



# **NASA Procedural Requirement**

**NPR 2810.7**

Effective Date: October 22, 2021  
Expiration Date: October 22, 2026

**Subject: Controlled Unclassified Information**

**Responsible Office: Office of the Chief Information Officer**

## **Table of Contents**

### **Preface**

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

### **Chapter 1. Introduction**

- 1.1 Overview
- 1.2 Responsibilities

### **Chapter 2. CUI Management**

- 2.1 General
- 2.2 Marking of CUI
- 2.3 Portion Marking (Optional)
- 2.4 Comingling CUI Markings with Classified National Security Information (CNSI) Markings
- 2.5 Legacy Materials
- 2.6 Working Papers
- 2.7 Using Supplemental Administrative Markings with CUI
- 2.8 Unmarked CUI
- 2.9 Sharing of CUI (Accessing and Disseminating)
- 2.10 CUI Disclosure Statutes
- 2.11 Challenges to Designation of Information as CUI
- 2.12 Decontrol of CUI
- 2.13 Safeguarding and Storage
- 2.14 Reproduction of CUI
- 2.15 Shipping or Mailing CUI

- 2.16 Transmittal Document Marking Requirements
- 2.17 Destruction of CUI
- 2.18 Misuse of CUI and Incident Reporting
- 2.19 Sanctions for Misuse of CUI
- 2.20 CUI Within Information Systems
- 2.21 CUI Self-Inspection Program
- 2.22 Waivers to CUI Requirements
- 2.23 CUI Education and Training

**Appendix A. Definitions**

**Appendix B. Acronyms**

**Appendix C. Web Resources**

# **Preface**

## **P.1 Purpose**

- a. This directive establishes Agency-wide requirements for the protection of Controlled Unclassified Information (CUI).
- b. This directive outlines personnel responsibilities and procedural requirements for the management of CUI to assist NASA Centers and Component Facilities in executing the NASA CUI program designed to protect people, property, and information.
- c. This directive establishes Agency procedures for the proper implementation and management of a uniform system for categorizing, safeguarding, and decontrolling CUI generated by, for, or in the possession of NASA.
- d. All unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI. CUI serves as the exclusive designation for identifying and controlling such unclassified information throughout NASA. All safeguarding or dissemination controls for unclassified information will be consistent with the CUI Program.

## **P.2 Applicability**

- a. This directive is applicable to NASA Headquarters and all NASA Centers, including Component Facilities, Federally Funded Research and Development Centers (FFRDCs) and Technical and Service Support Centers.
- b. This directive is applicable to all NASA civil service employees who require access to CUI in the performance of their duties.
- c. Consistent with Controlled Unclassified information (CUI), Accessing and Disseminating, 32 CFR § 2002.16; and Chapter 2 of this directive, the requirements of this directive should be made applicable to all individuals and entities with whom NASA shares or intends to share CUI, including:
  - (1) Government owned, contractor operated (GOCO) facilities;
  - (2) Partners under the Space Act;
  - (3) Partners under the Commercial Space Act of 1997;
  - (4) Partners under cooperative agreements; or
  - (5) Commercial or university facilities.
- d. All document citations in this directive are assumed to be the latest version unless otherwise noted.
- e. 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 materials.

### **P.3 Authority**

- a. The National Aeronautics and Space Act, 51 United States Code (U.S.C.) § 20132.
- b. Executive Order (E.O.) 13556, Controlled Unclassified Information.
- c. Controlled Unclassified Information, 32 CFR pt. 2002.

### **P.4 Applicable Documents and Forms**

- a. Freedom of Information Act (FOIA), 5 U.S.C § 552.
- b. Privacy Act of 1974, 5 U.S.C. § 552a.
- c. Whistleblower Protection Act, 5 U.S.C. § 2302.
- d. Accessing and Disseminating, 32 CFR § 2002.16.
- e. NASA Policy Directive (NPD) 2521.1, Communications and Material Review.
- f. NASA Procedural Requirement (NPR) 1600.2, NASA Classified National Security Information (CNSI).
- g. NPD 1440.6, NASA Records Management.
- h. NPR 1441.1, NASA Record Management Program Requirements.
- i. NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.
- j. NPR 8000.4, Agency Risk Management Procedural Requirements.
- k. NPR 9710.1, General Travel Requirements.
- l. National Archives and Records Administration (NARA) CUI Marking Handbook (<https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>).
- m. NASA CUI Handbook ([https://cset.nasa.gov/wp-content/uploads/2021/05/ITS-HBK-CUI\\_v1.0.0.pdf](https://cset.nasa.gov/wp-content/uploads/2021/05/ITS-HBK-CUI_v1.0.0.pdf)).
- n. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 (FIPS PUB 199).
- o. NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 (FIPS PUB 200).
- p. NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020 (updated 12-10-2020) (NIST SP 800-53).
- q. NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, December 2014 (NIST SP 800-88).

r. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 2, February 2020.

## **P.5 Measurement/Verification**

a. To determine Center compliance with E.O. 13556, Controlled Unclassified Information, 32 CFR pt. 2002, and this directive, NASA HQ, Mission Directorates, Center Directors, and Center Chief Information Security Officers (CISOs) will determine and document compliance through annual self-assessments (see self-inspections at 2.21) and reviews conducted by the Office of the Chief Information Officer (OCIO). Each year OCIO will provide guidance from the CUI Executive Agent to help the Center CUI Liaisons complete the self-inspection process for their organization.

b. The NARA Information Security Oversight Office (ISOO), as the CUI executive agent, maintains continuous relationships with agency counterparts on all matters relating to the CUI Program and 32 CFR pt. 2002. ISOO also conducts on-site assessments to monitor agency compliance. Each year ISOO gathers statistical data regarding each agency's security classification program. ISOO analyzes and reports this data, along with other relevant information in its Annual Report to the President. NASA follows ISOO guidance and is subject to ISOO inspections and reviews.

c. Internal and external auditors responsible for ensuring Agency compliance and effective implementation of the E.O. 13556 will evaluate the NASA CUI program.

## **P.6 Cancellation**

a. NASA Interim Directive (NID) 1600.54, Safeguarding Sensitive But Unclassified Information (SBU), dated October 2, 2007.

b. NID 1600.55, Sensitive But Unclassified (SBU) Information, dated October 16, 2007.

c. NID 2810.135, Controlled Unclassified Information, dated February 2, 2021.

d. NASA Policy Statement (NPS) 1600.99, Safeguarding Sensitive But Unclassified Information, dated October 2, 2016.

e. NASA Requirement Waiver (NRW) 1400-48, Waiver for NID 1600-54 and NID 1600-55, dated, December 16, 2011.

f. NRW 1600-34, Waiver for NID 1600-54, dated December 15, 2011.

# **Chapter 1. Introduction**

## **1.1 Overview**

1.1.1 In November 2010, the United States President issued E.O. 13556 to “establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls” pursuant to and consistent with law, regulations, and Government-wide policies.

1.1.2 Prior to that time, more than 100 different markings for such information existed across the executive branch. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency specific policies are often hidden from public view has only aggravated these issues.

1.1.3 As a result, E.O. 13556 established the CUI Program to standardize and simplify the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and Government-wide policies.

1.1.4 NARA and their ISOO is the CUI Executive Agent responsible for developing policy and providing oversight for the CUI Program.

## **1.2 Responsibilities**

1.2.1 NARA established a CUI Registry on its website that serves as the authoritative reference for all CUI categories and markings.

1.2.2 Pursuant to E.O. 13556 and 32 CFR pt. 2002, the NASA Administrator shall:

- a. Demonstrate personal commitment, commit senior management, and commit necessary resources to the successful implementation of the program established under this directive and in accordance with the E.O. 13556.
- b. Designate a senior agency official (SAO) to direct and administer the information security program for managing and safeguarding CUI in accordance with the E.O. 13556.
- c. Advise NARA of any changes to the designated SAO.
- d. Approve policies to implement the CUI Program.

1.2.3 The NASA Chief Information Officer (CIO) is the designated SAO for CUI and shall:

- a. Direct and oversee the NASA’s CUI Program.
- b. Designate a CUI Program Manager (PM).
- c. Ensure NASA has CUI implementing policies and plans.
- d. Develop and execute current NASA-wide policies and procedures to manage a CUI program that complies with E.O. 13556 and 32 CFR pt. 2002.

- e. Implement and monitor compliance for a CUI education and training program.
- f. Ensure the training program for CUI includes sufficient information that allows all personnel to understand and carry out their obligations with respect to protecting, storing, transmitting, transporting, and destroying CUI.
- g. Provide updates of the NASA's CUI implementation and management efforts to NARA.
- h. Assist in and respond to audits.
- i. Manage the annual reporting requirements to NARA.
- j. Develop and implement NASA's CUI self-inspection program.
- k. Establish and maintain a process to accept and manage challenges to CUI status (including improper or absence of marking) in accordance with laws, regulations, and Government-wide policies.
- l. Establish and maintain processes and criteria for reporting and investigating misuse of CUI.
- m. Submit to NARA any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that the Agency proposes to use to designate unclassified information for safeguarding or dissemination controls.
- n. Coordinate with NARA and the NASA CUI PM, any proposed law, regulation, or Government-wide policy that would establish, eliminate, or modify a category or subcategory of CUI, or change information controls relating to CUI.
- o. Establish and maintain processes for handling CUI decontrol requests submitted by authorized holders.
- p. Establish and maintain a mechanism by which authorized holders can contact a designated representative for instructions when they receive unmarked or improperly marked information that NASA has designated as CUI.
- q. Coordinate with the Office of Procurement to ensure the Agency's contracts reflect the most current Federal Acquisition Regulation (FAR) provisions.
- r. Ensure that NASA CUI policy-related documents reflect current CUI guidance and requirements specified by NIST.
- s. Coordinate with the Office of Protective Services (OPS) to ensure that Agency-level physical security controls for CUI are consistent with current physical security policy.
- t. Issue guidance regarding requirements for protecting CUI within information technology (IT) systems and tools and when transmitting CUI via electronic means (e.g., email, Teams, etc.).
- u. Retain a record of each waiver.
- v. Include a description of all current waivers and waivers issued during the preceding year in the annual report to NARA, along with the rationale for each waiver and the alternate steps the Agency takes to ensure sufficient protection of CUI.

w. Notify authorized recipients and the public of these waivers through means such as notices or websites.

1.2.4 The NASA CUI PM (as designated by the NASA SAO) shall:

- a. Manage the day-to-day operations of NASA's CUI Program, as directed by the CUI SAO.
- b. Coordinate CUI policy development and updates.
- c. Serve as NASA's official representative to NARA on NASA's CUI Program operations and related matters, including submission of required reports.
- d. Serve as NASA's official representative on the Interagency CUI Advisory Council to advise NARA on the development and issuance of policy and implementation guidance for the CUI Program.
- e. Serve as NASA's primary subject matter expert in CUI, advising NASA offices on their CUI programs to ensure CUI operations comply with government requirements.
- f. Investigate and lead mitigation efforts for incidents involving CUI.
- g. Inform the CUI SAO of any significant CUI incidents as well as any incident trends.
- h. Issue guidance regarding requirements for:
  - (1) protecting CUI within IT systems;
  - (2) transmitting CUI from NASA information systems;
  - (3) physical protections for CUI materials; and
  - (4) destruction of CUI materials.
- i. Convey requirements for training and reporting to NASA organizations.
- j. Act as the primary point of contact for CUI reporting and audit responses.
- k. Organize and oversee CUI training efforts.
- l. Maintain an internal website that contains information about the CUI Program, with a section for each Center to list their frequently encountered CUI categories and special instructions.
- m. In collaboration with the OPS, manage NASA physical self-inspections of areas storing and processing CUI materials.
- n. Develop and maintain reporting mechanisms (e.g., 1-800 numbers, dedicated email addresses) and procedures for the timely reporting of incidents involving CUI.
- o. Develop a phased, high-level implementation plan and post it to the [NASA CUI webpage](#) and ensure that the plan includes the targeted date of full implementation of the program as directed by the NASA CUI SAO.

1.2.5 Center Directors shall:



- a. Ensure that the Center has the ability to destroy CUI when NASA no longer needs the information, and NASA Records Retention Schedules (NRRS) 1441.1 no longer require retention of the records.
- b. In accordance with NASA NPD 1440.6, NASA Records Management, July 11, 2019, ensure CUI is destroyed, including CUI in electronic form, in a manner that makes it unreadable, indecipherable, and irrecoverable in accordance with current NIST guidelines and the requirements of this directive (see section 2.14).
- c. Ensure that physical materials that contain CUI have CUI markings as per 32 CFR § 2002.20.
- d. Ensure their Centers protect all CUI in accordance with NASA policy and guidelines to ensure that all individuals and entities, with whom NASA shares or intends to share CUI, including contractors, grant recipients, and cooperative partners exercise the same care and remove any CUI controls on the information once CUI is decontrolled.

*Note: These specific Center requirements will include or identify all CUI that is routinely handled by personnel. The [NASA CUI webpage](#) will be the central repository for these guidelines and any specific Center requirements.*

1.2.6 Center Directors may issue local policies that complement overarching requirements identified in this directive.

1.2.7 The Center CIOs and HQ CIO shall:

- a. For NASA systems within their purview, assess systems that contain CUI and ensure that all Federal information technology systems that process CUI are categorized at no less than the Federal baseline of moderate confidentiality impact level per NIST FIPS Publication 199, Standards for Security Categorization of FIPS PUB 199.
- b. Ensure security requirements and controls from FIPS PUB 199, FIPS PUB 200, and NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations Rev.5 (NIST SP 800-53) for Federal Information Systems that process, store, or transmit CUI are applied.
- c. Ensure the Agency applies NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST SP 800-171), when establishing security requirement agreements to protect CUI's confidentiality on non-Federal Information Systems.
- d. Document methods for protecting CUI on public-facing websites and in cloud-based systems implemented at the Center.
- e. Ensure information systems that contain CUI have CUI markings or warnings as per 32 CFR pt. 2002.
- f. Designate CUI Liaisons and alternates to the CUI PM.

1.2.8 CUI Liaisons and alternates shall:

- a. Complete all required CUI training.

- b. Conduct oversight actions to ensure compliance within their area of responsibility and report findings to the NASA CUI PM.
- c. Serve as their office or organization's CUI subject matter expert, responding to inquiries from their organizations and consulting with the CUI PM on questions beyond their expertise.
- d. Ensure all personnel within their organization complete training as required and report the status of training to the NASA CUI PM.
- e. Conduct annual self-inspections of their CUI Program according to the guidance provided by the CUI PM.
- f. Provide input from their respective offices on all other reporting requirements to the CUI PM.
- g. Report instances of substantiated CUI misuse, violation, or infractions in accordance with the NASA Cybersecurity and Privacy Rules of Behavior. Track and report such instances to the CUI PM.
- h. Confirm their status as a CUI Liaison with the CUI PM on an annual basis (by the dates designated by the CUI PM) and provide notification within five business days if their status changes.
- i. Use the CUI Handbook to guide their duties in the Liaison role.

1.2.9 Contracting Officers, Contract Specialists, and Agreement Managers shall include CUI security clauses and standards in their assigned contracts and agreements that deal with CUI. Consider incorporating elements of model statements of work, task statements, and deliverables shared on the NASA CUI website.

1.2.10 Contracting Officer Representatives (CORs) shall:

- a. Identify the types of CUI in the contract or potentially shared as part of the activity covered by their assigned contracts.
- b. Include the CUI requirements of this policy in all pertinent contracts and agreements. Consider incorporating elements of model statements of work, task statements, and deliverables shared on the NASA CUI website.
- c. Ensure contractors receive training on CUI within 30 days of contract award or prior to accessing CUI, whichever occurs first.
- d. Report any violations of CUI requirements by contractors to the CO and CUI PM.

1.2.11 Supervisors and Managers shall:

- a. Review and ensure that all CUI products for their organization are properly marked in accordance with this policy.
- b. Annually verify that:
  - (1) All physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevention of unauthorized access) in compliance with this directive.

(2) All electronic safeguarding measures are adequate for the protection of CUI (i.e., prevention of unauthorized access).

c. Ensure that all personnel under their purview receive required CUI training.

1.2.12 Information Owners (IO) and Information System Owners (ISO) shall:

a. Ensure all CUI collected under their purview is properly designated using a category or subcategory approved by the CUI Executive Agent and published in the [CUI Registry](#).

b. Ensure the secure transmission and storage of CUI in accordance with Federal law, regulations, Government-wide and NASA policies and these procedural requirements. See Sections 2.13–2.15, and 2.20.

1.2.13 Executive Branch personnel including NASA Civil Servants that receive NASA CUI shall:

a. Complete all initial, recurring, and CUI Specified assigned CUI training within the required timeframes.

b. Manage, mark, and protect CUI in accordance with this policy, the E.O. 13556, the CFR 32 pt. 2002.02, the NASA CUI Handbook, and NARA CUI Marking Handbook.

c. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), SBU, or that contains other legacy security markings is re-marked as CUI before the information leaves NASA.

*Note: Only markings that are contained in the NARA CUI Registry may be used to annotate CUI.*

d. Report CUI violations to NASA Security Operations Center (SOC).

*Note: CUI violations may also be reported to line management.*

1.2.14 Non-Executive Branch entities and individuals, including but not limited to contractors, contractor employees, detailees, guest researchers, interns, shall, to the extent specified in agreements entered into pursuant to Chapter 2.10:

a. Complete all initial, recurring, and CUI Specified assigned CUI training within the required timeframes.

b. Manage, mark, and protect CUI in accordance with this policy, E.O. 13556, 32 CFR pt. 2002, and the NASA CUI Handbook.

c. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), SBU, or that contains other legacy security markings is re-marked as CUI before the information leaves NASA.

*Note: Only markings that are contained in the NARA CUI Registry may be used to annotate CUI.*

d. Report CUI violations to NASA SOC.

1.2.15 The NASA Senior Agency Official for Privacy (SAOP) shall advise the CUI SAO and CUI PM on all policies, procedures, laws, regulations, and guidance relating to the Privacy Act of 1974, 5 U.S.C. § 552a, and Personally Identifiable Information (PII) and coordinate with the CUI SAO and CUI PM to ensure consistency between privacy policy and CUI requirements.

*Note: The NASA SAOP may delegate this function to the Agency Privacy Officer.*

1.2.16 The NASA Chief FOIA Officer shall:

- a. Advise the CUI SAO and CUI PM on all policies, procedures, laws, regulations, and guidance pertaining to the disclosure of information for requests for records made under Freedom of Information Act (FOIA), 5 U.S.C § 552 and 5 U.S.C. § 552a.
- b. Coordinate with the CUI SAO and CUI PM to resolve any conflicts between 5 U.S.C § 552 and CUI requirements.

*Note: The NASA Chief FOIA Officer may delegate this function to Center FOIA Officers.*

1.2.17 The NASA Chief Data Officer (CDO) shall consult, if needed, with the SAO for CUI and the CUI PM to ensure required safeguards are applied to protect CUI in NASA digital assets.

## Chapter 2. CUI Management

### 2.1 General

2.1.1 The [CUI Registry](#) is NARA's online repository for all information, guidance, policy, and requirements on handling CUI. The CUI Registry identifies all Federal-approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. There are two subsets of CUI: CUI Basic and CUI Specified. All CUI falls into one of these two subsets.

2.1.2 "CUI Basic" is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.

2.1.3 "CUI Specified" is the subset of CUI for which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that exceed those for CUI Basic. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic.

2.1.4 The distinction between "CUI Basic" and "CUI Specified" is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific handling guidance.

#### 2.1.5 CUI categories

a. CUI categories are those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which NARA has approved and listed in the CUI Registry.

b. Personnel may use only CUI categories approved by NARA and published in the [CUI Registry](#) to designate information as CUI.

2.1.6 Personnel who encounter information described in law, regulations, or Government-wide policy that is not described in the CUI Registry will contact their CUI Liaison so that a request for a new information category can be entered into the Registry by the CUI PM.

2.1.7 The CUI Liaison shall recommend and coordinate the request through CUI PM. The request should include:

- a. A description of the information to be marked as CUI,
- b. The law(s), regulation(s), or Government-wide policy(ies) that apply,
- c. The name of the category applying to the information, and
- d. A suggested name, along with a suggested acronym for the category.

2.1.8 The CUI PM, in coordination with the Office of the General Counsel (OGC), will submit the recommendation to NARA in accordance with the procedures contained in [CUI Notice 2018-06: Establishing, Eliminating or Modifying Categories of Controlled Unclassified Information \(CUI\)](#).

2.1.9 Publication of CUI or its posting on public websites or social media is prohibited unless the CUI has been properly decontrolled in accordance with NPD 2521.1, Communications and Material Review and 2.12 below.

## **2.2 Marking of CUI**

2.2.1 CUI markings listed in the CUI Registry are the only markings authorized to designate controlled unclassified information requiring safeguarding or dissemination controls.

2.2.2 Personnel and authorized holders will uniformly and conspicuously apply CUI markings to all CUI in accordance with the CUI Registry, unless NASA has issued a limited CUI marking waiver.

2.2.3 NASA waivers will be documented on the [NASA CUI webpage](#).

2.2.4 Information will not be designated as CUI:

- a. To conceal violations of law, inefficiency, or administrative error;
- b. To prevent embarrassment to the United States Government, any United States official, organization, or agency;
- c. To improperly or unlawfully interfere with competition;
- d. To improperly or unlawfully interfere with any right of employees provided for by statute or government-wide regulation;
- e. To prevent or delay the release of information that does not require such protection; or
- f. If the CUI is required by law, regulation, or government-wide policy to be made available to the public or if it has been released to the public under proper authority.

2.2.5 The lack of CUI markings on information that qualifies as CUI does not exempt the authorized holder from abiding by CUI markings and handling requirements.

2.2.6 When it is impractical for an organization to individually mark CUI due to quantity or nature of the information, or when the CUI SAO has issued a limited CUI marking waiver, the authorized holders will make recipients aware of the information's CUI designation using an alternate marking method that is readily apparent. This could be done through methods such as user access agreements, computer system digital splash screen, coversheets, or signs in storage areas or in containers.

2.2.7 32 CFR pt. 2002, the [CUI Registry](#), and NARA's supplemental guidance, their NARA CUI Marking Handbook, (<https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>) will be followed to mark the CUI on paper and electronic documents. The NARA handbook provides examples of correctly marked CUI.

2.2.8 CUI markings. Authorized holders will mark all CUI with a CUI banner marking. The content of the CUI banner marking will be inclusive of all CUI within the document and will be the same on each page. Banner markings will appear at the top of each page of any document that contains CUI, including email transmissions, if authorized.

2.2.9 If NASA personnel believe that CUI is marked incorrectly, they should provide notice of the error to their respective CUI Liaison within their organization.

## **2.3 Portion Marking (Optional)**

2.3.1 Portion markings are a means to provide information about the sensitivity of a specific section of text, paragraph, bullet, picture, or chart. They consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title.

2.3.2 Portion marking is not required, but it is permitted to facilitate information sharing and proper handling, and to assist reviewers in identifying the CUI within a large document that may be primarily Uncontrolled Unclassified Information.

2.3.3 If portion markings are used in any portion of a document, then portion markings will be used throughout the entire document. All portions or sections will be portion marked, even those that do not contain CUI. Sections that do not contain CUI should be marked as Uncontrolled Unclassified Information, designated with a [U].

2.3.4 For examples on portion marking of documents, see the NASA CUI Handbook and the [NARA CUI Marking Handbook](#).

## **2.4 Comingling CUI Markings with Classified National Security Information (CNSI) Markings**

2.4.1 Authorized holders, who include CUI in documents that contain CNSI shall:

- a. Portion mark all CUI to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information.
- b. Include the CUI control marking, CUI Specified category markings, and any Limited Dissemination Control Markings (LDCMs) in the overall banner marking.
- c. The decontrolling provisions of the CUI Program apply only to portions marked as CUI.

2.4.2 Whether originally generated, derived, or reproduced by someone with an active clearance and a need to know, documents containing CUI and CNSI will be classified at the highest level of the information contained therein. All precautions necessary to properly mark, disseminate, transport, transmit, reproduce, and store those documents are specified in NPR 1600.2, NASA CNSI.

2.4.3 The CUI Registry and the [NARA CUI Marking Handbook](#) contain guidance on marking CUI when comingled with CNSI.

## **2.5 Legacy Materials**

2.5.1 Documents created prior to October 1, 2021, and prior to NASA CUI implementation, are considered legacy information and are not required to be reviewed and re-marked unless they contain information that qualifies as CUI and the information is reused or expected to be transmitted outside of NASA. Transmission of CUI outside NASA is the delivery of any document to a third party that is not: a NASA civil servant or contractor supporting NASA, a

prime contractor to NASA and its subcontractors for NASA contracts, or an entity with a relationship to NASA described in P.2c.(1) – (4) of this directive. If the legacy material is not re-marked, an alternate permitted marking method will be used (i.e., CUI coversheet).

2.5.2 Legacy materials will be handled and protected as CUI unless decontrolled.

2.5.3 The following protocols guide the handling of legacy materials:

a. For information recipients receiving marked legacy materials:

(1) If the receiving organization plans to reuse or transmit the legacy marked information to another agency, then it shall evaluate the information and remark it as CUI.

(2) The receiving organization shall also adhere to any Agency marking waivers as they apply to internal dissemination. See 2.22 regarding waivers.

(3) The receiving organization shall apply any LDCMs. See also 2.9.2.

(4) Receiving organizations shall not reuse legacy markings, such as FOUO or SBU, on new documents that are derived from marked legacy information.

(5) Authorized holders should contact the originator of the material if they have any questions.

b. For authorized holders transmitting marked legacy information within NASA:

(1) The authorized holder shall provide a point of contact in case the recipient has questions about safeguarding the material.

(2) Any special handling requirements associated with the information, such as limited dissemination controls, should be conveyed through transmittal or in a manner apparent to the recipient of the information.

## **2.6 Working Papers**

2.6.1 Working papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

2.6.2 Working papers containing CUI will be marked the same way as the finished product containing CUI would be marked and as required for any CUI contained within. Working papers will be protected as any other CUI. This protection applies whether or not the working papers will be destroyed. When no longer needed, working papers need to be destroyed in accordance with section 2.17 below.

## **2.7 Using Supplemental Administrative Markings with CUI**

Supplemental administrative markings (e.g., “Pre-decisional,” “Deliberative,” “Draft”) may be used at NASA with CUI with specific restrictions. The NASA CUI Handbook and [NARA CUI Marking Handbook](#) both provide examples of permitted supplemental administrative markings.

2.7.1 Deliberative: Makes recommendations or expresses opinions on legal or policy matters.

2.7.2 Pre-decisional: Prepared in order to assist an agency decisionmaker in arriving at their decision.



2.7.3 Draft: Universally accepted marking to indicate a product is not finalized.

## 2.8 Unmarked CUI

Unmarked CUI is information that qualifies as CUI but is not legacy information (i.e., previously marked). It will be marked and treated as described in this policy upon recognition that it qualifies as CUI.

*Note: legacy information, such as that categorized as SBU, need only be remarked as CUI if it is re-shared. See section 2.5.*

## 2.9 Sharing of CUI (Accessing and Disseminating)

2.9.1 NASA disseminates and permits access to CUI, provided that such access or dissemination:

- a. Complies with laws, regulations, or Government-wide policies that established the CUI category;
- b. Furthers a lawful Government purpose;
- c. Is not restricted by an authorized limited dissemination control established by the CUI Executive Agency; and
- d. Is not otherwise prohibited by law.

2.9.2 Only the [limited dissemination controls](#) published in the CUI Registry may be used to restrict the dissemination of CUI to certain individuals, agencies, or organizations. These dissemination controls may only be used to further a lawful government purpose, or if laws, regulations, or Government-wide policies require or permit their use. LDCM examples include:

- a. no foreign dissemination, NOFORN;
- b. federal employees only, FED ONLY;
- c. federal employees and contractors only, FED CON;
- d. no dissemination to contractors, NO CON;
- e. dissemination list controlled, DL ONLY;
- f. authorized for release to certain nationals only, REL TO [USA, LIST] - [see list; and](#)
- g. display only, DISPLAY ONLY.

2.9.3 The following additional LDCMs may only be used with the PRIVILEGE categorization:

- a. attorney client, Attorney-Client;
- b. attorney work product, Attorney-WP; and
- c. deliberative process, Deliberative.

2.9.4 Organizations are required to use the dissemination list-controlled designation when they need to limit access to individuals, offices, or organizations.

2.9.5 NASA may not impose controls that unlawfully or improperly restrict access to CUI.

2.9.6 CUI may be shared with a non-executive branch or a foreign entity under the following conditions in addition to the requirements listed in Section 2.9.1:

a. When intended recipients are authorized to receive the CUI and understand safeguarding and handling requirements.

b. Whenever feasible, Centers and Mission Directorates shall enter into some type of formal information-sharing agreement with the recipient of the CUI or incorporate language into domestic and international agreements. The agreement will include a requirement for the recipient to, at a minimum, comply with E.O. 13556; 32 CFR pt. 2002; and the CUI Registry.

2.9.7 Sharing information with a foreign entity. When entering into information-sharing agreements or arrangements with a foreign entity, such as Foreign Guest Researchers, personnel should encourage that entity to protect CUI in accordance with E.O. 13556; 32 CFR pt. 2002; and the CUI Registry. Personnel are cautioned to use judgment as to what and how much to communicate, keeping in mind the objective of safeguarding CUI. If such agreements or arrangements include safeguarding or dissemination controls on controlled unclassified information, only the CUI markings and controls may be allowed. No other markings or protective measures may be used.

2.9.8 Information-sharing agreements that were made prior to establishment of the CUI Program should be modified whenever feasible so they do not conflict with CUI Program requirements.

2.9.9 Information-sharing agreements with non-executive branch entities will include provisions on the CUI handling in accordance with the CUI Program. The non-executive branch entities and authorized CUI holders should be familiar with the distinctions between CUI Basic and CUI Specified information and their respective markings and handling procedures. They will be responsible for handling CUI in compliance with the requirements of this rule and the CUI Registry through a forthcoming FAR clause. The rule's applications to non-executive branch entities imposes new potential liability. The misuse of CUI by non-executive branch entities is subject to penalties established in laws, regulations, or Government-wide policies; and any noncompliance with handling requirements will be reported to the CUI PM. When NASA is not the designating agency, personnel will report any non-compliance to the designating agency.

2.9.10 CUI Basic may be disseminated to persons and entities meeting the access requirements of this section. NASA may further restrict the dissemination of CUI Basic by using an authorized LDCM published on the CUI Registry.

2.9.11 Authorized recipients of CUI Basic may further disseminate the information to individuals or entities meeting and complying with the requirements of this CUI Program. CUI Specified may only be disseminated to persons and entities as authorized in the underlying legislation or authority contained in the CUI Registry. Further dissemination of CUI Specified may be made to such authorized persons if not restricted by the underlying authority (governing law, regulation, or Government-wide policy). As in the case of CUI Basic, CUI Specified may further restrict the dissemination of CUI Specified using authorized LDCMs.

## **2.10 CUI Disclosure Statutes**

2.10.1 The fact that information is designated as CUI does not prohibit its disclosure to individuals authorized to receive such information and who need the information in order to further a lawful government purpose.

2.10.2 CUI and 5 U.S.C § 552. 5 U.S.C § 552 may not be cited as a CUI safeguarding or disseminating control authority for CUI. When determining whether to disclose information in response to a FOIA request, the decision will be based upon the content of the information and applicability of any statutory exemptions, regardless of whether the information is designated or marked as CUI. There may be circumstances in which CUI may be disclosed to an individual or entity, including a request and response pursuant to 5 U.S.C. § 552 or 5 U.S.C. § 552a, but such disclosure does not always constitute public release. Although disclosed via a FOIA response, the CUI may still need to be controlled while NASA continues to hold the information, despite the disclosure, unless it is otherwise decontrolled (or the NASA FOIA Officer indicates that disclosure results in public release and the CUI does not otherwise have another legal requirement for its continued control).

2.10.3 32 CFR pt. 2002 and Whistleblower Protection Act, 5 U.S.C. § 2302. The CUI Program does not change or affect existing legal protections for whistleblowers. The fact that information is designated or marked as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, executive order, or directive.

2.10.4 CUI and the 5 U.S.C. § 552a. The fact that records are subject to 5 U.S.C. § 552a does not mean that the records should be marked as CUI. Information contained in 5 U.S.C. § 552a systems of records may also be subject to controls under other CUI categories and may need to be marked as CUI for that reason. Additionally, when determining whether certain information will be protected under 5 U.S.C. § 552a, or whether 5 U.S.C. § 552a allows an individual the right to access their information maintained in a system of records, the decision to release will be based upon the content of the information as well as 5 U.S.C. § 552a criteria, regardless of whether the information is designated or marked as CUI. Decontrol of CUI for the limited purpose of making an individual's information available to them under 5 U.S.C. § 552a does not result in decontrol for any other purpose.

## **2.11 Challenges to Designation of Information as CUI**

Authorized holders of CUI who, in good faith, believe that a designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the designating agency (POC identified on the document and/or the NASA CUI PM). Challenges may be made anonymously, and challengers cannot be subject to retribution for bringing such challenges. Challenges to other agencies should be coordinated with the NASA CUI PM.

## **2.12 Decontrol of CUI**

2.12.1 When control is no longer needed, NASA should decontrol any CUI that it designates. The information should be removed from the protection of the CUI program when it no longer

requires safeguarding or dissemination controls, unless doing so conflicts with the underlying law, regulation, or Government-wide policy. In addition, central authorities, like the Archivist of the United States, may direct decontrol of CUI across agencies. The NASA CUI Handbook covers the processes by which CUI is decontrolled.

2.12.2 Centers or Mission Directorates, and HQ offices may designate in their CUI policies which personnel it authorizes to decontrol CUI, consistent with law, regulation, and Government-wide policy.

2.12.3 NASA personnel shall not decontrol CUI to conceal, or to otherwise circumvent accountability for, an unauthorized disclosure.

2.12.4 When laws, regulations, or Government-wide policies require specific decontrol procedures, NASA personnel shall follow such requirements.

## **2.13 Safeguarding and Storage**

2.13.1 The objective of safeguarding is to prevent the unauthorized disclosure of or access to CUI. These guidelines set forth the minimum standards for safeguarding; however, organizations may adopt specific organization requirements for safeguarding CUI within their organization per FIPS 140-2.

2.13.2 Unless different protection is specified in the CUI Registry, physical documents containing CUI will be stored in a locked office, locked drawer, or locked file cabinet if unattended. Electronic files will be protected using NASA approved methods such as encryption and access restriction. See CUI Handbook for more detailed information.

2.13.3 NASA personnel working with CUI Specified shall comply with the safeguarding standards outlined in the underlying law, regulation, or Government-wide policy in addition to those described in this policy.

2.13.4 Safeguarding During Working Hours. NASA personnel working with CUI shall be careful not to expose CUI to unauthorized users or others who do not have a lawful Government purpose to have, transport, store, use, or process CUI. Cover sheets may be placed on top of documents to conceal the contents from casual viewing. Personnel may use cover sheets to protect CUI documents while in use, but will secure CUI documents in a locked location, such as a desk drawer, file cabinet, or office, when not in use. Other precautions include the following:

a. NASA personnel should reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed.

b. CUI should be kept in a controlled environment which is defined as any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) for protecting CUI from unauthorized access or disclosure.

c. If it is necessary to remove CUI from a controlled environment of the work location (e.g., telework, official travel), NASA personnel shall keep CUI under their direct control at all times or protect it with at least one physical barrier (i.e., a cover sheet) and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.

2.13.5 Safeguarding While Traveling. All reasonable measures will be taken (e.g., secure transmission, approved electronic USB, or other authorized methods to mitigate risk and limit the necessity to hand carry CUI while in official travel status). CUI will not be viewed while on public transportation where it can be exposed to others. In hotel rooms, CUI will be stored in a locked briefcase or room safe when not in use. CUI may be stored in a locked automobile only if it is in an envelope, briefcase, or otherwise covered from view. The trunk is the most secure location for storing CUI in an automobile.

2.13.6 Safeguarding During Foreign Travel. Specific instructions for handling and safeguarding of sensitive information, including CUI, are contained in NPR 9710.1, General Travel Requirements, and NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

2.13.7 Unless allowed by law, regulation or Government-wide policy, NASA may not require their contractors or other partners with whom they share CUI to apply more restrictive safeguarding standards than those described in this policy or 32 CFR pt. 2002

## **2.14 Reproduction of CUI**

2.14.1 CUI may be reproduced (e.g., copied, scanned, printed, electronically duplicated) in furtherance of a lawful government purpose (in a manner consistent with the CUI marking).

2.14.2 When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, management officials will ensure that the equipment does not retain data, or else they will sanitize the equipment in accordance with NIST SP 800-53. Prior to purchasing equipment, management should ensure that the equipment does not store or transmit data to non-federal entities and that at the end of the equipment's lifecycle any hard drives or memory are sanitized in accordance with NIST SP 800-88, Revision 1, Guidelines for Media Sanitization.

## **2.15 Shipping or Mailing CUI**

2.15.1 CUI may be sent through the United States Postal Service or any commercial delivery service that offers in-transit automated tracking and accountability tools.

2.15.2 CUI may also be sent through interoffice or interagency mail systems.

2.15.3 Address packages and parcels that contain CUI for delivery only to an individual recipient, not to an office or organization. As a best practice, mark the package "Open by Addressee Only." Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI. Any transmittal document accompanying the package should be contained within the package wrappings, so the CUI markings are not visible.

## **2.16 Transmittal Document Marking Requirements**

2.16.1 When a transmittal document accompanies CUI, the transmittal document shall include, on its face, a distinctive notice that CUI is attached or enclosed. This serves to notify the recipient about the sensitivity of the document beneath the cover letter.

2.16.2 The notice shall include the CUI marking (“CUI”) along with the following or similar instructions:

- a. “When enclosure is removed, this document is Uncontrolled Unclassified Information (UUI)”
- b. “When enclosure is removed, this document is (indicate control level);” or, “upon removal, this document does not contain CUI.”

## **2.17 Destruction of CUI**

CUI may be destroyed:

2.17.1 When the information is no longer needed by the Agency, and

2.17.2 When the NRRS or other records disposition schedules, published or approved by NARA no longer require retention of the records qualifying as CUI. The Controlled Unclassified Information Handbook contains detailed provisions on the methods of destruction for information designated as CUI.

## **2.18 Misuse of CUI and Incident Reporting**

2.18.1 Any Authorized Holder shall report suspected or confirmed misuse of CUI to the SOC.

2.18.2 Reportable CUI incidents include, but are not limited to:

- a. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of CUI.
- b. Any knowing, willful, or negligent action to designate information as CUI contrary to the requirements of E.O. 13556 and 32 CFR pt. 2002.
- c. Any incident involving computer, telecommunications equipment, or media that may result in disclosure of CUI to unauthorized individuals, or that results in unauthorized modification or destruction of CUI system data, loss of CUI computer system processing capability, or loss or theft of CUI computer system media.
- d. Any incident involving the processing of CUI on computer equipment that has not been specifically approved and accredited for CUI processing by an authorized official, as described in 2.21.
- e. Any incident involving the shipment of CUI by an unapproved method, or any evidence of tampering with a shipment, delivery, or mailing of packages containing CUI.
- f. Any incident in which CUI is not stored by an approved means as identified in 2.13. (i.e., material stored in the open).
- g. Any incident in which CUI is inadvertently revealed to or released to a person not authorized access.
- h. Any incident in which CUI is destroyed by unauthorized means as identified in 2.17. (i.e., not shredding to correct size).

- i. Any incident in which CUI is reproduced without authorization or contrary to specific restrictions imposed by the originator.
- j. Any incident in which CUI is shared contrary to an applied dissemination control marking.
- k. Any other incident in which CUI is not safeguarded or handled in accordance with prescribed procedures.

2.18.3 The CUI PM, in conjunction with the CUI SAO and Office of the Chief Human Capital Officer (OCHCO), will advise the supervisor of an employee who has misused CUI.

- a. Depending on the circumstances of the employee's misuse of CUI, the supervisor shall take disciplinary action as suitable, and/or assess whether other corrective action may be warranted (e.g., emphasis in training).
- b. The CUI PM shall report misuse of CUI that has been designated by another executive agency to that agency.

2.18.4 Incidents involving PII will be reported in accordance with [ITS-HBK-1382.05, Privacy Incident Response and Management: Breach Response Team Checklist](#).

## **2.19 Sanctions for Misuse of CUI**

2.19.1 Misuse of CUI can result in sanctions, up to and including a Federal employee's removal from Federal service. In the event a contractor employee misuses CUI, the matter will be referred to the cognizant Contracting Officer who will notify the contractor and then determine whether other action is necessary.

2.19.2 An employee found to be responsible for the commission of a CUI incident, may be subject to administrative, disciplinary, or criminal sanctions. The type of sanctions imposed is based on several considerations, including the following:

- a. Severity of the incident;
- b. Intent of the person committing the incident;
- c. Extent of training the person(s) has received;
- d. Prior acknowledgement of enterprise or system rules of behavior;
- e. Frequency of which the individual has been found responsible in the commission of other such incidents, to include Security Violations or Infractions involving classified information; and
- f. Consistency of the sanction with those imposed on other employees for the commission of the same or similar CUI incident.

2.19.3 Sanctions include, but are not limited to, verbal or written counseling, reprimand, suspension from duty and pay, removal, removal of access to CUI, or criminal penalties. The underlying law, regulation, or Government-wide policy is consulted for guidance.

## **2.20 CUI Within Information Systems**

2.20.1 IT systems containing CUI will minimally meet the Federal baseline of moderate for confidentiality per FIPS PUB 199.

2.20.2 In accordance with FIPS PUB 199, CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines security impact levels for federal information and Federal information systems. The security requirements and controls identified in FIPS PUB 200 and NIST SP 800-53, Revision 5 will be applied to CUI in accordance with any risk-based tailoring decisions made by an approving official. NASA, including contractors operating an information system on behalf of NASA, may increase CUI Basic's confidentiality impact level above moderate only within NASA, or by means of agreements between NASA and other agencies or non-executive branch entities. However, this cannot be used to limit access to CUI beyond statutory requirements. NASA may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating CUI Basic outside NASA.

2.20.3 Information systems that process, store, or transmit CUI are of two different types:

- a. A Federal information system is an information system used or operated by a Federal agency or by a contractor of an agency or other organization on behalf of an agency. Information systems that any entity operates on behalf of NASA are subject to the requirements of the CUI Program as though they are NASA systems, and NASA may require these systems to meet the same requirements as NASA's own internal systems.
- b. A non-Federal information system is any information system that does not meet the criteria for a Federal information system. Personnel may not treat non-Federal information systems as though they are NASA systems, so non-executive branch entities cannot be required to protect these systems in the same manner that NASA might protect its own information systems. Instead, personnel will inform entities employing non-Federal information systems that they will follow the requirements of NIST SP 800-171 to protect CUI, unless specific requirements are specified by law, regulation, or Government-wide policy for protecting the information's confidentiality.

2.20.4 NIST SP 800-171 contains standards that NASA Contractors and other non-executive branch entities that receive CUI incidental to providing a service or product to the government will meet if they have NASA CUI on their computer systems.

2.20.5 National Security Systems authorized to store, process, and/or transmit classified information under NPR 1600.2 are considered compliant with the necessary protections of CUI.

## **2.21 CUI Self-Inspection Program**

NASA will implement a Self-Inspection Program as follows:

2.21.1 The CUI PM, under the authority of the CUI SAO, shall provide technical guidance, training, and materials for NASA to conduct reviews and assessments of their CUI Programs at least annually, and to report the results to the CUI PM as NARA requires.



2.21.2 Following training of the designated CUI Liaisons, Centers and Mission Directorates will conduct annual self-inspections of their CUI Programs and report the results on a schedule determined by the CUI PM.

2.21.3 Centers and Mission Directorates will include in the self-inspection any Contractors that are under their purview by on-site inspections or by examining any self-inspections conducted by the Contractors.

2.21.4 Following guidance and inspection materials received from the CUI PM, self-inspection methods, reviews, and assessments serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation.

2.21.5 The CUI PM shall provide to the Centers and Mission Directorates formats for documenting self-inspections and recording findings and provide advice for resolving deficiencies and taking corrective actions.

2.21.6 Results from NASA-wide self-inspections will inform updates to the CUI training provided to personnel.

## **2.22 Waivers to CUI Requirements**

2.22.1 In compliance with NPR 8000.4, Agency Risk Management Procedural Requirements on the risk-informed decision-making process, the CUI SAO may approve waivers of the CUI marking requirements while the CUI remains within NASA, or if it is determined that because of a substantial amount of stored information with legacy markings, removing legacy markings or re-marking it as CUI would be excessively burdensome. As indicated in 2.5.3, the NASA CUI SAO has granted a legacy material limited re-marking waiver.

2.22.2 However, when an authorized holder re-uses any legacy information or information derived from legacy documents that qualifies as CUI, the authorized holder shall remove or redact legacy markings and designate or re-mark the information as CUI, even if the information is under NASA's legacy material re-marking waiver prior to re-use.

2.22.3 In exigent circumstances, such as natural disaster, pandemic, or other emergency, the CUI SAO may waive certain requirements of the CUI Program for any CUI in NASA's possession or control, unless specifically prohibited by laws, regulations, or Government-wide policies.

2.22.4 Exigent circumstances waivers may apply when NASA shares the information with other agencies or non-Federal entities, if the need to share is immediate. In such cases, recipients will be made aware of the CUI status of any disseminated information.

2.22.5 Non-exigent circumstance waivers approved by the NASA CUI SAO are valid only while the information remains within NASA. CUI markings will be uniformly and conspicuously applied to all CUI prior to disseminating it outside NASA unless otherwise specifically permitted by NARA.

2.22.6 Refer to Section 2.5 for NASA legacy material waiver information.

## **2.23 CUI Education and Training**

2.23.1 After December 30, 2021, every NASA authorized holder shall complete initial CUI awareness training within 30 days of employment and prior to access.

*Note: There will be an initial CUI training course with refresher training to be included in annual security training.*

2.23.2 Refresher training is required annually after the initial training, or whenever CUI policy and process change significantly.

2.23.3 Authorized holders shall take additional training for CUI Specified categories they have access to or for which they are required to safeguard.

2.23.4 Authorized holders who have access to CUI shall receive training on designating CUI, relevant CUI categories, the CUI Registry, associated markings, and safeguarding, disseminating, and decontrolling policies and procedures.

## Appendix A Definitions

**Agreements and arrangements** are any vehicle that sets up specific CUI handling requirements for Contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information sharing agreements or arrangements. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into agreements or arrangements when feasible.

**Authorized holder** is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR pt. 2002, and approved NASA CUI policy and guidelines. Generally, this is all trained NASA employees and contractors.

**Controlled** is an alternative banner marking used by some departments and agencies to indicate that the presence of CUI information in the document. “Controlled” is equivalent to the banner marking “CUI.”

*Note: NASA will not use this banner marking.*

**Controlled Environment** is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

**Controls** are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may specify controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case the agency applies controls from the E.O., 32 CFR pt. 2002, and the CUI Registry).

**CUI** is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or Government-wide policy requires or permits an agency to handle with safeguarding or dissemination controls.

**CUI Basic** is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle *CUI Basic* according to the uniform set of controls set forth in 32 CFR pt. 2002 and the CUI Registry. *CUI Basic* differs from *CUI Specified* (see definition for *CUI Specified* in this section), and CUI Basic controls apply whenever CUI Specified controls do not cover the involved CUI.

**CUI Executive Agent** is The National Archives and Records Administration (NARA) who has delegated those responsibilities to the Director of their Information Security Oversight Office (ISOO).

**CUI Registry** is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than the CUI regulations in 32 CFR pt. 2002. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

**CUI Specified** is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that requires or permits agencies to use procedures and protections that exceed those for *CUI Basic*. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. *CUI Specified* controls may be more stringent than, or may simply differ from, those required by *CUI Basic*; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for *CUI Basic* information. *CUI Basic* controls apply to those aspects of *CUI Specified* where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

**Decontrolling** occurs when an authorized holder, consistent with the CUI regulations and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action. See 32 CFR § 2002.18.

**Designating** CUI occurs when an authorized holder, consistent with 32 CFR pt. 2002 and the CUI Registry, determines that a specific item of information falls into a CUI category.

**Designator** is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR pt. 2002, and approved NASA CUI policy and guidelines. Generally, this is all trained NASA employees and contractors.

**Dissemination** occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external to an agency.

**Handling** is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

**Lawful Government Purpose** is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

**Legacy material** is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

**Limited Dissemination Control** is any CUI Executive Agent-approved control that agencies may use to limit or specify CUI dissemination.

**Misuse** of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in these guidelines, the CUI regulations, E.O. 13556, 32 CFR pt. 2002, the CUI Registry, agency CUI policy, or the laws, regulations, and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

**Uncontrolled Unclassified Information or UUI** is information that neither the E.O. 13556 nor the authorities governing classified information cover as protected. Although this information is

not controlled or classified, agencies will still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.

**Underlying Authority** is any law, regulation, or Government-wide policy that prescribes a type of CUI Specified.

## **Appendix B      Acronyms**

<b>CDO</b>	Chief Data Officer
<b>CFR</b>	Code of Federal Regulations
<b>CIO</b>	Chief Information Officer
<b>CISO</b>	Chief Information Security Officer
<b>CNSI</b>	Classified National Security Information
<b>COR</b>	Contracting Officer Representative
<b>CUI</b>	Controlled Unclassified Information
<b>DL ONLY</b>	Distribution List Only
<b>E.O.</b>	Executive Order
<b>FAR</b>	Federal Acquisition Regulation
<b>FED ONLY</b>	Federal Agencies Only
<b>FIPS</b>	Federal Information Processing Standard
<b>FOIA</b>	Freedom of Information Act
<b>FOUO</b>	For Official Use Only
<b>FFRDC</b>	Federally Funded Research and Development Center
<b>GOCO</b>	Government Owned Contractor Operated
<b>GSA</b>	General Services Administration
<b>HQ</b>	Headquarters
<b>IG</b>	Inspector General
<b>IO</b>	Information Owner
<b>ISO</b>	Information System Owner
<b>ISOO</b>	Information Security Oversight Office
<b>IT</b>	Information Technology
<b>LDCM</b>	Limited Dissemination Control Marking
<b>MOA</b>	Memorandum of Agreement
<b>MOU</b>	Memorandum of Understanding
<b>NARA</b>	National Archives and Records Administration
<b>NASA</b>	National Aeronautics and Space Administration
<b>NID</b>	NASA Interim Directive

<b>NIST</b>	National Institute for Standards and Technology
<b>NOCON</b>	No Contractors
<b>NOFORN</b>	No Foreign Nationals
<b>NPD</b>	NASA Policy Directive
<b>NPR</b>	NASA Procedural Requirement
<b>NPS</b>	NASA Policy Statement
<b>NRW</b>	NASA Requirement Waiver
<b>OCHCO</b>	Office of the Chief Human Capital Officer
<b>ODNI</b>	Office of the Director of National Intelligence
<b>OGC</b>	Office of General Counsel
<b>OPS</b>	Office of Protective Services
<b>PII</b>	Personally Identifiable Information
<b>PM</b>	Program Manager
<b>POC</b>	Point of Contact
<b>PRA</b>	Paperwork Reduction Act
<b>SAO</b>	Senior Agency Official
<b>SAOP</b>	Senior Agency Official for Privacy
<b>SBU</b>	Sensitive But Unclassified
<b>SF</b>	Standard Form
<b>SOC</b>	Security Operations Center
<b>SP-[number]</b>	[NIST] Special Publication
<b>SP-[category]</b>	Specified [CUI category]
<b>SSP</b>	System Security Plan
<b>TR</b>	Transfer Request
<b>USB</b>	Universal Serial Bus
<b>UUI</b>	Uncontrolled Unclassified Information
<b>WP</b>	

## Appendix C      Web Resources

C.1 CUI Registry Website: <<https://www.archives.gov/cui/registry/category-list>>

C.2 NASA CUI Website: <<https://nasa.sharepoint.com/sites/privacy/>>

C.3 CUI Notice 2018-06: Establishing, Eliminating or Modifying Categories of Controlled Unclassified Information (CUI): <<https://www.archives.gov/files/cui/documents/20181116-cui-notice-2018-06-establishing-eliminating-modifying-cui-categories.pdf>>

C.4 NARA CUI Marking Handbook: <<https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>>

C.5 CUI Registry: Limited Dissemination Controls:  
<<https://www.archives.gov/cui/registry/limited-dissemination>>

C.6 Trigraph Country Codes for Use with REL TO or DISPLAY ONLY Limited Dissemination Controls CUI Ma for CUI: <<https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/20161214-country-trigraph-codes.pdf>>

C.7 Standard Form 901 (11-2018) cover sheet: <<https://www.gsa.gov/cdnstatic/SF901-18a.pdf>>

C.8 National Security Agency-approved devices for device sanitization:  
<<https://www.nsa.gov/Resources/Media-Destruction-Guidance/>>