NASA Interim Directive

NID 2810.135
Effective Date: February 2, 2021
Expiration Date: February 2, 2022

Subject: Controlled Unclassified Information

Responsible Office: Office of the Chief Information Officer

DISTRIBUTION:

NODIS

Table of Contents

Preface

P.1 Purpose

a. This NASA Interim Directive (NID) establishes Agency-wide requirements for the protection of Controlled Unclassified Information (CUI).

b. This NID prescribes 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 NID 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. In other words, CUI shall serve 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 NID is applicable to NASA Headquarters and all NASA Centers, including Component Facilities, Federally Funded Research and Development Centers and (FFRDCs) and Technical and Service Support Centers.

b. This NID is applicable to all NASA civil service employees who require access to CUI in the performance of their duties.

c. Consistent with 32 C.F.R. § 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 contractors, grant recipients, and cooperative partners, by incorporation into agreements or other information sharing agreements. , NASA contractor employees, personnel completing work through domestic and international agreements,

d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

e. In this NID, 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. E.O. 13556, Controlled Unclassified Information.

c. Controlled Unclassified Information, 32 CFR Part 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. NPR 1600.2, NASA Classified National Security Information (CNSI)

d. NPD 2521.1, Communications and Material Review

e. NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

f. NPR 9710.1, General Travel Requirements

g. NARA CUI Marking Handbook (www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf)

h. 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)

i. NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

j. NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020 (updated 12-10-2020)

k. NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, December 2014

l. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 1, December 2016

m. Standard Form (SF) 901, Controlled Unclassified Information Coversheet

P.5 Measurement/Verification

a. To determine Center compliance with E.O. 13556, 32 CFR pt. 2002, and this NID, Center Directors and Center Chief Information Security Officers (CISOs) will determine and document compliance through annual self-assessments and reviews conducted by the Office of the Chief Information Officer (OCIO). Each Center CISO or designee will conduct assessments of select organizations throughout their Center on a yearly basis to determine if Center organizations are in compliance with this NID. OCIO will provide the Centers with a NARA Information Security Oversight Office (ISOO) annual data call to ensure that all Center reviews will be tailored to include all steps necessary to perform a comprehensive review of all pertinent areas within a Center.

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 Controlled Unclassified Information 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. Not applicable—new policy.

Chapter 1. Introduction

1.1 Overview

1.1.1 In November 2010, the President issued E.O. 13556, Controlled Unclassified Information (CUI), 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 applicable laws, regulations, and government-wide policies.

1.1.4 The National Archives and Records Administration (NARA) and their Information Security Oversight Office (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 Part 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 NID and in accordance with the E.O.

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.

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 Part 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. Notify authorized recipients and the public of any waivers NASA grants, and separately notify NARA.

n. 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.

o. 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 applicable to CUI.

p. Establish and maintain processes for handling CUI decontrol requests submitted by authorized holders.

q. Establish and maintain a mechanism by which authorized holders can contact a designated representative for instructions when they receive unmarked or improperly marked information NASA designated as CUI.

r. Coordinate with the Office of Procurement to ensure the Agency's Information Technology (IT)-focused contracts reflect the most current Federal Acquisition Regulation (FAR.

s. Ensure that NASA CUI policy-related documents reflect current CUI guidance and requirements specified by NIST.

t. 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.

u. Issue guidance regarding requirements for protecting CUI within IT systems and transmitting CUI via NASA email systems.

v. Retain a record of each waiver.

w. 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.

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

1.2.4 The NASA Chief Privacy Officer is designated as the CUI PM who 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. Throughout implementation, legacy markings and safeguarding

practices will exist at the same time but as implementation progresses, legacy markings and safeguarding practices will be phased out.

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 disposition schedules no longer require retention of the records.

b. In accordance with NASA records management policy, 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 NID.

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 it 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 NID.

1.2.7 The Center CIOs and HQ CIO shall:

a. Assess NASA systems that contain CUI and ensure that all federal information technology systems that are used to process CUI are categorized at no less than the federal baseline of moderate confidentiality impact level per FIPS PUB 199.

b. Ensure the agency applies security requirements and controls from FIPS PUB 199 and 200 and NIST SP 800-53 for Federal information systems that process, store, or transmit CUI.

c. Ensure the agency applies NIST SP 800-171 when establishing security requirement agreements to protect CUI's confidentiality on non-Federal information systems.

d. Issue guidance regarding methods for protecting CUI on public-facing websites and in cloud-based systems.

e. Ensure information systems that contain CUI have CUI markings or warnings as per 32 CFR Part 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

1.2.9 Contracting Officers, Contract Specialists, and Agreement Managers shall:

a. Include CUI security clauses and standards in their assigned contracts and agreements that deal with CUI.

1.2.10 Contracting Officer Representatives (CORs)

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 applicable contracts and agreements.

c. Ensure contractors receive training on CUI within 30 days of contract award or prior to accessing CUI, whichever occurs first.

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 NID.

(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 2.14–2.16, and 2.21.

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., and CFR.

c. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), Sensitive But Unclassified (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).

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, the E.O., and CFR.

c. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), Sensitive But Unclassified (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).

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 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 Freedom of Information Act (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 the FOIA and the Privacy Act.

b. Coordinate with the CUI SAO and CUI PM to resolve any conflicts between FOIA policy and CUI requirements.

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

1.2.17 The Chief Data Officer (CDO) shall consult, as necessary, with the SAO for CUI and the CUI PM to ensure appropriate 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 must 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, 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 2521.1B "Communications and Material Review" and sections 2.11.3 and 2.13 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.

Note: Examples of requirements for markings are included in sections C.2–C.4 of Appendix C.

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 or to prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency;

b. To improperly or unlawfully interfere with competition;

c. To improperly or unlawfully interfere with any right of employees provided for by statute or government-wide regulation;

d. To prevent or delay the release of information that does not require such protection; or

e. 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 a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding CUI marking 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, authorized holders must 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 Part 2002, the CUI Registry, and NARA's supplemental guidance (NARA CUI Marking Handbook) will be followed for the marking of CUI on paper and electronic documents. The NARA handbook provides examples of correctly marked CUI.

2.2.8 CUI markings. Designators of CUI 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 must 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. Banner markings may include up to three elements:

a. *The CUI control marking*. The CUI control marking will consist of the acronym "CUI". The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of CUI basic categories. Authorized holders who designate CUI may not use alternative markings to identify or mark items as CUI; e.g. NASA SENSITIVE.

b. *CUI category markings (mandatory for CUI Specified)*. If any part of a document contains CUI Specified, as found in the CUI Registry, then the category marking must appear in the banner, preceded by a "SP-" to indicate the specified nature of the category (e.g., CUI//SP-PRVCY). The CUI control marking, and any category markings are separated by a double forward slash (//). When including multiple categories in the banner they must be alphabetized, with specified categories appearing before any basic categories.

> Note: Multiple categories in a banner line will be separated by a single forward slash (/) and in alphabetical order, e.g. CUI//SP-EXPT/SP-PRVCY.

c. *Limited Dissemination Control Markings (LDCM)*. NARA has published a list of LDCMs that are the only ones that may be applied. These markings appear in the CUI Registry and include such controls as FED ONLY (Federal Employees Only), NOCON (No dissemination to Contractors), and DL ONLY (Dissemination authorized only to those individuals or entities on an accompanying distribution list). LDCMs are preceded by a double forward slash (//) and appear as the last element of the CUI banner marking, e.g. CUI//SP-EXPT/SP-PRVCY//NOFORN.

2.2.9 LDCMs may only be applied to CUI to bring attention to any dissemination control called for in the underlying authority or to limit the dissemination of CUI. LDCMs should be used only after carefully considering the potential impacts on the timely dissemination of the information to authorized recipients.

2.2.10 The content of the CUI banner marking must apply to the whole document (i.e., inclusive of all CUI within the document) and must be the same on each page of the document.

2.2.11 Specific marking, disseminating, informing, distribution limitation, or warning statements that are required by underlying authorities also may be placed on the document, but not within the banner or portion markings. These markings or indicators must be placed on the document as prescribed by the underlying law, regulation, or government-wide policy. Questions regarding the placement of such markings may be referred to the responsible authority for the information. For example, additional warnings may be required for export controlled information, questions about export controlled information should be directed to the cognizant export control administrator.

2.2.12 CUI designation indicator (Mandatory). On the first page or cover page of all documents containing CUI, the person or office that designated the CUI (the designator) will be identified. This identification may be accomplished through a "Controlled by" line.

2.2.13 Where feasible, a specific decontrolling date or event will be included with all CUI. This inclusion may be accomplished in a manner that makes the decontrolling schedule clear to an authorized holder.

2.2.14 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 must be used throughout the entire document. All portions or sections must be portion marked, even those that do not contain CUI. Sections that do not contain CUI should be marked with as Uncontrolled Unclassified Information, designated with a [U].

2.3.4 For examples on portion marking of documents, see the NARA CUI Marking Handbook.

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

2.4.1 Authorized holder who includes CUI in documents that also 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 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 which contain both 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 1600.2A NASA Classified National Security Information (CNSI).

2.4.3 The CUI Registry and the NARA CUI Marking Handbook contain guidance on marking CUI when commingled with CNSI.

2.5 CUI Cover Sheets

2.5.1 Standard Form (SF) 901 is the only authorized CUI cover sheet. The SF 901 cover sheet may be obtained from GSA or downloaded from the NARA CUI site and may then be reproduced by user offices. An example cover sheet is included in section C.5 of Appendix C.

2.5.2 Cover sheets identify CUI and serve as a shield to protect the attached CUI from inadvertent disclosure. See Section 2.14.

2.6 Legacy Materials

2.6.1 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 and expected to be transmitted outside of NASA. If the legacy material is not re-marked, an alternate permitted marking method must be used (i.e. CUI coversheet).

2.6.2 The following protocols guide 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 must evaluate the information and remark it as CUI.

(2) The receiving organization must also adhere to any Agency marking waivers as they apply to internal dissemination. See 2.23 regarding waivers.

(3) The receiving organization will apply any Limited Dissemination Control Markings (LDCMs). See also 2.10.2.

(4) Receiving organizations will 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:

(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.

2.7 Working Papers

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

2.7.2 Working papers containing CUI must be marked the same way as the finished product containing CUI would be marked and as required for any CUI contained within. Working papers must be protected as any other CUI. This protection applies whether or not the working papers will be destroyed. When no longer needed, working papers shall be destroyed in accordance with section 2.18 below.

2.8 Using Supplemental Administrative Markings with CUI

2.8.1 Supplemental administrative markings (e.g., “Pre-decisional,” “Deliberative,” “Draft”) may be used at NASA with CUI with specific restrictions as described in this section. The NARA CUI Marking Handbook provides examples of permitted supplemental administrative markings.

2.8.2 Supplemental administrative markings may not impose additional safeguarding requirements or disseminating restrictions or designate the information as CUI. Their purpose is to inform recipients of the status of documents under development to avoid confusion and maintain the integrity of a decision-making process.

2.8.3 Supplemental markings may not appear in the CUI banners, nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings.

2.8.4 Supplemental administrative markings must not duplicate any CUI marking described in the CUI Registry.

2.8.5 Supplemental markings, other than the universally-accepted "DRAFT," will, on the first page or the first time it appears, include an explanation or intent of the marking, e.g, Pre-decisional – "The information in this document provides background, options, and/or recommendations about [topic]. It is not yet an accepted policy." (This is an example only. The language may be changed to suit the topic.)

2.9 Unmarked CUI

2.9.1 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 Sensitive But Unclassified, need only be remarked as CUI if it is re-shared. See section 2.6.

2.10 Sharing of CUI (Accessing and Disseminating)

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

a. Abides by the 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.

2.10.2 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

g. display only, DISPLAY ONLY

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

a. attorney client, Attorney-Client

b. attorney work product, Attorney-WP

c. deliberative process, Deliberative

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

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

2.10.6 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 2.10.1:

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 must include a requirement for the recipient to, at a minimum, comply with E.O. 13556; 32 CFR Part 2002; and the CUI Registry.

2.10.7 Foreign entity sharing. 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 Part 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. Other markings or protective measures may not be used.

2.10.8 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.

2.10.9 Information-sharing agreements with non-executive branch entities must include provisions that CUI be handled in accordance with the CUI Program; non-executive branch entities should familiarize themselves with the distinction between CUI Basic and CUI Specified information, and the markings and handling procedures for each; non-executive branch entities and other authorized holders of CUI will be responsible for handling CUI in compliance with the requirements of this rule and the CUI Registry, through a forthcoming Federal Acquisition Regulation (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 must be reported to the CUI PM. When NASA is not the designating agency, personnel must report any non-compliance to the designating agency.

2.10.10 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.

2.10.11 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 through the use of authorized LDCMs.

2.11 CUI Disclosure Statutes

2.11.1 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 purposes.

2.11.2 CUI and the Freedom of Information Act (FOIA). FOIA 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 must be based upon the content of the information and applicability of any FOIA 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 through a FOIA or Privacy Act request and response, 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 FOIA disclosure results in public release and the CUI does not otherwise have another legal requirement for its continued control).

2.11.3 CUI and the Whistleblower Protection Act. 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, E.O. or directive.

2.11.4 CUI and the Privacy Act. The fact that records are subject to the Privacy Act of 1974 does not mean that the records should be marked as CUI. Information contained in Privacy Act systems of records may also be subject to controls under other CUI categories and may need to be marked as CUI for that reason. In addition, when determining whether certain information must be protected under the Privacy Act or whether the Privacy Act allows an individual the right to access their information maintained in a system of records, the decision to release must

be based upon the content of the information as well as Privacy Act 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 the Privacy Act does not result in decontrol for any other purpose inconsistent with this NASA policy.

2.12 Challenges to Designation of Information as CUI

2.12.1 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.

2.12.2 If the information at issue is involved in litigation, or the challenge to its designation or marking as CUI arises as part of litigation, whether the challenger may access the information will be addressed via the litigation process.

2.12.3 Challengers should nonetheless notify the CUI PM of the issue through the process described below and include its litigation connection.

2.12.4 If any NASA organization receives a challenge, the CUI Liaison for that organization shall work with the NASA CUI PM to take the following measures:

a. Acknowledge receipt of the challenge,

b. Provide an expected timetable for response to the challenger,

c. Review the merits of the challenge with a subject matter expert,

d. Offer an opportunity to the challenger to define a rationale for belief that the CUI in question is incorrectly designated,

e. Notify the challenger of NASA's decision, and

f. Provide contact information of the official making the decision in this matter.

2.12.5 Until the challenge is resolved, the challenged CUI, including challenges to unmarked CUI, should continue to be safeguarded and disseminated at the control level indicated in the markings or presumed category.

2.12.6 If a challenging party disagrees with NASA's response to a challenge, that party may use the dispute resolution procedures described in 32 CFR § 2002.52.

2.13 Decontrol of CUI

2.13.1 When control is no longer needed, NASA should decontrol any CUI that it designates. This means the information should be removed from the protection of the CUI program as soon as practicable when the information 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. This section covers the processes by which CUI is decontrolled.

2.13.2 Automatic Decontrol. CUI may be decontrolled automatically for all or limited purposes upon the occurrence of one of the conditions below, or through an affirmative decision by the designator:

a. When laws, regulations or government-wide policies no longer require the information's control as CUI and the authorized holder has the authority under the authorizing law, regulation, or government-wide policy

b. When the designating agency decides to release the CUI to the public by making an affirmative, proactive disclosure

c. When an agency discloses the information in accordance with an information access statute, such as the Freedom of Information Act (FOIA) or the Privacy Act (when legally permissible), provided the designator's agency incorporates such disclosures into its public release processes

(1) Disclosure under FOIA does not automatically constitute CUI decontrol for all purposes. For more information, see section 2.11.2.

(2) Disclosures under the Privacy Act constitute decontrol only with respect to the limited purpose of disclosure to the individual who requested access to their records maintained in a system of records. For more information, see section 2.11.4.

d. When indicated by a decontrol marking specifying a decontrol date or event, CUI is decontrolled without further review by the originator.

e. Information controlled for export control regulations are not subject to automated decontrol.

2.13.3 Positive Decontrol. A designating agency may also decontrol CUI:

a. In response to a request from an authorized holder to decontrol it

b. Concurrently with any declassification action under E.O. 13526 or any predecessor or successor order, as long as the information also qualifies for decontrol as CUI

c. Information controlled for export control regulations shall not be decontrolled without the concurrence from the Headquarters Export Administrator

2.13.4 Central Decontrol.

a. The Archivist of the United States may decontrol records transferred to the National Archives and Records Administration (NARA) in accordance with 32 CFR § 2002.34, absent a specific agreement to the contrary with the designating agency.

b. The Archivist decontrols records to facilitate public access pursuant to 44 U.S.C. 2108 and NARA's regulations at 36 CFR parts 1235, 1250, and 1256. When feasible, CUI is decontrolled prior to the transfer of records to the NARA. When decontrol is not feasible prior to transfer, the CUI status of the information is indicated on a Transfer Request or an SF 258 paper form. Any other indication of CUI status, such as markings on the container, are not valid.

2.13.5 A Center or Mission Directorate may designate in its CUI policies which personnel it authorizes to decontrol CUI, consistent with law, regulation, and government-wide policy.

2.13.6 Decontrolling CUI for purposes other than FOIA disclosure relieves the requirement to handle the information under the CUI Program but does not constitute authorization for public release.

2.13.7 Personnel must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, releasing to the public, or donating the CUI to a private institution. Otherwise, personnel do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

2.13.8 For relatively short documents, all CUI markings within a decontrolled CUI document will be removed or struck through. For large documents, personnel may remove or strike through only those CUI markings on the first or cover page of the decontrolled CUI and markings on the first page of any attachments that contain CUI. They shall also mark or stamp a statement on the first page or cover page indicating that the CUI markings are no longer applicable.

2.13.9 If personnel use decontrolled CUI in a newly created document, they must remove all CUI markings for the decontrolled information. When indicated by a decontrol marking specifying a decontrol date or event, CUI is decontrolled without further review by the originator.

2.13.10 Once decontrolled, any public release of information that was formerly CUI must be in accordance with law and policies on the public release of information.

2.13.11 Authorized holders may request that the designating agency decontrol CUI that they believe should be decontrolled.

2.13.12 If an authorized holder publicly releases CUI in accordance with the designating agency's (not NASA) authorized procedures, the release constitutes decontrol of the information.

2.13.13 Unauthorized disclosure of CUI does not constitute decontrol.

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

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

2.14 Safeguarding and Storage

2.14.1 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.

2.14.2 Unless different protection is specified in the CUI Registry, documents and removable storage containing CUI must be password protected or otherwise stored in a locked office, locked drawer, or locked file cabinet whenever it is unattended.

2.14.3 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.

2.14.4 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 document while in use, but must 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 authorized to remove CUI from a controlled environment, NASA personnel shall keep CUI under their direct control at all times or protect it with at least one physical barrier and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.

2.14.5 Safeguarding While Traveling. All reasonable measures will be taken (e.g. secure transmission, approved electronic USB or other authorized method 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 others may be exposed to it. 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.

2.14.6 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.

2.14.7 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 Part 2002.14

2.15 Reproduction of CUI

2.15.1 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).

2.15.2 When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, management officials must ensure that the equipment does not retain data, or else they must 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.

2.16 Shipping or Mailing CUI

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

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

2.16.3 Address packages and parcels that contain CUI for delivery only to an individual recipient, not to an office or organization. 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.

2.17 Transmittal Document Marking Requirements

2.17.1 When a transmittal document accompanies CUI, the transmittal document must 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.

2.17.2 The notice will 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."

2.18 Destruction of CUI

2.18.1 CUI may be destroyed:

a. When the information is no longer needed by the agency, and

b. When records disposition schedules, published or approved by NARA or other laws, regulations, or government-wide policies, no longer require retention of the CUI.

2.18.2 Destruction of CUI, including in electronic form, must make the CUI unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI must be destroyed according to directives regarding the information. If the authority does not specify a destruction method, agencies must use one of the following methods:

a. Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-88, Guidelines for Media Sanitization or guidance in NARA CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form.

b. Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or succeeding guidance.

c. Using National Security Agency approved devices for device sanitization. See https://www.nsa.gov/resources/evervone/media-destruction.

2.19 Misuse of CUI and Incident Reporting

2.19.1 The CUI PM shall report suspected or confirmed misuse of CUI via NASA's incident response process (i.e. through the Security Operations Center) and to the organization's CUI Liaison immediately.

2.19.2 The CUI Liaison shall obtain the details of the situation, coordinate with a subject matter expert regarding the severity of the incident and report the results of the investigation to the CUI PM within 24 hours of discovery.

2.19.3 The CUI Liaison shall coordinate mitigation measures within their incident response and management structures and provide regular status reports to the CUI PM until mitigation efforts are complete.

2.19.4 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 Executive Order 13556 and 32 CFR 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 2.14. (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 2.18. (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.

2.19.5 The CUI PM, in conjunction with the CUI SAO and Office of the Chief Human Capital Officer (OCHCO), will advise the supervisor of the employee's misuse of CUI and recommend that the supervisor take appropriate action. Depending of the circumstances of the employee's misuse of CUI, the supervisor shall take her disciplinary action as appropriate, and/or assess whether other corrective action may be warranted. (e.g., emphasis in training). The CUI PM shall report misuse of CUI that has been designated by another Executive agency to that agency of the offending organization.

2.19.6 Incidents involving PII will be reported in accordance with ITS-HBK-1382.05, Privacy Incident Response and Management: Breach Response Team Checklist.

2.20 Sanctions for Misuse of CUI

2.20.1 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 shall be referred to the cognizant contracting officer who will notify the contractor and then determine whether other appropriate action is necessary.

2.20.2 When an employee is found to be responsible for the commission of a CUI incident, he/she 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;

f. Consistency of the sanction with those imposed on other employees for the commission of the same or similar CUI incident.

2.20.3 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, as appropriate.

2.21 CUI Within Information Systems

2.21.1 IT systems containing CUI must minimally meet the federal baseline of moderate per FIPS PUB 199.

2.21.2 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 must 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. 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.

2.21.3 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 must inform entities employing non-federal information systems that they must follow the requirements of NIST SP 800-171 to protect CUI Basic, unless specific requirements are specified by law, regulation, or government-wide policy for protecting the information's confidentiality.

2.21.4 NIST Special Publication 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 must meet if they have NASA CUI on their computer systems.

2.21.5 National Security Systems authorized to store, process, and/or transmit classified information under NPR 1600.2, *NASA Classified National Security Information (CNSI)*, are considered compliant with the necessary protections of CUI.

2.22 CUI Self-Inspection Program

2.22.1 NASA will implement a Self-Inspection Program as follows:

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

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

2.23 Waivers to CUI Requirements

2.23.1 In compliance with NPR 8000.4's 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, due to 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 2.6.2, the NASA CUI SAO has granted a legacy material limited re-marking waiver.

2.23.2 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.

2.23.3 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 while it is within NASA's possession or control, unless specifically prohibited by laws, regulations, or government-wide policies.

2.23.4 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 must be made aware of the CUI status of any disseminated information.

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

2.23.6 Refer to Section 2.6 for NASA legacy material waiver information.

2.24 CUI Education and Training

2.24.1 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.

2.24.2 Refresher training is required annually after the initial training, or whenever there are significant changes to CUI policy or processes.

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

2.24.4 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 Part 2002, and approved NASA CUI policy and guidelines. Generally, this is all trained NASA employees and contractors.

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 Part 2002, and the CUI Registry).

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

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.

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 Part 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 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.

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 Part 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.

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 Part 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 Part 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 Controls 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 Part 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 must 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

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

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

Appendix C Resources

C.1 Web Resources

C.1.1 CUI Registry Website: <https://www.archives.gov/cui/registry/>

C.1.2 NASA CUI Website: <https://nasa.sharepoint.com/sites/privacy/>

C.1.3 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.1.4 NARA CUI Marking Handbook: <https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>

C.1.5 CUI Registry: Limited Dissemination Controls: <https://www.archives.gov/cui/registry/limited-dissemination>

C.1.6 Trigraph Country Codes for Use with REL TO Limited Dissemination Control for CUI: <https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/20161214-country-trigraph-codes.pdf>

C.1.7 Standard Form 901 (11-2018) cover sheet: <https://www.gsa.gov/cdnstatic/SF901-18a.pdf>

C.1.8 National Security Agency-approved devices for device sanitization: <https://www.nsa.gov/Resources/Media-Destruction-Guidance/>

C.2 Example CUI Markings

Example CUI Markings

CUI	CUI Basic information
CUI//SP-PROPIN	CUI Specified, proprietary information
CUI//NOFORN	CUI Basic, no foreign dissemination
CUI//SP-PROPIN//NOFORN	CUI Specified, proprietary information, no foreign dissemination

CUI Control Marking	CUI Category Marking(s)	Limited Dissemination Marking(s)
The CUI control marking will consist of the acronym "CUI". The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of CUI basic categories.	If any part of a document contains CUI Specified, a category marking must appear to indicate the specified nature of the category. CUI Basic can optionally include a category marking.	Limited Dissemination Control Markings may only be applied to CUI to bring attention to any dissemination control called for in the underlying authority or to limit the dissemination of CUI.

Common CUI Categories and Dissemination Controls

CUI Specified

SP-CTI Controlled Technical Information
SP-EXPT Export control information
SP-PERS Personnel records
SP-PROCURE General Procurement and Acquisition
SP-PROPIN Proprietary records
SP-SSEL Source Selection

CUI Basic

PRIVILEGE Legal Privilege

Note: full list available on the NARA CUI repository at: https://www.archives.gov/cui/registry/category-list

DL ONLY Dissemination List Controlled
FED ONLY Federal Employees Only
FEDCON Federal Employees and Contractors
NOFORN No Foreign Nationals
REL TO [USA, LIST] Authorized for release to certain nationals only

Used only with PRIVILEGE Category

Attorney-Client Attorney-client privileged
Attorney-WP Attorney Work Product
Deliberative Deliberative Process

Note: full list available on the NARA CUI repository at: https://www.archives.gov/cui/registry/limited-dissemination

Figure C-1. Example CUI markings

C.3 CUI Marking Locations

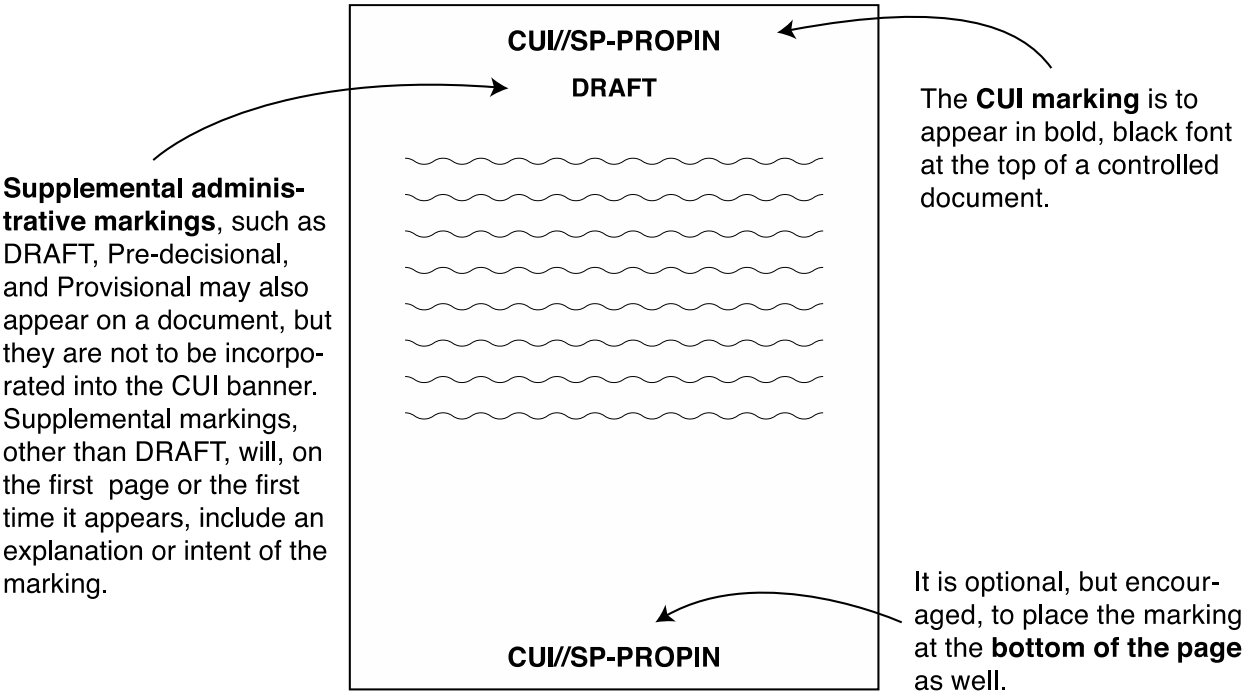

Figure C-2. Overview of marking locations on a CUI document

C.4 CUI Email Marking

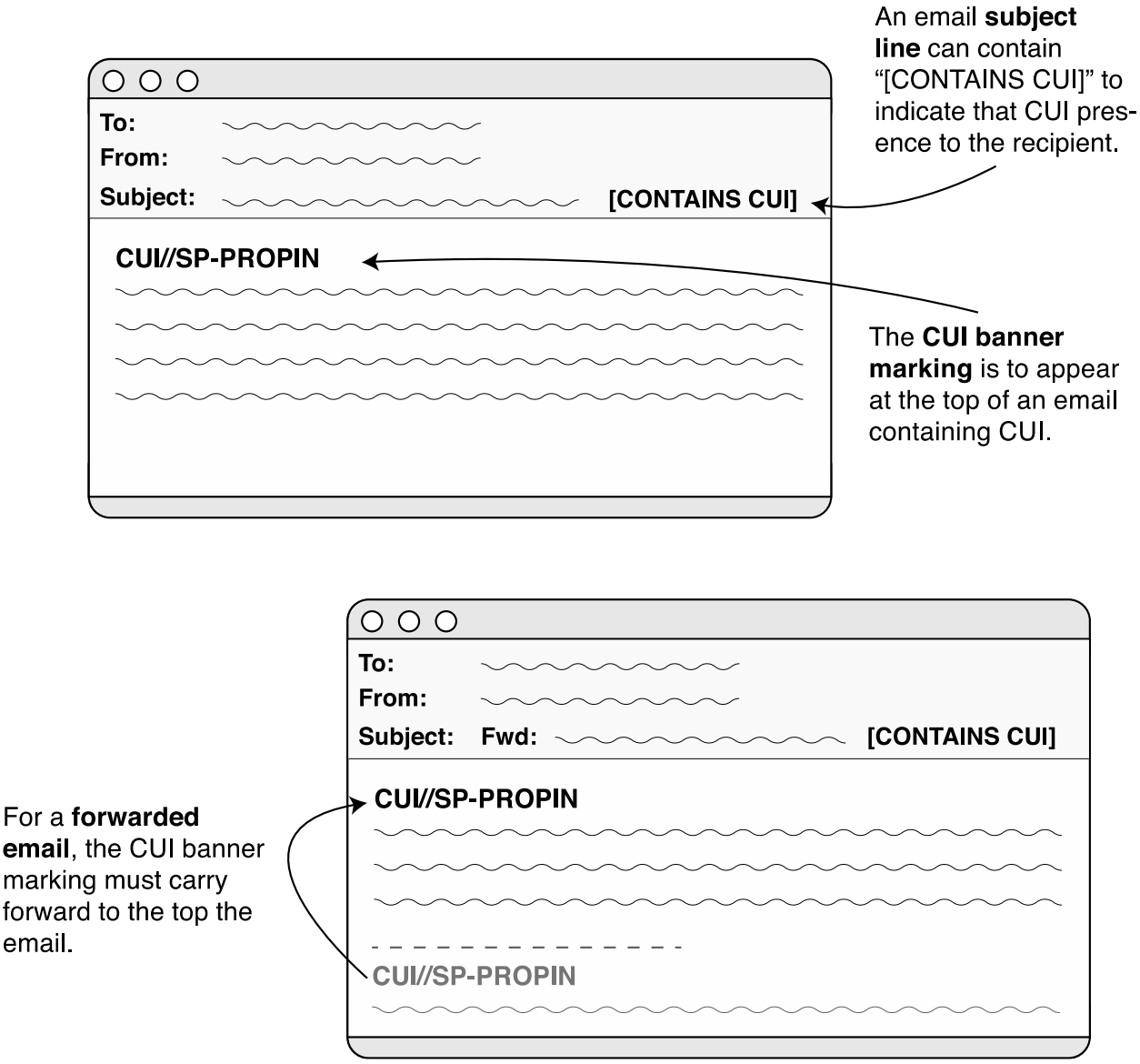

Figure C-3. CUI email marking information

C.5 CUI Cover Sheet

Figure C-4. CUI cover sheet (click to download PDF)