

February 10, 2022

ACTION MEMORANDUM TO THE SECRETARY

From: Philip McNamara
Office of the Assistant Secretary for Administration

Subject: DOT Order 1650.5, Controlled Unclassified Information Program

ACTION REQUESTED

I request that you approve the attached proposed U.S. Department of Transportation (DOT) Order, DOT Order 1650.5, Controlled Unclassified Information (CUI) Program.

SUMMARY

The attached Order serves several purposes:

- Cancels Chapter 5, For Official Use Only Information (FOUO), of DOT Order 1640.4D and creates DOT Order 1650.5 to reflect current authorities.
- Ensures proper handling, safeguarding, and dissemination control of CUI per Executive Order (EO) 13356 and part 2002 of Title 32, Code of Federal Regulations. This Order will formally establish the Agency CUI Program in accordance with those authorities.

BACKGROUND

In November 2010, the President issued EO 13356, establishing an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls. Prior to this EO, the federal government employed agency specific policies, procedures and marking for information. The Department employed the marking “For Official Use Only,” but other departments used “Sensitive But Unclassified,” “Law-Enforcement Sensitive,” and other markings, or combinations thereof. The diversity of markings and associated protection requirements led to inconsistent implementation, particularly when sharing within the government. EO 13356 established a program for managing CUI and emphasized openness and uniformity of Government-wide practice.

The Information Security Oversight Office (ISOO), National Archive and Records Administration (NARA) was established as the Executive Agent and tasked with implementing the CUI program throughout the executive branch. After extensive interagency consultations, ISOO promulgated 32 CFR part 2002 to define the CUI program. The program standardizes the way the executive branch handles unclassified controlled information that requires protection under laws, regulations, or government wide policies that do not qualify as national security information under EO 13526, Classified National Security Information. This includes consistent marking as “Controlled Unclassified

Information” or “CUI,” and markings for specific types of unclassified information subject to heightened protection requirements by law, regulation, or government-wide policy.

Once approved, the order will be signed by the Assistant Secretary for Administration.

RECOMMENDATION

I recommend that you approve the proposed Order, DOT Order 1650.5, Controlled Unclassified Information Program.

The Secretary

APPROVED:



DATE:

2/10/22

COMMENTS:

Attachments:

- Proposed order, DOT 1650.5
- Chapter 5 – DOT Order 1640.4D

Subject: CONTROLL OF UNCLASSIFIED INFORMATION PROGRAM

1. PURPOSE. This Order implements Executive Order (EO) 13556 and 32 CFR part 2002 concerning Controlled Unclassified Information (CUI). These directives establish national policy on the handling, safeguarding, and control of unclassified information the Government creates, stores, transmits, processes, or possesses that a law, regulation, or Government-wide policy requires or specifically permits an agency to handle by means of safeguarding and dissemination controls. Classified National Security Information (CNSI) is not included in the CUI Program.
2. CANCELLATIONS. This order cancels Chapter 5, For Official Use Only Information (FOUO), of DOT Order 1640.4D, December 9, 1997.¹
3. BACKGROUND.
 - a. In November 2010, the President issued EO 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010) to establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls.” At the time EO 13556 was issued, more than 100 different markings for such information existed across the executive branch. This ad hoc, agency-specific approach created inefficiency and confusion, led to a patchwork system that failed to adequately safeguard information requiring protection in some instances, and unnecessarily restricted information-sharing in others.
 - b. As a result, the EO established the CUI Program to standardize the way the executive branch handles information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (excluding information that is classified under EO 13526, Classified National Security Information, 75 FR 707 [December 29, 2009], or any predecessor or successor order; or the Atomic Energy Act of 1954 [42 U.S.C. § 2011, *et seq*], as amended).
 - c. The National Archives and Records Administration (NARA) is the CUI Executive Agent (EA) responsible for developing policy and providing oversight for the CUI Program. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
 - d. The CUI EA has established an internet-based CUI Registry that serves as the authoritative reference for all information, guidance, policy, and requirements on

¹ DOT Order 1640.4 was cancelled earlier except for its Chapter 5 which remained in effect until cancelled. This Order cancels Chapter 5.

handling CUI, including everything issued by the CUI EA other than 32 CFR part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

4. SCOPE. Except as provided in section 3, this Order applies to all Department of Transportation (DOT) Operating Administrations and Secretarial Offices (components), the Office of Inspector General (OIG), and to all DOT CUI users in these components. For the purposes of this Order, DOT CUI users include every DOT employee, contract employee, and affiliated person who may encounter CUI in their duties. This Order also applies to DOT affiliated parties such as consultants, researchers, organizations, students, interns, individuals detailed or assigned to DOT and State, Local, Tribal, and private sector partners with whom DOT may share CUI.
5. LIMITATIONS ON SCOPE OF THIS ORDER. Any CUI requirements contained within this Order or DOT component CUI policies that are not supported by law, regulation, or Government-wide policy may not be applied to entities outside DOT unless a law, regulation, or Government-wide policy requires or permits the controls contained in the agency policy to be applied to entities outside DOT, and the CUI Registry lists that law, regulation, or Government-wide policy as a CUI authority. When entering into information-sharing agreements with entities outside DOT, DOT components may not include additional requirements or restrictions on handling CUI other than those permitted in the CUI Program requirement.
6. REFERENCES.

EO 13556, Controlled Unclassified Information, dated November 4, 2010.

EO 13526, Classified National Security Information, dated December 10, 2009.

32 CFR part 2002, Controlled Unclassified Information, dated September 14, 2016.

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.

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

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

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

NIST SP 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, dated February 2020 (updated February 2021).
7. DEFINITIONS. See Appendix B, Definitions,

8. POLICY.

DOT will protect all CUI in accordance with national directives and this Order, ensure that sharing partners exercise the same care, and remove any CUI-mandated controls on the information once it loses its sensitivity.² If an authorized holder of information has significant doubt about whether it should be treated as CUI, he/she should consult with the Office of the General Counsel, M-40 Senior Agency Official (SAO), CUI Program Manager, and/or other interested stakeholders as appropriate. After that, if there remains significant doubt about whether information should be designated as CUI, it will not be designated unless approved by the CUI SAO.

There will be a phased implementation of the CUI program over a two-year period, in accordance with guidance issued by the CUI EA. Upon full implementation, all DOT CUI users will discontinue using any legacy³ or other markings not permitted by the CUI Program not listed in the CUI Registry.

9. RESPONSIBILITIES.

a. The Assistant Secretary for Administration will:

- 1) Ensure senior leadership support;
- 2) Make adequate resources available to implement, manage, and comply with the requirements of EO 13556, 32 CFR part 2002, and this Order;
- 3) Designate and advise the CUI EA of the CUI SAO responsible for oversight of CUI Program implementation, compliance, and management, and include the official in all contact listings;
- 4) Advise the CUI EA of any changes to the designated SAO; and
- 5) Approve DOT policies as needed to implement the CUI Program.

b. The Director, Office of Security will:

- 1) Serve as DOT designated SAO for CUI;
- 2) Direct and oversee DOT's CUI Program;
- 3) Make requests for adequate resources to implement, manage, and comply with the National CUI Program;

² Removal of CUI controls does not constitute authorization to release the information. Public availability of information remains to be determined under 5 U.S.C. § 552 and 49 CFR part 7.

³ Legacy-marked information contains markings that were in use before the advent of the CUI Program, e.g., For Official Use Only (FOUO) and Sensitive But Unclassified (SBU). Some legacy markings are carried over as Subcategories of the CUI Program (e.g., Sensitive Security Information [SSI]), and some are discontinued (e.g., FOUO and SBU).

- 4) Designate a CUI Program Manager;
- 5) Develop and execute current DOT-wide policies and procedures necessary to manage a CUI program that complies with EO 13556 and 32 CFR part 2002;
- 6) Develop and implement an education and training program pursuant to 32 CFR part 2002.30 to include monitoring for compliance with training requirements;
- 7) Ensure the training and education program includes sufficient information to allow all DOT CUI users to understand and carry out their obligations with respect to protecting, storing, transmitting, transporting, and destroying CUI materials;
- 8) Upon request of the CUI EA, provide updates of DOT's CUI implementation efforts;
- 9) Assist in and respond to audits conducted by the CUI EA;
- 10) Provide a description of all waivers granted in the annual report to the CUI EA, along with the rationale for each waiver and the alternative steps being taken to ensure sufficient protection of CUI within DOT (see section 33e);
- 11) Develop and implement DOT's self-inspection program;
- 12) Establish processes and criteria for reporting and investigating misuse of CUI;
- 13) Establish a process to manage waiver requests of CUI requirements within DOT and those submitted by other agencies. Notify authorized recipients and the public of any waivers DOT grants (unless such notice is otherwise prohibited by law, regulation, and Government-wide policy) and separately notify the CUI EA;
- 14) Submit to the CUI EA any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that the agency proposes to use to designate unclassified information as CUI;
- 15) Coordinate with the CUI EA, as appropriate, 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;
- 16) Establish processes for managing CUI decontrol requests submitted by authorized holders;
- 17) Establish a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for instructions when they receive improperly marked information the agency designated as CUI; and
- 18) Establish a process to accept and manage challenges to CUI status (which may include improper or absent marking).

- c. The CUI Program Manager will:
- 1) Implement the CUI Program within DOT as described in this Order and in national policies and directives;
 - 2) Serve as DOT's official representative to the NARA CUI EA on DOT's day-to-day CUI Program operations, both within DOT and in interagency contexts;
 - 3) Serve as DOT's official representative on the Interagency CUI Advisory Council to advise the CUI EA on the development and issuance of policy and implementation guidance for the CUI Program;
 - 4) Serve as DOT's subject matter expert in CUI, advising DOT Components on their CUI programs, oversee the implementation and management of the CUI Program, and provide assistance where applicable to ensure consistent implementation of CUI requirements throughout DOT;
 - 5) Oversee the implementation and management of the CUI Program among the DOT components and provide assistance where applicable to ensure these components are conducting oversight for consistency throughout DOT;
 - 6) Lead a CUI Working Group of legal and program representatives from each component to develop and guide the implementation and continuing management of the CUI Program;
 - 7) Convey requirements for training and reporting to DOT components; consolidate status reports from the components and forward DOT reports to the NARA CUI EA;
 - 8) Consult with DOT components to develop a basic CUI training program for DOT;
 - 9) Coordinate and assist DOT components with developing additional or specialized training for their organization;
 - 10) Maintain a CUI Program information portal or SharePoint site with frequently encountered CUI Category, Sub-Category, and SP instructions; and
 - 11) Oversee and lead mitigation efforts to investigate incidents involving CUI. Inform SAO and Agency Head, as appropriate, of any significant CUI incidents as well as any incident trends found within the agency or nationally.
- d. The Operating Administration Heads, the Inspector General, and Secretarial Office Directors will:
- 1) Appoint a primary and an alternate employee as CUI Points of Contact (POC) to assist in implementing and managing the CUI Program within their organizations, and

- to represent their organizations on the CUI Working Group established by the CUI PM to disseminate policy and training within their modes;
- 2) Notify the CUI PM of any change to the designated CUI POC for their organization;
 - 3) Ensure CUI procedures and practices within their organizations comply with DOT's CUI requirements as specified in this Order, including waiver requests from within DOT and outside agencies; and
 - 4) Make adequate resources available to implement, manage, and comply with the CUI Program.
- e. The Chief Information Officer will:
- 1) Establish an inventory of CUI systems and coordinate with Secretarial Offices and Operating Administrations to ensure these systems protect CUI using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards and Departmental Cybersecurity Policy.
 - 2) Establish standards/tools/processes for protecting CUI within IT systems (including email) and transmitting CUI from DOT email systems commensurate with moderate confidentiality; (for FAA see (1) of this section);
 - 3) Identify standards/tools/processes for sanitizing media processing or storing CUI consistent with NIST SP 800-88, Guidelines for Media Sanitization.
- f. The Office of the General Counsel will:
- 1) Advise the CUI SAO and PM on any CUI policy, plan, or guidance proposed to be issued to CUI users;
 - 2) Review any recommendation for a new CUI category proposed to be included in the CUI Registry before it is sent to the CUI EA;
 - 3) Participate in the CUI Working Group; and
 - 4) Provide any legal assistance and review of policy requested by the CUI SAO or PM on CUI.
- g. The Primary and Alternate CUI Point of Contact will:
- 1) Complete all training as required to ensure their full capability to function as the CUI POC for their organization; conduct oversight actions to ensure compliance within this area of responsibility and report findings to the DOT CUI PM;
 - 2) Serve as their organization's CUI program lead, responding to most inquiries from their organizations and consulting with DOT's CUI PM for matter outside of their experience;

- 3) Serve on DOT's CUI Working Group as their organization's representative to assist in developing, implementing, and managing CUI policy and programs throughout DOT;
 - 4) Coordinate with CUI PM to complement DOT's CUI materials and address needs of their organization; e.g., identify the categories and subcategories that would be frequently encountered in their components;
 - 5) Maintain their component's section of the CUI web site or SharePoint site with current information;
 - 6) Ensure all personnel within their component complete initial and recurring training as required, and report the progress of training to the CUI PM;
 - 7) Conduct annual self-inspections of their program to reflect the progress of implementation and report the results of those self-inspections to the CUI PM;
 - 8) Provide input from their components on all other reporting requirements to the CUI PM, to enable DOT response to NARA's CUI EA;
 - 9) Report instances of potential CUI violations or infractions to the CUI PM; and
 - 10) Keep track of violations for reporting purposes.
- h. The Contracting Officers (COs) and Contracting Officer Representatives (CORs) will:
- 1) Ensure that the applicable Federal and DOT CUI security clauses are included in their assigned contracts executed after issuance of this order, including, where applicable, required Federal Acquisition Regulation and Transportation Acquisition Regulation clauses (for FAA, Acquisition Management System (AMS)) and in agreements including memoranda of agreement (MOAs) and interagency agreements (IAAs), other transactions (OTs). CORs will also ensure contractors, and those entering into agreements, are aware of and understand the CUI security clauses in their assigned contracts/agreements; and
 - 2) Include in all contracts and agreements including MOAs, IAAs, and OTs that may involve CUI a clause requiring that the contractor and the parties to the agreement comply with NIST SP 800-171 for any nonfederal computer system they operate that contains CUI. See 32 CFR 2002.14(h)(2) for more information.
- i. The DOT CUI Users will:
- 1) Complete all initial and recurring assigned CUI training within the required timeframes;
 - 2) Manage, mark, and protect in accordance with this Order and national directives; and

- 3) Ensure that legacy-marked information (e.g., For Official Use Only (FOUO), or Sensitive But Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the information leaves DOT. Only markings that are contained in the NARA CUI Registry⁴ may be used to mark CUI. (See section 17c. of this Order).

10. KEY ELEMENTS OF THE CUI PROGRAM.

- a. The CUI Registry: The CUI Registry has been established by NARA as the central repository (other than EO 13556 and 32 CFR part 2002) for all information, guidance, policy, and requirements on handling CUI, including authorized CUI categories and subcategories, associated markings, and applicable decontrolling procedures. The CUI Registry can be found at: <http://www.archives.gov/cui>.
- b. Types of CUI: CUI will be safeguarded according to one of the following standards:
 - 1) CUI BASIC: 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.
 - 2) CUI SPECIFIED: 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 that differ from 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.
 - 3) When the laws, regulations, or Government-wide policies governing a specific type of CUI Specified are silent on either a safeguarding or disseminating control, DOT CUI users will apply CUI Basic standards to that aspect of the information's controls.
- c. CUI categories and subcategories.
 - 1) CUI categories and subcategories are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies throughout the executive branch to handle by means of safeguarding or dissemination controls. All unclassified information throughout the executive branch that requires any kind of safeguarding or dissemination control is CUI. 32 CFR part 2002 does not allow any organization to implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Program.

⁴ The NARA CUI Registry is the authoritative source for all markings that may be used to identify CUI.

- 2) DOT CUI users may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI.

11. SAFEGUARDING.

- a. The objective of safeguarding is to protect against the unauthorized disclosure or access of CUI to persons not authorized to view it.
- b. Unless different protection is specified in the CUI Registry for a particular category or subcategory of CUI Specified (see subparagraph c of this section), or other applicable policy, CUI will be protected with at least one physical barrier. It must be stored in a locked office, locked drawer, or locked file cabinet when left unattended. CUI within an unlocked office or cubical space must be secured in a locked desk drawer or locked file cabinet. The safeguarding of digital information within information systems is covered under section 13 of this Order.
- c. Individuals working with CUI Specified categories and subcategories, (e.g., Sensitive Security Information - SSI) must comply with the safeguarding standards outlined in the applicable laws, regulations or Government-wide policies⁵ for those categories and subcategories. If safeguarding measures are not described for that specific category and subcategory, then DOT CUI users will follow the guidance in this Order and apply CUI Basic safeguards, unless this results in treatment that does not accord with the CUI Specified authority. In such cases, DOT CUI users must apply the CUI Specified standards and limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI Specified authority.
- d. Optional Protective Measures: DOT CUI users will be careful not to expose CUI to others who do not have a lawful Government purpose to see it. The Standard Form 901 may be placed on top of documents to conceal contents from casual viewing. DOT CUI users may use cover sheets to protect CUI while they are in the vicinity of the information, but must secure CUI whenever they leave the area.
- e. Controlled Environment: This refers to 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.
- f. Other Precautions:
 - 1) DOT CUI users should reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed;
 - 2) DOT CUI users should keep CUI under their direct control always 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 when outside a controlled environment; and

⁵ Regulations for SSI are contained in 49 CFR part 1520.

- 3) DOT CUI users should protect the confidentiality of CUI that is processed, stored, or transmitted on Federal information systems in accordance with the applicable security requirements and controls established in Federal Information Processing Standard (FIPS) PUB 199, FIPS PUB 200, and NIST SP 800-53.
- g. Care While Traveling: CUI will not be viewed while on a public conveyance or outside controlled spaces where others may be exposed to it. During official travel, CUI should be kept in a locked briefcase, hotel room safe, or in a sealed envelope in the hotel reception safe. 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. For more information see DOT Rules of Behavior applicable to the protection of CUI, e.g., guidance on locking computer screens, ensuring that unauthorized individuals cannot view CUI on computer screens, encrypting CUI attachments to email, storage on portable devices, Wi-Fi, etc.
- h. DOT components may not require more restrictive safeguarding standards than those described in this Order or 32 CFR part 2002 for their contractors or other partners with whom they share CUI.

12. CUI WITHIN INFORMATION SYSTEMS.

- a. IT systems containing CUI must meet NIST's Moderate Confidentiality standard.
- b. All CUI within DOT IT systems must be marked, encrypted, and where available, protected with rights-based-access-controls (rights management). All CUI within DOT IT systems must be entered into the DOT Enterprise Data Inventory and will include metadata specifying the level of CUI that applies.
- c. 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 appropriate 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. DOT CUI users may increase CUI Basic's confidentiality impact level above moderate only within DOT, including contractors operating an information system on behalf of DOT, or by means of agreements between DOT and other agencies. DOT CUI users may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside DOT.
- d. DOT IT systems that process, store, or transmit CUI is of two different types:
 - 1) A Federal IT 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. (See Appendix B, Definitions, for more information about Federal information systems.) Information systems that any entity operates on behalf of DOT are subject to the requirements of the CUI Program as though they are DOT's systems, and DOT may require these systems to meet the same requirements as our own internal systems.

- 2) A non-federal IT system is any information system that does not meet the criteria for a Federal information system. (See Appendix B, Definitions, for more information about nonfederal information systems.) DOT CUI users may not treat non-federal information systems as though they are DOT systems, so non-federal executive branch entities cannot be required to protect these systems in the same manner that DOT might protect its own information systems. Instead, DOT CUI users employing non-federal information systems must follow the requirements of NIST SP 800-171 to protect CUI Basic, unless specific requirements are specified by a law, regulation, or Government-wide policy listed in the CUI Registry for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality.
- e. NIST SP 800-171 revision 2: Contains standards that DOT contract companies and those bound by a DOT agreement must meet if they have CUI on their computer systems.
 - f. <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>
- g. Telework and CUI: For specific policy standards regarding telework, please see the attached link, DOT Telework Policy.

13. DESTRUCTION.

- a. CUI may be destroyed when all the following conditions are met:
 - 1) When DOT CUI users no longer need the information;
 - 2) When records disposition schedules published, or approved by NARA or other applicable laws, regulations, or Government-wide policies no longer require retention; and
 - 3) When any hold preventing destruction, such as a litigation hold, has been lifted from the material to be destroyed (unless normal retention period still applies requiring continued retention after the litigation hold has been lifted).
- b. Destruction of CUI, including in electronic form, must be accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI Specified must be destroyed according to specific directives regarding the information.
- c. In accordance with Appendix A to NIST SP 800-88, Revision 1, SAO should conduct a cost versus risk evaluation of the destruction of paper documents through various means and determine adequate security for CUI Basic can be obtained by the following:
 - 1) Employing cross-cut shredders which produce shreds that are nominally 1 mm x 5 mm (0.04 in. x 0.2 in.) particles or smaller; or

- 2) Pulverizing/disintegrating paper using a disintegrator device with a 2.4 mm (3/32 in.) security screen and recycled as part of a DOT verified multi-step destruction process; or
- 3) Using M-40 procured contracting services with commercial destruction companies that mix the shredded CUI material with the residue of other offices and/or organizations for recycling. These companies may employ machines that produce a larger shred size that renders it suitable for recycling. At DOT and FAA headquarters buildings, CUI may be placed in special document destruction consoles and barrels located throughout the buildings. Other organizations outside of DOT and FAA headquarters should evaluate the destruction vendor's process for collection, protection, transport, and destruction before issuing a contract. Questions regarding the use of commercial destruction companies may be forwarded to the Headquarters DOT (CUIProgram@dot.gov) or FAA Security offices; or
- 4) Using any equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) for classified national security information as contained in:

<https://www.nsa.gov/resources/everyone/media-destruction/assets/files/epl-18-may-2015.pdf>; or

- 5) Using other means only as approved by the Headquarters DOT (CUIProgram@dot.gov) or FAA security offices.
 - 6) DOT may include these destruction standards in contract specifications, but must specify that DOT-specific destruction standards apply only to DOT information that the contractors handle. If the contractor also handles CUI from other agencies, the contractors must abide by (first) the other agency's standards or 32 CFR part 2002.
- d. Destruction of electronic media must be in accordance with the NIST SP 800-88, Revision 1, Guidelines for Media Sanitization: <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>. The sanitization methods contained in Table 5-1 of NIST SP 800-88, Revision 1 are the most common. DOT CUI PM or Designated CUI POC should categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the plans for the media. Then, using information in Table 5-1, decide on the appropriate method for sanitization. The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risks of an unauthorized disclosure of information. Once a decision is made based on factors such as those described in section 4 of NIST SP 800-88, and after applying relevant organizational environmental factors, then the tables in Tables A-1 through A-9 can be used to determine recommended sanitization of specific media.

14. SHARING OF CUI (Accessing and Disseminating).

- a. CUI may only be shared with others who have a bona fide need for access in furtherance of a lawful Government purpose, if such sharing:

- 1) Is in accordance with the laws, regulations, or Government-wide policies that established the CUI category or subcategory;
- 2) Is not restricted by an authorized limited dissemination control established by the NARA CUI EA; and
- 3) Is not otherwise prohibited by law.

For sharing with non-Federal executive branch entities and foreign entities, additional requirements apply, as described in section 15.d of this Order.

- b. 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. If there is significant doubt about whether it is appropriate to use a limited dissemination control, DOT CUI users should consult with and follow the designating agency's policy. If, after consulting the policy, significant doubt remains, the limited dissemination control should not be applied.
- c. Limited Dissemination Controls are markings such as: NOFORN, FEDONLY, FEDCON, NOCON, DL ONLY, REL TO (US, LIST), DISPLAY ONLY. DOT users should consult the CUI Registry for general dissemination principles and authorized use. Using limited dissemination controls to unnecessarily restrict access to CUI is contrary to the goal of the CUI Program and information-sharing.
- d. In addition to the conditions of subparagraph (a) of this Order, the following conditions apply when sharing CUI with a non-Federal executive branch recipient:
 - 1) Must have an official need, is authorized to receive the CUI, and has a basic understanding of proper handling.
 - 2) The component has entered into some type of formal information-sharing agreement with the recipient, whenever feasible. Such agreements must include a requirement for the recipient to comply with EO 13556, 32 CFR 2002, and the CUI Registry.
 - 3) If the mission requires information-sharing, but a formal agreement is not possible, DOT CUI users should strongly encourage the recipient to protect CUI as described in this CUI Program and to have such protections accompany the CUI if the recipient disseminates it further.
 - 4) When entering into information-sharing agreements or arrangements with a foreign entity, DOT CUI users should encourage that entity to protect CUI in accordance with EO 13556, 32 CFR 2002, and the CUI Registry. DOT CUI users are cautioned to use judgment as to what and how much to communicate, keeping in mind the goal of safeguarding CUI. If such agreements or arrangements include safeguarding or dissemination controls on unclassified information, DOT CUI users may only use the

CUI markings and controls. They may not use other markings or protective measures.

- 5) Information-sharing agreements that have been made prior to establishment of the CUI Program should be modified so they do not conflict with CUI Program requirements when feasible.
 - 6) Information-sharing agreements with non-Federal executive branch entities must include provisions that CUI be handled in accordance with the CUI Program; misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies; and the non-Federal executive branch entity must report any non-compliance with handling requirements to DOT via protected communications described in paragraph 14 b of this Order. When DOT is not the designating agency, DOT CUI users must notify the designating agency.
 - 7) DOT components need not enter a written agreement when they share CUI with the following entities: (i) Congress, including any committee, subcommittee, joint committee, joint subcommittee, or office thereof; (ii) a court of competent jurisdiction, or any individual or entity when directed by an order of a court of competent jurisdiction or a Federal Administrative Law Judge (ALJ) appointed under 5 U.S.C. § 3501; (iii) the Comptroller General, in the course of performing duties of the Government Accountability Office; or (iv) individuals or entities, when the agency releases information to them pursuant to a Freedom of Information Act (FOIA) or Privacy Act request.
- e. CUI Basic may be disseminated to persons and entities meeting the access requirements of this section. Further dissemination of CUI Basic may not be restricted without approval by NARA's CUI EA, who will publish any exceptions in the CUI Registry. Authorized recipients of CUI Basic may further disseminate the information to individuals or entities meeting and complying with the requirements of the CUI Program.
 - f. CUI Specified may only be disseminated to persons and entities as authorized in the underlying authority contained in the CUI Registry that established that category or subcategory of CUI Specified. Further dissemination of CUI Specified may be made by authorized recipients if not restricted by the underlying authority. SSI may be disseminated in accordance with 49 CFR part 1520. In the absence of specific dissemination restrictions in the authorizing law, regulation, or Government-wide policy for the relevant CUI category or subcategory, DOT components may disseminate CUI Specified as they would CUI Basic.

15. DECONTROL OF CUI.

- a. When control is no longer needed, DOT CUI users 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 authority.

- b. CUI may be decontrolled automatically upon the occurrence of one of the conditions below, or through an affirmative decision by the designator, i.e., the holder of the material:
 - 1) When laws, regulations, or Government-wide policies no longer require its control as CUI and the authorized holder⁶ has the appropriate authority to affect the decontrol under the authorizing law, regulation, or Government-wide policy;
 - 2) When DOT decides to release the CUI to the public by making an affirmative, proactive disclosure from the holder;
 - 3) When DOT discloses it in accordance with an applicable information access statutes, such as the Freedom of Information Act (FOIA), provided that DOT incorporates such disclosures into its public release processes; or
 - 4) When a pre-determined event or date occurs, as described in 32 CFR 2002.20 (g), unless law, regulation, or Government-wide policy requires additional coordination first.
- c. A designating or original creating agency may also decontrol CUI:
 - 1) In response to a request from an authorized holder to decontrol it; or
 - 2) Concurrently with any declassification action under EO 13526, Classified National Security Information or any predecessor or successor order, if the information also appropriately qualifies for decontrol as CUI.
- d. DOT and its components may designate in its CUI policies which personnel it authorizes to decontrol CUI, consistent with law, regulations, and Government-wide policy.
- e. Decontrolling CUI removes the requirement to handle the information under the CUI Program, but does not constitute authorization for public release. When considering public release, DOT Order 1351.34, DOT Data and Information Management Policy, applies.
- f. DOT CUI users 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. DOT CUI users do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.
 - 1) For relatively short documents, all CUI markings within a decontrolled CUI document must be removed or struck through. For large documents, DOT CUI users 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

⁶ An authorized holder is any person who lawfully possesses CUI. Because DOT CUI users and their affiliated parties per this order will encounter CUI while performing work, they are authorized holders.

CUI. They must also mark or stamp a statement on the first page or cover page that the CUI markings are no longer applicable.

- 2) If DOT CUI users use decontrolled CUI in a newly created document, they must remove all CUI markings for the decontrolled information.
- 3) Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and DOT (or other agency) policies on the public release of information.
- 4) Authorized holders may request that the designating agency decontrol CUI that they believe should be decontrolled.
- 5) If an authorized holder publicly releases CUI in accordance with the designating agency's authorized procedures, the release constitutes decontrol of the information. CUI markings must be cancelled prior to public release as described in subparagraph 16.f(1) of this section.
- 6) Unauthorized disclosure of CUI does not constitute decontrol.
- 7) DOT CUI users should not decontrol CUI in an attempt to conceal, or to otherwise circumvent accountability for, an identified unauthorized disclosure.
- 8) When laws, regulations, or Government-wide policies require specific decontrol procedures, CUI users should follow such requirements.
- 9) Records Management Note: The Archivist of the United States may decontrol a record transferred to the National Archives in accordance with 32 CFR 2002.34, absent a specific agreement to the contrary with the designating agency. 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.

16. MARKING OF CUI.

- a. CUI users may mark information as CUI based upon the categories/subcategories that are listed in the CUI Registry. CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls. Such markings should appear on CUI datasets registered in DOT Enterprise Data Inventory.
- b. Information may not be marked as CUI:
 - 1) To conceal violations of law, inefficiency, negligence, ineptitude, or administrative error;
 - 2) To prevent embarrassment to the U.S. Government, any U.S. official, organization, agency, or any partner;

- 3) To improperly or unlawfully interfere with competition;
 - 4) To prevent or delay the release of information that does not require such protection;
or
 - 5) If the CUI is required by statute or EO to be made available to the public or if it has been released to the public under proper authority.
- c. DOT CUI users must follow 32 CFR part 2002, the CUI Registry, and the NARA CUI Marking Guide for the marking of CUI on paper and electronic documents except where an appropriate waiver has been granted. Appendix C of this Order augments the information in the marking guide. The following markings apply:
- 1) CUI Banner Markings.
 - a) Designators of CUI must mark all CUI with a CUI banner marking. The content of the CUI banner marking must be inclusive of all CUI within the document and must be the same on each page. Banner markings must appear at the top of each page of any document that contains CUI, including email transmissions. Banner markings may include up to three elements:
 - i. The CUI control marking. The CUI control marking may consist of either the word "CONTROLLED" or the acronym "CUI," at the designator's discretion. The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of CUI Basic categories or subcategories.
 - ii. If portion markings (see section 19 of this Order) are used, all pages must display CUI portion markings. Computer screens must also display a CUI banner on each screen that contains CUI category or subcategory markings.
 - iii. If a part of a document contains CUI Specified, then the applicable category or subcategory marking must appear in the banner, preceded by a "SP-" to indicate the specified nature of the category or subcategory (e.g., CUI//SP-PCII). The CUI control marking and any category or subcategory markings are separated by a double forward slash (i.e., //). When including multiple categories or subcategories in the banner they must be alphabetized, with specified categories (or subcategories) appearing before any basic categories (or subcategories). Multiple categories or subcategories in a banner line must be separated by a single forward slash (i.e., /).
 - 2) Other Markings or Statements on the Document.
 - a) Specific marking, disseminating, informing, distribution limitation, or warning statements that are required by underlying authorities must be additionally placed on the document, but not within the banner or portion markings, e.g., SSI protective marking(s) and distribution limitation statement in accordance with 49

CFR 15.13 and 1520.13. Questions regarding the placement of such markings may be referred to DOT CUI PM at (CUIProgram@dot.gov).

- b) Identification of the designator (i.e., CUI designation indicator). All documents containing CUI must identify the person or office that designated the CUI (the designator) in that document on the first page or cover. This should include DOT component and office within that component, e.g., letterhead and/or FROM line; or by adding a “Controlled by” line at the bottom of the first page (for example, “Controlled by: John Doe, M-40, OST, DOT”). See Appendix D of this Order.
- c) CUI decontrolling indicators. Where feasible a specific decontrolling date or event will be included with all CUI. This may be accomplished in a manner that makes the decontrolling schedule clear. See Appendix C of this Order.
- d) When used, decontrolling indicators must use the format: “Decontrol On (YYYYMMDD):” or “Decontrol On (specific event).” See Appendix C of this Order.
 - i. Decontrol is presumed at midnight local time on the date indicated. If CUI is marked with a decontrol date, no further review by, or communication with, the designator is required at the time when CUI is decontrolled.
 - ii. If using a specific event after which the CUI is considered decontrolled:
 - A. The event must be foreseeable and verifiable by any authorized holder – not based on or requiring special access or knowledge (e.g., the day of a press release, or after a dignitary has made a visit, or after a special operation has been completed); and
 - B. A point of contact and preferred method of contact must be included in the decontrol indicator to allow verification that a specified event has occurred, whenever possible.
- d. If DOT CUI users encounter an incorrectly or unmarked document, email, or electronic screen containing information that qualifies as CUI, they should notify either the disseminating entity or the designating agency of the error. Also, notification to the OA CUI POC or the CUI PM may be appropriate.
- 1) Due to the quantity of legacy-marked information within DOT, the burden that would result from re-marking all legacy information makes such an effort impractical. Instead, per 32 CFR 2002.38, the following applies:
 - a) Information containing legacy markings (e.g., FOUO or SBU) need not be re-marked if it remains within DOT. DOT CUI users should make users aware of the information's CUI status using an alternate marking method that is clear (for example, through user access agreements, a computer system digital splash screen [e.g., alerts that flash up when accessing the system], or signs in storage areas or on containers).

- b) Any time legacy information is used to produce new material, or if the legacy information qualifies as CUI and is sent outside DOT, the legacy markings must be removed or struck through, and the appropriate CUI markings applied to this requirement and cannot be waived.
- 2) The lack of a CUI marking on information that qualifies as CUI does not exempt the holder from abiding by applicable handling requirements as described in this Order and its references.

17. PORTION MARKING.

- a. Optional portion markings are a means to provide information about the sensitivity of a section of text, paragraph, bullet, picture, chart, etc. They consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title.
- b. Portion marking is not required, but it is permitted and encouraged to facilitate information-sharing and proper handling, and to assist FOIA reviewers in identifying the sensitive information within a large document that may be primarily non-sensitive. See Appendix C of this Order for the description and use of portion markings.

18. COMMINGLING CUI MARKINGS WITH CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI).

- a. If CUI documents also contain CNSI, the decontrolling provisions of the CUI Program apply only to the CUI portions. In addition, DOT CUI users will adjust the CUI marking scheme to:
 - 1) Portion mark all CUI to ensure that CUI portions can be distinguished from portions containing classified and uncontrolled unclassified information;
 - 2) Include the CUI control marking (“CUI”) in the overall marking banner;
 - 3) Include CUI Specified category, subcategory markings in the overall banner marking directly after the CUI control marking; and
 - 4) If law, regulation or Government-wide policy requires specific markings. disseminating, informing, distribution limitation, or warnings statements, DOT organizations must use those indicators as those authorities require or permit.
- b. The CUI Registry and the NARA CUI Marking Guide contains additional specific guidance on marking CUI when commingled with CNSI.

19. COMMINGLING RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD) WITH CUI.

- a. Restricted Data (RD) and Formerly Restricted Data (FRD) are categories of classified information concerning nuclear weapons design and utilization.

- b. To the extent possible, DOT CUI users should avoid commingling RD or FRD with CUI in the same document. When it is not practicable to avoid such commingling, DOT CUI users should follow the marking requirements of the CUI Program as well as the marking requirements for RD and FRD contained in 10 CFR part 1045, Nuclear Classification and Declassification.
- c. DOT CUI users must follow the marking requirements of 10 CFR part 1045 when extracting an RD or FRD portion for use in a new document.
- d. DOT CUI users must follow the requirements of the CUI Program as described in this Order if extracting a CUI portion for use in a new document.
- e. The lack of declassification instructions for RD or FRD portions does not eliminate the requirement to process commingled documents for declassification in accordance with the Atomic Energy Act, or 10 CFR part 1045.

20. TRANSMITTING/TRANSPORTING CUI.

- a. Standard voice telephony is acceptable for the discussion of CUI, but information transmitted via email and websites should be encrypted, password-protected, or placed on a restricted site unless a risk-based tailoring decision has been made to compensate for encryption.
- b. CUI may be sent through the United States Postal Service (USPS) or any commercial delivery service that offers in-transit automated tracking and accountability tools provided the CUI is shipped using these tools.
- c. CUI may also be sent through interoffice or interagency mail systems.
- d. DOT CUI users must address packages that contain CUI for delivery **only** to a specific recipient, not to an office or organization. Do not apply CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI.

21. TRANSMITTAL DOCUMENT MARKING REQUIREMENTS.

- a. When a transmittal document accompanies CUI, the transmittal document must include a CUI marking (“CONTROLLED” or “CUI”) on its face. This serves to notify the recipient about the sensitivity of the document beneath the cover letter.
- b. The transmittal document must also conspicuously include the following or similar instructions, as appropriate:
 - 1) “When enclosure is removed, this document is Uncontrolled Unclassified Information”, or
 - 2) “When enclosure is removed, this document is (control level); upon removal, this document does not contain CUI”.

22. REPRODUCTION OF CUI.

- a. CUI may be reproduced (e.g., copy, scan, print, electronically duplicate) in furtherance of a lawful Government purpose; and
- b. When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, DOT CUI users must ensure that the equipment does not retain data (i.e. volatile memory) or they must otherwise sanitize in accordance with NIST SP 800-53 to include electronically duplicated information.
- c. The Multifunction printers at Headquarters DOT and FAA facilities are protected against the inadvertent release of CUI to unauthorized personnel by login procedures and meet this requirement. CUI users in other locations should check with their equipment provider or the appropriate information technology office to determine whether the equipment retains information for any amount of time after it is processed, and how to clear the equipment of the information if necessary. This information should be posted on any equipment that retains data.

23. WORKING PAPERS.

- a. Working papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.
- b. 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 them. Working papers must be protected as any other CUI regardless of their future disposal/disposition. When no longer needed, working papers must be destroyed in accordance with section 15 of this Order.

24. USING SUPPLEMENTAL ADMINISTRATIVE MARKINGS WITH CUI.

- a. Supplemental administrative markings (e.g., “Pre-decisional,” “Deliberative,” “Draft, Provisional – In Work”) may be used with CUI. The NARA CUI MARKING GUIDE provides examples of supplemental administrative markings.
- b. 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 non-final status of documents under development to avoid confusion and maintain the integrity of a decision-making process. Additionally, their purpose is to provide additional information to recipients about privileges or other protections afforded the document. For example, in the case of drafts, the supplemental markings may advise the recipient of the non-final status of a document under development to avoid confusion and maintain the integrity of the decision-making process, or to advise the recipient that the document includes attorney-client privileged information.
- c. 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.) Supplemental markings may not appear in the CUI banners; nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings.

- d. Supplemental administrative markings must not duplicate any CUI marking described in the CUI Registry.
25. UNMARKED CUI. Unmarked information that qualifies as CUI must be marked and treated appropriately as described in this CUI Program. Legacy information not marked because of the exception allowed in paragraph 17.d(1) of this Order must still be handled (e.g., protected, stored, destroyed) in accordance with CUI requirements.
26. CUI SELF-INSPECTION PROGRAM. In accordance with 32 CFR 2002.8(b)(4), DOT will implement a Self-Inspection Program as follows:
- a. The CUI PM, under the authority of the CUI SAO, must provide technical guidance, training, and materials to ensure that DOT components conduct reviews and assessments of their CUI Programs at least annually, and report the results to the CUI PM as required by the NARA CUI EA;
 - b. Following training of the designated CUI POCs of each DOT component, DOT components must conduct annual self-inspections of their CUI Program and report the results on a schedule determined by the CUI SAO. DOT self-inspection must incorporate CUI in the possession of contractor personnel through on-site inspections at DOT facilities, or by examining results of self-inspections conducted by the contractor company or by another Federal agency;
 - c. Following guidance and inspection materials received from the CUI PM, self-inspection methods, reviews, and assessments will serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;
 - d. The CUI PM must provide to DOT components formats for documenting self-inspections and recording findings, and provide advice for resolving deficiencies and taking corrective actions; and results from DOT-wide self-inspections will be used to inform updates to the CUI training provided to DOT CUI users.

27. EDUCATION AND TRAINING.

- a. Every DOT employee, contract employee, and affiliated person who may encounter CUI in their work (CUI users) will complete initial CUI training prior to access or handling CUI. Refresher training will be required every two years after the initial training. Individual training will be computer-based, classroom, webinar, pre-recorded video, or desk-side (training that involves actual site visit and office/individual training), depending on the circumstances. Newly assigned personnel must complete initial training within three months of on-boarding. These personnel will not be required to complete additional annual training within their first year.
- b. Personnel who have access to CUI receive training on designating CUI, relevant CUI categories and subcategories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures. Contact M-40 CUI PM for specific training elements that must be conveyed in initial and refresher training.
- c. Continuing periodic education must be provided using brochures, posters, DOT web or SharePoint pages, or other methods.

28. CUI COVER SHEETS.

- a. DOT CUI users may use cover sheets for non-electronic CUI, but their use is optional. Optional (OP) Form 901, OP Form 902, and OP Form 903 were rescinded on December 14, 2018 but are authorized until DOT has exhausted any supplies. The current Standard Form 901 may be downloaded from:

<https://www.gsa.gov/cdnstatic/SF901-18a.pdf?forceDownload=1>
- b. DOT CUI users may use cover sheets to identify CUI and to serve as a shield to protect the attached CUI from unintentional disclosure.

29. TRANSFERRING RECORDS TO NARA.

- a. When feasible, records containing CUI will be decontrolled prior to transferring to NARA.
- b. If records cannot be decontrolled before transferring to NARA, the following procedures will be followed:
 - 1) Indicate on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) that the records should continue to be controlled as CUI (subject to NARA's regulations on transfer, public availability, and access; see 36 CFR parts 1235, 1250, and 1256); and

- 2) For hard copy transfer, do not place a CUI marking on the outside of the container or envelope. Double-wrapping is not required, but if used, only the interior envelope should be marked as “Controlled” or “CUI.”
- c. If the status as CUI is not indicated on the TR, NARA may assume the information was decontrolled prior to transfer, regardless of any CUI markings on the actual records. Therefore, DOT CUI users must clearly indicate the CUI status (whether it is still active or decontrolled) prior to transfer.

30. WAIVERS OF CUI REQUIREMENTS.

- a. In exigent circumstances,⁷ the CUI SAO may waive certain requirements of the CUI Program for any CUI while it is within DOT’s possession or control, unless specifically prohibited by applicable laws, regulations, or Government-wide policies. In normal circumstances, when an agency designates information as CUI but determines that marking it as CUI is excessively burdensome, an agency’s CUI SAO may approve waivers of all or some of the CUI marking requirements while that CUI remains within agency control.
- b. Exigent circumstances waivers may apply when DOT shares the information with other Federal agencies or non-Federal entities. In such cases, recipients must be made aware of the CUI status of any disseminated information. When the exigent circumstances requiring the waiver end, the waiver will be terminated and all requirements for CUI subject to the waiver must be reinstated without delay.
- c. Per 32 CFR 2002.38(e), the CUI SAO will:
 - 1) Retain a record of each waiver;
 - 2) Include a description of all current waivers and waivers issued during the preceding year in the annual report to the CUI EA, along with the rationale for each waiver and the alternate steps the agency takes to ensure sufficient protection of CUI; and
 - 3) Notify authorized recipients and the public of these waivers through means such as notices or web sites.

31. CUI AND DISCLOSURE STATUTES.

- a. General Policy: The fact that information is designated as CUI does not prohibit its disclosure if the disclosure is made according to criteria set out in a governing law.
- b. CUI and 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

⁷ Exigent circumstances exist when following proper procedures would cause an unacceptable delay due to the urgency of the situation; the SAO may waive certain CUI requirements within DOT only.

designated or marked as CUI. There may be circumstances in which records marked CUI are disclosed to an individual or entity, including through a FOIA response, but such disclosure does not always constitute public release as defined by the CUI Program. Although disclosed via a FOIA response, the CUI may still need to be controlled while DOT continues to hold the information, despite the disclosure, unless it is otherwise decontrolled. DOT FOIA disclosures always results in public release unless the CUI does not otherwise have another legal requirement for its continued control.

- c. 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 applicable affect whistleblower legal protections provided by law, regulation, EO or directive.

32. CUI AND THE PRIVACY ACT. Records in a Privacy Act system of records containing Personally Identifiable Information (PII) must be marked as CUI Basic in accordance with the CUI Registry. Information contained in Privacy Act systems of records may also be subject to controls under other CUI categories or subcategories and may need to be marked as CUI Specified for that reason. In addition, when determining whether certain information must be protected under the Privacy Act or whether the Privacy Act allows the release of information to the subject of a record, the decision to release must be based upon the individual's right of access under the Privacy Act and the FOIA, regardless of whether the information is designated or marked as CUI.

33. CUI AND THE ADMINISTRATIVE PROCEDURE ACT (APA). Nothing in the CUI Program regulations alters the Administrative Procedure Act (APA) or the powers of Administrative Law Judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor does the CUI Program impose requirements concerning the way ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

34. CHALLENGES TO DESIGNATION OF INFORMATION AS CUI.

- a. 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 CUI PM, CUI Coordinator or the disseminating agency. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency. Thus, if DOT receives a challenge from a CUI recipient, and DOT is not the designating agency for the CUI, DOT must notify the designating agency. Challenges may be made anonymously; and challengers cannot be subject to retribution for bringing such challenges.
- b. If the information at issue is involved in Government litigation, or the challenge to its designation or marking as CUI arises as of the litigation, the issue of whether the challenger may access the information will be addressed via the litigation process instead of by DOT SAO. Challengers should nonetheless notify DOT SAO of the issue through the agency process described below, and include its litigation connection. Internal

coordination between the Office of the General Counsel and M-40 is encouraged. OAs are encouraged to notify their Chief Counsel, but are not required to do so prior to notifying DOT OGC and M-40 CUI SAO.

- c. If any DOT organization receives a challenge, the CUI POC for that organization must work with the CUI PM to take the following measures:
 - 1) Acknowledge receipt of the challenge;
 - 2) Provide an expected timetable for response to the challenger;
 - 3) Review the merits of the challenge with a subject matter expert and offer an opportunity to the challenger to define a rationale for belief that the CUI in question is inappropriately designated;
 - 4) Notify the challenger of DOT's decision; and
 - 5) Provides contact information of the official making the decision in this matter.
- d. Until the challenge is resolved, the challenged CUI should continue to be safeguarded and disseminated at the control level indicated in the markings.
- e. If a challenging party disagrees with DOT's response to a challenge, that party may use the Dispute Resolution procedures described in 32 CFR § 2002.52.

35. MISUSE OF CUI AND INCIDENT REPORTING.

- a. Suspected or confirmed CUI misuse whether intentional or accidental, must be reported to the organization's CUI POC within 72 hours, e.g., unauthorized disclosure. The CUI POC will 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.
- b. If the investigation determines an employee has misused CUI, the CUI PM, in conjunction with the CUI SAO, employee manager, and other management officials, will determine if sanctions under section 37 of this Order are appropriate, or if other corrective action may be warranted (e.g., emphasis on training). Misuse of CUI that has been designated by another Executive Department or agency will be reported to that agency by the CUI PM.
- c. Reporting mechanisms such as office phone notification waterfall lists and dedicated email addresses for areas of responsibility is highly recommended for the timely reporting process.
- d. Coordination by the CUI POC is imperative for mitigation measures as needed and providing status reports until mitigation is complete.

36. SANCTIONS FOR MISUSE OF CUI.

- a. Depending upon the severity of the misuse and the offender's history of prior incidents, the CUI SAO may recommend to the Operating Administrator whether administrative actions should be applied to the offender.
- b. Any sanctions or administrative actions specifically established by laws, regulations, or Government-wide policies governing certain categories or subcategories of CUI will be considered and applied per requirements.

37. SENSITIVE SECURITY INFORMATION (SSI).

- a. SSI is a subcategory of CUI Specified that is governed by the regulations of Transportation Security Administration (49 CFR 1520). Any questions or concerns regarding SSI must be directed to the Office of Intelligence, Security and Emergency Response at <mailto:SSI@dot.gov>.
- b. In the case of conflict, the provisions of parts 1520 override the CUI Program policies, except that the word CONTROLLED or the acronym CUI will appear as the first item on the security banners of documents. Refer to the CUI Marking Guide for marking format. Authorized holders of SSI must comply with both parts 2002 and part 1520. DOT CUI users must follow the provisions and any implementing directives from DOT (S-60) and TSA regarding SSI.
- c. SSI will be marked as CUI Specified because its subject has specific provisions regarding its access, distribution and warning statements.

38. RAILROAD SAFETY ANALYSIS RECORDS (RAIL).

- a. RAIL is a subcategory of CUI administered by DOT (49 U.S.C. § 20118) related to the establishment, implementation, or modification of a railroad safety risk reduction program or pilot program, if the record is: (1) Supplied to the Secretary of Transportation pursuant to that safety risk reduction program or pilot program; or (2) made available for inspection and copying by an officer, employee, or agent of the Secretary pursuant to that safety risk reduction program or pilot program.
- b. RAIL is CUI Basic because it only has limitations regarding its disclosure, and no provisions regarding safeguarding or handling. The term "RAIL" is optional whether to include in any CUI markings.

39. PUBLICATION OF CUI. Publication of CUI or its posting on public web sites or social media is prohibited unless the CUI has been properly decontrolled in accordance with section 16 of this Order.

40. REQUESTING NEW CATEGORIES OR SUBCATEGORIES OF CUI.

- a. DOT CUI users who encounter sensitive information that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding

dissemination controls that is not described in the CUI Registry, may recommend that a new CUI category or subcategory be entered the Registry.

- b. DOT CUI should submit their recommendation through the DOT Office of the General Counsel for OST personnel, or through the relevant OA Chief Counsel Office and the CUI PM. The request should include:
 - 1) A description of the information to be marked as CUI;
 - 2) The law(s) regulation(s), or government-wide policy(-ices) that require or permit the agency to handle the information using safeguarding or dissemination controls;
 - 3) If a subcategory, the name of the category applying to the information; and
 - 4) A suggested name, along with a suggested acronym for the category or subcategory.
- c. The CUI PM, in coordination with the Office of the General Counsel, will review the recommendation and, if appropriate, submit the recommendation to the CUI EA.

Phillip McNamara
Assistant Secretary for Administration

APPENDIX A

DOT Order 1650.5, Controlled Unclassified Information

ACRONYMS

ALJ – Administrative Law Judge

CNSI – Classified National Security Information

COR – Contractor Officer Representative

CUI – Controlled Unclassified Information

DL ONLY – Dissemination List Controlled

EA – Executive Agent

EO – Executive Order

FAA – Federal Aviation Administration

FOIA – Freedom of Information Act

FEDONLY – Federal Employees Only

FEDCON – Federal Employees and Contractors Only

FIPS – Federal Information Processing Standards

FOUO – For Official Use Only

FRD – Formerly Restricted Data

GSA – General Services Administration

ISOO – Information Security Oversight Office at the National Archives and Records Administration

IT – Information Technology

MOA – Memorandum of Agreement

NARA – National Archives and Records Administration (the CUI Executive Agent)

NOCON – No Dissemination to Contractors

NOFORN – No Foreign Dissemination

OA – Operating Administration

OMB – Office of Management and Budget within the Executive Office of the President

PM – Program Manager

POC – Point of Contact

RD – Restricted Data

REL TO – Authorized for Release to Certain Nationals Only

SAO – The designated Senior Agency Official

SBU – Sensitive But Unclassified

SME – Subject Matter Expert

SSI – Sensitive Security Information

TR – Transfer Request in NARA’s Electronic Records Archives (ERA)

USPS – United States Postal Service

APPENDIX B

DOT Order 1650.5, Controlled Unclassified Information

DEFINITIONS

The following terms are associated with the CUI Program. Additional definitions may be found in 32 CFR Part 2002.4.

Agency Head – Individual or body of individuals whom legal authority of the agency is vested by statute. An agency head may retain full undelegated review authority, or designate a Senior Official who will report directly to the head of the agency.

Affiliated person – Consultants, researchers, organizations, and State, local, Tribal, and private sector partners with whom DOT may share CUI. Individuals who have no contact with CUI are excluded from this definition.

Authorized holder – Any person who lawfully possesses CUI and further is an individual, agency, organization, or group of users that is permitted to designate or handle CUI. Because almost all DOT CUI users and their affiliated OA's will encounter CUI while performing work, they are authorized holders. (See also Lawful Government Purpose.)

Banner – A distinctive marking across the top and/or bottom of a document (paper or electronic) that provides information or a caution about the contents of the document.

Controlled Unclassified Information (CUI) – Information the Government creates or possesses that a law, regulation, or Government-wide policy requires or specifically permits an agency to handle by means of safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

CUI Basic – 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 CUI Program's 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 ones do not cover the involved CUI.

CUI Categories and Subcategories – Those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the CUI Registry. The controls for any CUI Basic categories and any CUI Basic subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic ones and from each other. A CUI category may be Specified, while some or all its subcategories may not be, and vice versa. If dealing with CUI that falls into a CUI Specified category or subcategory, review the controls for that category or subcategory on the CUI Registry.

CUI Category or Subcategory Markings – The markings approved by the CUI EA for the categories and subcategories listed in the CUI Registry.

CUI Executive Agent (EA) – The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

CUI Program – The executive branch-wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry. This Order implements the CUI Program within DOT.

CUI Program Manager (CUI PM) – The DOT official, designated by the CUI SAO, to serve as the official representative to the NARA CUI EA on DOT’s day-to-day CUI Program operations, both within DOT and in interagency contexts.

CUI Point of Contact (CUI POC) - DOT’s employee appointed by a DOT Component who is assigned specific duties to assist the CUI Program Manager in implementing and managing the CUI Program.

CUI Registry – The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. The CUI Registry may be easily located by entering “CUI Registry” in any web browser. The full URL is <https://www.archives.gov/cui/registry/category-list>.

UI Specified – The subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from 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 the controls for CUI Specified information and does not for CUI Basic information.

Decontrol – The removal of information from the protection of the CUI Program.

Designating Agency or Organization – Designating agency is the executive branch agency that designates or approves the designation of a specific item of information as CUI.

Designators of CUI – Employees, contractors, or other DOT affiliated persons who mark information as CUI based upon the Categories/Subcategories that are listed in the CUI Registry. “Designator” may also refer to the organization that designates information as CUI.

Disseminating Agency or Organization – Any organization that distributes CUI by transmitting it to an authorized holder or by placing onto accessible media such as SharePoint, a web site, or electronic bulletin board.

DOT Component: Any DOT Operating Administration, the Office of Inspector General, or Secretarial Office.

DOT CUI Users –For the purposes of this Order, DOT CUI users include every DOT employee, contract employee, and affiliated person who may encounter CUI in their work. DOT employees, contractors (on-site and off-site), and affiliated parties such as consultants, researchers, organizations, students, interns, individuals detailed or assigned to DOT and State, Local, Tribal, and private sector partners with whom DOT may share CUI.

Federal Information System – Federal information system is an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. 44 U.S.C. § 3554(a)(1)(A)(ii).

Formerly Restricted Data – See Restricted Data.

Lawful Government Purpose – 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 Markings – Markings that were in use before the advent of the CUI Program for sensitive but unclassified information, e.g., For Official Use Only (FOUO) and Sensitive But Unclassified (SBU).

Non-federal Information System – Any information system that does not meet the criteria for a Federal information system. When a non-executive branch entity receives Federal information only incidental to providing a service or product to the Government other than processing services, its information systems are not considered Federal information systems. NIST SP 800-171 defines the requirements necessary to protect CUI Basic on nonfederal information systems in accordance with the requirements of the CUI Program.

Protected Communications – Means of transmission of information that is reasonably expected to be available only to authorized personnel.

Restricted Data (RD) and Formerly Restricted Data (FRD) – Categories of classified information concerning nuclear weapons design and utilization. These categories of information are classified under the Atomic Energy Act, and defined in 10 CFR Part 1045, Nuclear Classification and Declassification. Despite the potentially misleading nature of the phrase

“Formerly Restricted Data,” documents with this marking remain classified and must be protected.

Senior Agency Official (SAO) – The senior DOT official responsible for oversight of DOT’s CUI Program implementation, compliance, and management.

Sensitive Security Information (SSI) – Information that, if publicly released, would be detrimental to transportation security, as defined by Federal Regulation 49 C.F.R. Part 1520. As persons receiving SSI to carry out responsibilities related to transportation security, TSA stakeholders and non-DHS government employees and contractors, are considered “covered persons” under the SSI regulation and have special obligations to protect this information from unauthorized disclosure.

Uncontrolled unclassified information – Information that neither EO 13556 nor classified information authorities 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 – The law, regulation, or Government-wide policy that is the basis for designating information as CUI.

Volatile memory – Computer storage that only maintain its data or memory while the device is powered i.e. random access memory (RAM) of personal devices.

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

APPENDIX C

DOT Order 1650.5, Controlled Unclassified Information

PORTION MARKINGS

Portion markings are a means to provide information about the sensitivity of a section of text, paragraph, bullet, picture, chart, etc. They consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title. For CUI, only portion markings approved by the CUI EA and listed in the CUI Registry may be applied. The NARA CUI MARKING GUIDE provides examples of the use of portion markings.

- a. CUI portion markings consist of the following elements:
 - (1) The CUI control marking, which must be the acronym “CUI”;
 - (2) CUI category/subcategory portion markings (required for CUI Specified; optional for CUI Basic); and
 - (3) CUI limited dissemination control portion markings (if required).
- b. When using portion markings:
 - (1) Indicate CUI portions by placing the required portion marking for each portion inside parentheses, immediately before the portion to which it applies (*e.g.*, “(CUI)” or “(CUI/LEI/NF).”
 - (2) If any of a document is portion-marked, then the entire document must contain portion markings. Non-sensitive information contained in that document must then be identified as “Uncontrolled Unclassified,” with the mark “(U)” immediately preceding the portion to which it applies. Additionally, the top banner marking must appear on every page. As an optional best practice, the CUI Banner Marking may be placed at the bottom of the document as well. [§ 2002.20(f)(4)(ii)]
- c. In cases where portions consist of several segments, such as paragraphs, sub-paragraphs, bullets, and sub-bullets, and the control level is the same throughout, DOT CUI users may place a single portion marking at the beginning of the primary paragraph or bullet. However, if the portion includes different CUI categories or subcategories, DOT CUI users must portion mark all segments separately to avoid improper control of any one segment.
- d. Each portion marking must reflect the control level of that individual portion and not any other portions. If the information contained in a sub-paragraph or sub-bullet is a different CUI category or subcategory from its parent paragraph or parent bullet, this does not make the parent paragraph or parent bullet controlled at that same level.

Example of a portion-marked document

Refer to 32 CFR 2002.20(f) and the CUI Registry for more detailed instructions regarding portion markings. Questions regarding portion markings may be addressed to the organization's CUI Point of Contact or the CUI Program Manager.

Any page that contains CUI must also have a banner. Top banner is required, bottom banner is optional but encouraged.

Even if the first page does not contain sensitive information, it must still have the banner if other pages within the document contain CUI.

Note that the SSI Warning Statement does not appear on this page...there was not sufficient room on the sample to include it:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR part 1520, except with the written permission of the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR part 1520.

CUI or CONTROLLED//SP-SPECIFIED-SSI



U.S. Department of
Transportation
Office of the Secretary
of Transportation

Memorandum

Subject: (U) Portion Marking of CUI Specified Content **Date:** November 14, 2017

From: DOT CUI Program Manager **Reply to:**
Attn. of

To: All DOT Personnel

(U) This sample shows how portion markings may be applied to documents. Portion marking are not required, but are an optional method of informing the reader where any sensitive information is located. If portion markings are used, the all non-sensitive paragraphs must be marked with a "(U)," including the subject line.

(CUI) This is how a paragraph that contains Controlled Unclassified Information should be marked.

(CUI//SP-SSI) This is how a paragraph that contains Sensitive Security Information should be marked. The "SP" indicate the presence of CUI Specified and the document must be handled different than CUI Basic.

(U) **Banner marking:** The word CONTROLLED or the acronym CUI in upper case bold type must appear at the top every page of the document. Then add a double forward slash (/), the acronym SP (for specified), a hyphen, and the applicable subcategory (in this case, Sensitive Security Information, or the acronym SSI). If there is no room at the top, the banner must appear distinctively elsewhere on the page. For large documents, the banner may be placed only on the pages where CUI appears. A banner may also be placed at the bottom of the page, if desired.

(U) **Identification of the Designator:** This can be done in either of two ways:

- a. If the Designator can be identified from the letterhead, that is sufficient.
- b. If there is no letterhead identification, then the Designator's information must appear elsewhere on the page.

(U) **Decontrol Indicator:** Where feasible, include a specific decontrolling date or event with all CUI. If a date or event cannot be foreseen, then do not include the decontrol indicator.

Controlled by: DOT CUI Program Manager, Office of the Secretary
Decontrol on: (If possible, enter a date or event, e.g., "After the event has been completed or cancelled.")

Paragraph markings shown on this document are for illustration only. There is no sensitive information contained in this document.

CUI or CONTROLLED//SP-SPECIFIED-SSI

APPENDIX D

DOT Order 1650.5, Controlled Unclassified Information

Useful Links

CUI Marking Handbook:

<https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf>

CUI Registry:

<https://www.archives.gov/cui/registry/category-list>

DOT CUI Program:

CUIProgram@dot.gov

E.O. 13556, Controlled Unclassified Information:

<https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information>

NSA/CSS Evaluated Products List:

<https://www.nsa.gov/resources/everyone/media-destruction/assets/files/epl-18-may-2015.pdf>

NIST Publications:

<http://csrc.nist.gov/publications>

Code of Federal Regulations:

<http://www.ecfr.gov/cgi-bin/text-idx?tpl=%2Findex.tpl>

Executive Orders:

<https://www.federalregister.gov/executive-orders>

CUI Coversheet:

<https://www.gsa.gov/cdnstatic/SF901-18a.pdf?forceDownload=1>