

retention period. Also called *disposable records*.

(v) *Transclassification* means information that has been removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive orders as “National Security Information.”

(w) *Unscheduled records* means Federal records whose final disposition has not been approved by NARA. All records that fall under a NARA approved records control schedule are considered to be scheduled records.

PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Subpart A—General Information

Sec.

- 2002.1 Purpose and scope.
- 2002.2 Incorporation by reference.
- 2002.4 Definitions.
- 2002.6 CUI Executive Agent (EA).
- 2002.8 Roles and responsibilities.

Subpart B—Key Elements of the CUI Program

- 2002.10 The CUI Registry.
- 2002.12 CUI categories and subcategories.
- 2002.14 Safeguarding.
- 2002.16 Accessing and disseminating.
- 2002.18 Decontrolling.
- 2002.20 Marking.
- 2002.22 Limitations on applicability of agency CUI policies.
- 2002.24 Agency self-inspection program.

Subpart C—CUI Program Management

- 2002.30 Education and training.
- 2002.32 CUI cover sheets.
- 2002.34 Transferring records.
- 2002.36 Legacy materials.
- 2002.38 Waivers of CUI requirements.
- 2002.44 CUI and disclosure statutes.
- 2002.46 CUI and the Privacy Act.
- 2002.48 CUI and the Administrative Procedure Act (APA).
- 2002.50 Challenges to designation of information as CUI.
- 2002.52 Dispute resolution for agencies.
- 2002.54 Misuse of CUI.
- 2002.56 Sanctions for misuse of CUI.

APPENDIX A TO PART 2002—ACRONYMS

AUTHORITY: E.O. 13556, 75 FR 68675, 3 CFR, 2010 Comp., pp. 267–270.

SOURCE: 81 FR 63336, Sept. 14, 2016, unless otherwise noted.

Subpart A—General Information

§ 2002.1 Purpose and scope.

(a) This part describes the executive branch’s Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI.

(b) The CUI Program standardizes the way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526, Classified National Security Information, December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, *et seq.*), as amended.

(c) All unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI. Law, regulation (to include this part), or Government-wide policy must require or permit such controls. Agencies therefore may not implement safeguarding or dissemination controls for any unclassified information other than those controls consistent with the CUI Program.

(d) Prior to the CUI Program, agencies often employed *ad hoc*, agency-specific policies, procedures, and markings to handle this information. This patchwork approach caused agencies to mark and handle information inconsistently, implement unclear or unnecessarily restrictive disseminating policies, and create obstacles to sharing information.

(e) An executive branch-wide CUI policy balances the need to safeguard CUI with the public interest in sharing information appropriately and without unnecessary burdens.

(f) This part applies to all executive branch agencies that designate or handle information that meets the standards for CUI. This part does not apply directly to non-executive branch entities, but it does apply indirectly to non-executive branch CUI recipients, through incorporation into agreements (see §§ 2002.4(c) and 2002.16(a) for more information).

§ 2002.2

(g) This part rescinds Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556 (June 9, 2011).

(h) This part creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(i) This part, which contains the CUI Executive Agent (EA)'s control policy, overrides agency-specific or *ad hoc* requirements when they conflict. This part does not alter, limit, or supersede a requirement stated in laws, regulations, or Government-wide policies or impede the statutory authority of agency heads.

§ 2002.2 Incorporation by reference.

(a) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, NARA must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. You may inspect all approved material incorporated by reference at NARA's textual research room, located at National Archives and Records Administration; 8601 Adelphi Road; Room 2000; College Park, MD 20740-6001. To arrange to inspect this approved material at NARA, contact NARA's Regulation Comments Desk (Strategy and Performance Division (SP)) by email at regulation_comments@nara.gov or by telephone at 301.837.3151. All approved material is available from the sources listed below. You may also inspect approved material at the Office of the Federal Register (OFR). For information on the availability of this material at the OFR, call 202-741-6030 or go to http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.

(b) The National Institute of Standards and Technology (NIST), by mail at 100 Bureau Drive, Stop 1070; Gaithersburg, MD 20899-1070, by email at inquiries@nist.gov, by phone at (301) 975-NIST (6478) or Federal Relay Service (800)

32 CFR Ch. XX (7-1-18 Edition)

877-8339 (TTY), or online at <http://nist.gov/publication-portal.cfm>.

(1) FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004. IBR approved for §§ 2002.14(c) and (g), and 2002.16(c).

(2) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. IBR approved for §§ 2002.14(c) and (g), and 2002.16(c).

(3) NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (includes updates as of 01-22-2015), (NIST SP 800-53). IBR approved for §§ 2002.14(c), (e), (f), and (g), and 2002.16(c).

(4) NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1, December 2014, (NIST SP 800-88). IBR approved for § 2002.14(f).

(5) NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, June 2015 (includes updates as of January 14, 2016), (NIST SP 800-171). IBR approved for § 2002.14(h).

§ 2002.4 Definitions.

As used in this part:

(a) *Agency* (also Federal agency, executive agency, executive branch agency) is any "executive agency," as defined in 5 U.S.C. 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

(b) *Agency CUI policies* are the policies the agency enacts to implement the CUI Program within the agency. They must be in accordance with the Order, this part, and the CUI Registry and approved by the CUI EA.

(c) *Agreements and arrangements* are any vehicle that sets out 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 written