the debriefing is accomplished by completion of the debriefing section on an individual's originally signed Standard Form 312. Personnel should contact the CMCO to complete required CNSI debriefings.

## **CHAPTER 7: SECURITY INCIDENT AND VIOLATION PROCEDURES INVOLVING CNSI**

### **7.1 Security Incident and Violation Defined**

7.1.1. Security incidents are those occurrences or deviations from established security procedures in which there is a potential degradation of protection to CNSI. Common situations include a failure to conduct end-of-day checks; the use of improper cover sheets on classified material; or a failure to properly annotate security container opening, closing, and checks when required. Such occurrences pose no direct threat of loss or compromise of CNSI, but rather create an environment where potential trust and confidence in existing protection standards may be degraded.

7.1.2. Security violations are those occurrences that violate specific provisions of security requirements or where there is an actual or highly probable belief that an unauthorized disclosure of CNSI.

7.1.2.1. Classified Spills (also referred to as “contaminations” or “classified message incidents”) occur when CNSI is introduced onto unauthorized/uncertified information technology systems where access to the information may be obtained by a person or persons not authorized access. Classified Spills can also occur where CNSI of a particular level is introduced onto a system not authorized to that level of classification. An example would be the placing of CNSI classified at the Top Secret level on a system authorized for CNSI only at the Secret level.

7.1.3. A compromise of CNSI is defined as a situation in which the actual or highly likely physical loss or unauthorized access and exposure of CNSI to unauthorized parties is validated. All situations involving a potential compromise of CNSI must be reported to and investigated by SSB to determine the potential damage to national security and the development of actions to mitigate further damage.

### **7.2 Reporting Security Incidents and Violations**

7.2.1. Personnel who observe situations in their work environments that they determine pose a security concern related to the protection of CNSI (see 7.1.1 above) shall report their concerns to their area manager, supervisor, or appropriate classified custodian. Assistance and guidance from the CMCO can always be obtained upon request.

7.2.2. When personnel observe a situation and determine that a potential security violation exists concerning CNSI, they shall take immediate steps to secure and protect the information in question from further potential or actual unauthorized exposure.

7.2.2.1. Personnel shall immediately report potential security violations of CNSI to their organizational management, supervisor or appropriate classified custodian. The SSB

will also be notified immediately. During normal duty hours, contact should be made to the CMCO. If the potential violation occurs after duty hours or on weekends or holidays, notification should be made immediately to the Security Services Control Center (Security Dispatcher) at 864-5500.

7.2.2.2. The CMCO or designated SSB representative shall determine whether an SSB response is required. Response will be based on the circumstances surrounding the situation. Factors that may be considered to determine an immediate response include whether the classified information can be secured at the incident location, and whether key individuals involved in the situation have been identified for later interview.

7.2.2.3. Should origin of the information or responsible custodian not be determined at the time of the incident, a Security Officer shall be dispatched to safeguard the information until the SSB/CMCO can determine how the material will be maintained and secured.

7.2.4. If it is determined that a security violation or suspected compromise involving CNSI has occurred, the CCS or CMCO shall notify NASA HQ OPS with 24 hours of the reported incident. A preliminary appraisal of the incident will be provided. If a formal investigation/inquiry is opened by the CCS, NASA HQ OPS will be provided with the final report after any initiated inquiries or investigations are completed.

### **7.3 Security Incident and Violation Inquiries and Investigations**

7.3.1. The CCS shall appoint, in writing, a Security Specialist from the SSB staff to conduct any necessary inquiries regarding security incidents and violations involving CNSI. Inquiry Officers will identify and contact the parties involved in the incident. Interviews and statements will be gathered to determine the facts and circumstances that led to the security incident/violation. Analysis of the facts will be made to determine to what degree potential or actual compromise of CNSI occurred. The inquiry will also establish what immediate and long-term corrections will be needed to facilities, processes, and procedures to mitigate and prevent future occurrences.

7.3.2. In cases where sufficient facts indicate a serious breach in the security of CNSI, and where compromise of CNSI is indicated, the CCS shall notify the LaRC Counterintelligence(CI) office and the Office of Inspector General (OIG).

7.3.2.1. In situations where a confirmed or a highly probable compromise of CNSI is indicated, the original classification authority of the classified material shall be notified and an assessment of damage will be requested. In such instances where compromise is probable or confirmed, a full investigation will be conducted and a copy of the report provided to HQ NASA OPS as required under NPR 1600.2.

## **CHAPTER 8: INDUSTRIAL SECURITY ADMINISTRATIVE REQUIREMENTS AND DD FORM 254**

### **8.1 Administration of LaRC Federal Classified Cleared Contracts**

8.1.1. Federal contracts that require access to CNSI are identified through the Office of Procurement. These contracts are designated as classified cleared contracts and administered under the laws and rules outlined in the National Industrial Security Program Operations Manual (NISPOM).

8.1.1.1. Companies operating under designated NASA classified cleared contracts shall be assigned a Facility Clearance (FCL) granted by the Defense Security Service (DSS) and possess a valid Commercial and Government Entity (CAGE) Code identifier.

8.1.1.2. In cases where a contract company is identified as the prime provider on a NASA classified contract, but lacks the required DSS requirements, the CCS may direct the CMCO to assist the company in coordinating with DSS to acquire the necessary vetting and authorization to perform under a government classified contract.

8.1.2. The CMCO is the CCS point of contact on matters pertaining to LaRC classified contractors and the Office of Procurement (OP).

8.1.2.1. The CMCO maintains coordination on classified contract matters with the classified company-designated Facility Security Officers (FSO), OP Contracting Officers (CO), and OP Contracting Officers Representatives (COR).

8.1.2.2. LaRC classified cleared contractors are responsible for managing and maintaining oversight of any classified cleared sub-contractors under their control and direction.

8.1.2.3. The CMCO will monitor and conduct, as deemed necessary, periodic reviews of LaRC assigned classified cleared contractors and their associated classified cleared sub-contractors.

### **8.2 Administration and Management of DD Form 254 for LaRC Federal Classified Cleared Contracts**

8.2.1. The CMCO shall manage and coordinate with COs and CORs on all newly initiated, modified, and annually validated DD Forms 254 for LaRC classified clearance contract companies.

8.2.1.1. An annual revalidation of the FCL for all LaRC prime and sub classified cleared contractors shall be conducted by the CMCO through coordination with OP. These reviews will be documented on the classified clear contract's DD Form 254.

8.2.1.2. Once OP has verified existing active LaRC classified cleared prime and sub contracts, the CMCO shall validate these companies' current FCL status via the DSS Industrial Security Facilities Database (ISFD).

8.2.1.3. The CMCO shall work through each classified cleared contract's CO, COR, and company FSOs to ensure an up-to-date Classified Visit Authorization Request (VAR) lists all authorized classified cleared contract employees and reflects the necessary data to indicate that each employee meets the investigative requirements for the classified clearance level they hold. The VAR will be accepted only if it contains the required information, in the format directed in the NISPOM.

8.2.1.4. Whenever a change is made to security classification specifications pertaining to a current prime classified cleared contract, OP shall ensure, through coordination with the CMCO, that such changes are reflected in the contracting company's DD Form 254. It will be the responsibility of the prime classified contractor to ensure any subsequent changes in the security classification specifications of their associated sub-contracts meet documentation requirements as specified in NISPOM guidance.

8.2.1.5. Item 12 of DD Form 254 shall be modified to reflect the current instruction: "To the Office of Communications, National Aeronautics and Space Administration, Washington, DC 20546, for review."