the legal control of the Archivist pursuant to sections 2111, 2111 note, or 2203 of title 44, U.S.C.

(q) *Redaction* means the removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any reasonably known technique or analysis.

(r) *Risk management principles* means the principles applied for assessing threats and vulnerabilities and implementing security countermeasures while maximizing the sharing of information to achieve an acceptable level of risk at an acceptable cost.

(s) *Security-in-depth* means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

(t) *Supplemental controls* means prescribed procedures or systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.

(u) *Temporary records* means Federal records approved by NARA for disposal, either immediately or after a specified 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

Subpart B—Key Elements of the CUI Program

Subpart C—CUI Program Management

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).

(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) 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 agreements or arrangements that include CUI provisions whenever feasible (see § 2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see § 2002.16(a)(5)(iii) and (a)(6) for details).

(d) *Authorized holder* is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part.

(e) *Classified information* is information that 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, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.

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

(g) *Control level* is a general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

(h) *Controlled Unclassified Information* (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) 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.

(i) *Controls* are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may

specify the controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case, the agency applies controls from the Order, this part, and the CUI Registry).

(j) *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 this part 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.

(k) *CUI categories and subcategories* are those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which 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 of 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. Also consult the agency's CUI policy for specific direction from the Senior Agency Official.

(l) *CUI category or subcategory markings* are the markings approved by the CUI EA for the categories and subcategories listed in the CUI Registry.

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

(n) *CUI Program* is 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 the Order, this part, and the CUI Registry.

(o) *CUI Program manager* is an agency official, designated by the agency head or CUI SAO, to serve as the official representative to the CUI EA on the agency's day-to-day CUI Program operations, both within the agency and in interagency contexts.

(p) *CUI Registry* is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part. 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.

(q) *CUI senior agency official (SAO)* is a senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. The CUI SAO is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI EA.

(r) *CUI Specified* is 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 specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

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

(t) *Designating CUI* occurs when an authorized holder, consistent with this part and the CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with this part.

(u) *Designating agency* is the executive branch agency that designates or approves the designation of a specific item of information as CUI.

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

(w) *Document* means any tangible thing which constitutes or contains information, and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.

(x) *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).

(y) *Foreign entity* is a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.

(z) *Formerly Restricted Data (FRD)* is a type of information classified under the Atomic Energy Act, and defined in 10 CFR 1045, Nuclear Classification and Declassification.

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

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

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

(dd) *Limited dissemination control* is any CUI EA-approved control that agencies may use to limit or specify CUI dissemination.

(ee) *Misuse of CUI* occurs when someone uses CUI in a manner not in accordance with the policy contained in the Order, this part, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected

information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

(ff) *National Security System* is a special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42 and 44 U.S.C. 3542(b)(2).

(gg) *Non-executive branch entity* is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities as defined in this part, nor does it include individuals or organizations when they receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974.

(hh) *On behalf of an agency* occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

(ii) *Order* is Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267), or any successor order.

(jj) *Portion* is ordinarily a section within a document, and may include subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, bullets points, or other sections.

(kk) *Protection* includes all controls an agency applies or must apply when handling information that qualifies as CUI.

(ll) *Public release* occurs when the agency that originally designated particular information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though an agency may disclose some CUI to a member of the public, the Government must still control that CUI unless the agency publicly releases it through its official public release processes.

(mm) *Records* are agency records and Presidential papers or Presidential records (or Vice-Presidential), as those terms are defined in 44 U.S.C. 3301 and 44 U.S.C. 2201 and 2207. Records also include such items created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.

(nn) *Required or permitted (by a law, regulation, or Government-wide policy)* is the basis by which information may qualify as CUI. If a law, regulation, or Government-wide policy requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as ''is exempt from'' applying certain information release or disclosure requirements, ''may'' release or disclose the information, ''may not be required to'' release or disclose the information, ''is responsible for protecting'' the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

(oo) *Restricted Data (RD)* is a type of information classified under the Atomic Energy Act, defined in 10 CFR part 1045, Nuclear Classification and Declassification.

(pp) *Re-use* means incorporating, restating, or paraphrasing information from its originally designated form into a newly created document.

(qq) *Self-inspection* is an agency's internally managed review and evaluation of its activities to implement the CUI Program.

(rr) *Unauthorized disclosure* occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.

(ss) *Uncontrolled unclassified information* is information that neither the Order nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.

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

§ 2002.6 CUI Executive Agent (EA).

(a) Section 2(c) of the Order designates NARA as the CUI Executive Agent (EA) to implement the Order and to oversee agency efforts to comply with the Order, this part, and the CUI Registry.

(b) NARA has delegated the CUI EA responsibilities to the Director of ISOO. Under this authority, ISOO staff carry out CUI oversight responsibilities and manage the Federal CUI program.

§ 2002.8 Roles and responsibilities.

(a) The CUI EA:

(1) Develops and issues policy, guidance, and other materials, as needed, to implement the Order, the CUI Registry, and this part, and to establish and maintain the CUI Program;

(2) Consults with affected agencies, Government-wide policy bodies, State, local, Tribal, and private sector partners, and representatives of the public on matters pertaining to CUI as needed;

(3) Establishes, convenes, and chairs the CUI Advisory Council (the Council) to address matters pertaining to the CUI Program. The CUI EA consults with affected agencies to develop and document the Council's structure and procedures, and submits the details to OMB for approval;

(4) Reviews and approves agency policies implementing this part to ensure their consistency with the Order, this part, and the CUI Registry;

(5) Reviews, evaluates, and oversees agencies' actions to implement the CUI Program, to ensure compliance with the Order, this part, and the CUI Registry;

(6) Establishes a management and planning framework, including associated deadlines for phased implementation, based on agency compliance plans submitted pursuant to section 5(b) of the Order, and in consultation with affected agencies and OMB;

(7) Approves categories and subcategories of CUI as needed and publishes them in the CUI Registry;

(8) Maintains and updates the CUI Registry as needed;

(9) Prescribes standards, procedures, guidance, and instructions for oversight and agency self-inspection programs, to include performing on-site inspections;

(10) Standardizes forms and procedures to implement the CUI Program;

(11) Considers and resolves, as appropriate, disputes, complaints, and suggestions about the CUI Program from entities in or outside the Government; and

(12) Reports to the President on implementation of the Order and the requirements of this part. This includes publishing a report on the status of agency implementation at least biennially, or more frequently at the discretion of the CUI EA.

(b) Agency heads:

(1) Ensure agency senior leadership support, and make adequate resources available to implement, manage, and comply with the CUI Program as administered by the CUI EA;

(2) Designate a CUI senior agency official (SAO) responsible for oversight of

the agency's CUI Program implementation, compliance, and management, and include the official in agency contact listings;

(3) Approve agency policies, as required, to implement the CUI Program; and

(4) Establish and maintain a self-inspection program to ensure the agency complies with the principles and requirements of the Order, this part, and the CUI Registry.

(c) The CUI SAO:

(1) Must be at the Senior Executive Service level or equivalent;

(2) Directs and oversees the agency's CUI Program;

(3) Designates a CUI Program manager;

(4) Ensures the agency has CUI implementing policies and plans, as needed;

(5) Implements an education and training program pursuant to §2002.30;

(6) Upon request of the CUI EA under section 5(c) of the Order, provides an update of CUI implementation efforts for subsequent reporting;

(7) Submits 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 for safeguarding or dissemination controls;

(8) Coordinates 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;

(9) Establishes processes for handling CUI decontrol requests submitted by authorized holders;

(10) Includes a description of all existing waivers in the annual report to the CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps the agency is taking to ensure sufficient protection of CUI within the agency;

(11) Develops and implements the agency's self-inspection program;

(12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for instructions when they receive unmarked or improperly marked information the agency designated as CUI;

(13) Establishes a process to accept and manage challenges to CUI status (which may include improper or absent marking);

(14) Establish processes and criteria for reporting and investigating misuse of CUI; and

(15) Follows the requirements for the CUI SAO listed in §2002.38(e), regarding waivers for CUI.

(d) The Director of National Intelligence: After consulting with the heads of affected agencies and the Director of ISOO, may issue directives to implement this part with respect to the protection of intelligence sources, methods, and activities. Such directives must be in accordance with the Order, this part, and the CUI Registry.

Subpart B—Key Elements of the CUI Program

§2002.10 The CUI Registry.

(a) The CUI EA maintains the CUI Registry, which:

(1) Is the authoritative central repository for all guidance, policy, instructions, and information on CUI (other than the Order and this part);

(2) Is publicly accessible;

(3) Includes authorized CUI categories and subcategories, associated markings, applicable decontrolling procedures, and other guidance and policy information; and

(4) Includes citation(s) to laws, regulations, or Government-wide policies that form the basis for each category and subcategory.

(b) Agencies and authorized holders must follow the instructions contained in the CUI Registry in addition to all requirements in the Order and this part.

§2002.12 CUI categories and subcategories.

(a) CUI categories and subcategories are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies 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. Agencies may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Program.

(b) Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI.

§ 2002.14 Safeguarding.

(a) *General safeguarding policy.* (1) Pursuant to the Order and this part, and in consultation with affected agencies, the CUI EA issues safeguarding standards in this part and, as necessary, in the CUI Registry, updating them as needed. These standards require agencies to safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders.

(2) Safeguarding measures that agencies are authorized or accredited to use for classified information and national security systems are also sufficient for safeguarding CUI in accordance with the organization's management and acceptance of risk.

(3) Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies may not otherwise require controls for CUI Basic at a level higher than permitted in the CUI Basic requirements when disseminating the CUI Basic outside the agency.

(4) Authorized holders must comply with policy in the Order, this part, and the CUI Registry, and review any applicable agency CUI policies for additional instructions. For information designated as CUI Specified, authorized holders must also follow the procedures in the underlying laws, regulations, or Government-wide policies.

(b) *CUI safeguarding standards.* Authorized holders must safeguard CUI using one of the following types of standards:

(1) *CUI Basic.* CUI Basic is the default set of standards authorized holders must apply to all CUI unless the CUI Registry annotates that CUI as CUI Specified.

(2) *CUI Specified.* (i) Authorized holders safeguard CUI Specified in accordance with the requirements of the underlying authorities indicated in the CUI Registry.

(ii) When the laws, regulations, or Government-wide policies governing a specific type of CUI Specified are silent on either a safeguarding or disseminating control, agencies must apply CUI Basic standards to that aspect of the information's controls, unless this results in treatment that does not accord with the CUI Specified authority. In such cases, agencies must apply the CUI Specified standards and may apply limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI Specified authority.

(c) *Protecting CUI under the control of an authorized holder.* Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI. They must include the following measures among the reasonable precautions:

(1) Establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments;

(2) Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI;

(3) Keep CUI under the authorized holder's direct control or protect it with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment; and

(4) Protect the confidentiality of CUI that agencies or authorized holders process, store, or transmit on Federal information systems in accordance with the applicable security requirements and controls established in FIPS PUB 199, FIPS PUB 200, and NIST SP 800–53, (incorporated by reference, see § 2002.2), and paragraph (g) of this section.

(d) *Protecting CUI when shipping or mailing.* When sending CUI, authorized holders:

(1) May use the United States Postal Service or any commercial delivery service when they need to transport or deliver CUI to another entity;

(2) Should use in-transit automated tracking and accountability tools when they send CUI;

(3) May use interoffice or interagency mail systems to transport CUI; and

(4) Must mark packages that contain CUI according to marking requirements contained in this part and in guidance published by the CUI EA. See § 2002.20 for more guidance on marking requirements.

(e) *Reproducing CUI.* Authorized holders:

(1) May reproduce (*e.g.,* copy, scan, print, electronically duplicate) CUI in furtherance of a lawful Government purpose; and

(2) Must ensure, when reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, that the equipment does not retain data or the agency must otherwise sanitize it in accordance with NIST SP 800–53 (incorporated by reference, see § 2002.2).

(f) *Destroying CUI.* (1) Authorized holders may destroy CUI when:

(i) The agency no longer needs the information; and

(ii) Records disposition schedules published or approved by NARA allow.

(2) When destroying CUI, including in electronic form, agencies must do so in a manner that makes it unreadable, indecipherable, and irrecoverable. Agencies must use any destruction method specifically required by law, regulation, or Government-wide policy for that CUI. If the authority does not specify a destruction method, agencies must use one of the following methods:

(i) Guidance for destruction in NIST SP 800–53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800–88, Guidelines for Media Sanitization (incorporated by reference, see § 2002.2); or

(ii) Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or any implementing or successor guidance.

(g) *Information systems that process, store, or transmit CUI.* In accordance with FIPS PUB 199 (incorporated by reference, see § 2002.2), CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines the security impact levels for Federal information and Federal information systems. Agencies must also apply the appropriate security requirements and controls from FIPS PUB 200 and NIST SP 800–53 (incorporated by reference, see § 2002.2) to CUI in accordance with any risk-based tailoring decisions they make. Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies 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 the agency.

(h) Information systems that process, store, or transmit CUI are of two different types:

(1) A 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. An information system operated on behalf of an agency provides information processing services to the agency that the Government might otherwise perform itself but has decided to outsource. This includes systems operated exclusively for Government use and systems operated for multiple users (multiple Federal agencies or Government and private sector users). Information systems that a non-executive branch entity operates on behalf of an agency are subject to the requirements of this part as though they are the agency's systems, and agencies may require these systems to meet additional requirements the agency sets for its own internal systems.

(2) A non-Federal information system is any information system that does not meet the criteria for a Federal information system. Agencies may not treat non-Federal information systems as though they are agency systems, so

agencies cannot require that non-executive branch entities protect these systems in the same manner that the agencies might protect their own information systems. 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 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

§ 2002.16 Accessing and disseminating.

(a) *General policy*—(1) *Access.* Agencies should disseminate and permit access to CUI, provided such access or dissemination:

(i) Abides by the laws, regulations, or Government-wide policies that established the CUI category or subcategory;

(ii) Furthers a lawful Government purpose;

(iii) Is not restricted by an authorized limited dissemination control established by the CUI EA; and,

(iv) Is not otherwise prohibited by law.

(2) *Dissemination controls.* (i) Agencies must impose dissemination controls judiciously and should do so only to apply necessary restrictions on access to CUI, including those required by law, regulation, or Government-wide policy.

(ii) Agencies may not impose controls that unlawfully or improperly restrict access to CUI.

(3) *Marking.* Prior to disseminating CUI, authorized holders must label CUI according to marking guidance issued by the CUI EA, and must include any specific markings required by law, regulation, or Government-wide policy.

(4) *Reasonable expectation.* To disseminate CUI to a non-executive branch entity, authorized holders must reasonably expect that all intended recipients are authorized to receive the CUI and have a basic understanding of how to handle it.

(5) *Agreements.* Agencies should enter into agreements with any non-executive branch or foreign entity with which the agency shares or intends to share CUI, as follows (except as provided in paragraph (a)(7) of this section):

(i) *Information-sharing agreements.* When agencies intend to share CUI with a non-executive branch entity, they should enter into a formal agreement (see § 2004.4(c) for more information on agreements), whenever feasible. Such an agreement may take any form the agency head approves, but when established, it must include a requirement to comply with Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267) or any successor order (the Order), this part, and the CUI Registry.

(ii) *Sharing CUI without a formal agreement.* When an agency cannot enter into agreements under paragraph (a)(6)(i) of this section, but the agency's mission requires it to disseminate CUI to non-executive branch entities, the agency must communicate to the recipient that the Government strongly encourages the non-executive branch entity to protect CUI in accordance with the Order, this part, and the CUI Registry, and that such protections should accompany the CUI if the entity disseminates it further.

(iii) *Foreign entity sharing.* When entering into agreements or arrangements with a foreign entity, agencies should encourage that entity to protect CUI in accordance with the Order, this part, and the CUI Registry to the extent possible, but agencies may use their judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding

CUI. If such agreements or arrangements include safeguarding or dissemination controls on unclassified information, the agency must not establish a parallel protection regime to the CUI Program: For example, the agency must use CUI markings rather than alternative ones (*e.g.*, such as SBU) for safeguarding or dissemination controls on CUI received from or sent to foreign entities, must abide by any requirements set by the CUI category or subcategory's governing laws, regulations, or Government-wide policies, etc.

(iv) *Pre-existing agreements.* When an agency entered into an information-sharing agreement prior to November 14, 2016, the agency should modify any terms in that agreement that conflict with the requirements in the Order, this part, and the CUI Registry, when feasible.

(6) *Agreement content.* At a minimum, agreements with non-executive branch entities must include provisions that state:

(i) Non-executive branch entities must handle CUI in accordance with the Order, this part, and the CUI Registry;

(ii) Misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies; and

(iii) The non-executive branch entity must report any non-compliance with handling requirements to the disseminating agency using methods approved by that agency's SAO. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency.

(7) *Exceptions to agreements.* Agencies 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 FOIA or Privacy Act request.

(b) *Controls on accessing and disseminating CUI*—(1) *CUI Basic.* Authorized holders should disseminate and encourage access to CUI Basic for any recipient when the access meets the requirements set out in paragraph (a)(1) of this section.

(2) *CUI Specified.* Authorized holders disseminate and allow access to CUI Specified as required or permitted by the authorizing laws, regulations, or Government-wide policies that established that CUI Specified.

(i) The CUI Registry annotates CUI that requires or permits Specified controls based on law, regulation, and Government-wide policy.

(ii) In the absence of specific dissemination restrictions in the authorizing law, regulation, or Government-wide policy, agencies may disseminate CUI Specified as they would CUI Basic.

(3) *Receipt of CUI.* Non-executive branch entities may receive CUI directly from members of the executive branch or as sub-recipients from other non-executive branch entities.

(4) *Limited dissemination.* (i) Agencies may place additional limits on disseminating CUI only through use of the limited dissemination controls approved by the CUI EA and published in the CUI Registry. These limited dissemination controls are separate from any controls that a CUI Specified authority requires or permits.

(ii) Using limited dissemination controls to unnecessarily restrict access to CUI is contrary to the goals of the CUI Program. Agencies may therefore use these controls only when it furthers a lawful Government purpose, or laws, regulations, or Government-wide policies require or permit an agency to do so. If an authorized holder has significant doubt about whether it is appropriate to use a limited dissemination control, the authorized holder should consult with and follow the designating agency's policy. If, after consulting the policy, significant doubt still remains,

the authorized holder should not apply the limited dissemination control.

(iii) Only the designating agency may apply limited dissemination controls to CUI. Other entities that receive CUI and seek to apply additional controls must request permission to do so from the designating agency.

(iv) Authorized holders may apply limited dissemination controls to any CUI for which they are required or permitted to restrict access by or to certain entities.

(v) Designating entities may combine approved limited dissemination controls listed in the CUI Registry to accommodate necessary practices.

(c) *Methods of disseminating CUI.* (1) Before disseminating CUI, authorized holders must reasonably expect that all intended recipients have a lawful Government purpose to receive the CUI. Authorized holders may then disseminate the CUI by any method that meets the safeguarding requirements of this part and the CUI Registry and ensures receipt in a timely manner, unless the laws, regulations, or Government-wide policies that govern that CUI require otherwise.

(2) To disseminate CUI using systems or components that are subject to NIST guidelines and publications (*e.g.*, email applications, text messaging, facsimile, or voicemail), agencies must do so in accordance with the no-less-than-moderate confidentiality impact value set out in FIPS PUB 199, FIPS PUB 200, NIST SP 800–53 (incorporated by reference, see § 2002.2).

§ 2002.18 Decontrolling.

(a) Agencies should decontrol as soon as practicable any CUI designated by their agency that no longer requires safeguarding or dissemination controls, unless doing so conflicts with the governing law, regulation, or Government-wide policy.

(b) Agencies may decontrol CUI automatically upon the occurrence of one of the conditions below, or through an affirmative decision by the designating agency:

(1) When laws, regulations or Government-wide policies no longer require its control as CUI and the authorized holder has the appropriate authority under the authorizing law, regulation, or Government-wide policy;

(2) When the designating agency decides to release it to the public by making an affirmative, proactive disclosure;

(3) When the agency discloses it in accordance with an applicable information access statute, such as the FOIA, or the Privacy Act (when legally permissible), if the agency incorporates such disclosures into its public release processes; or

(4) When a pre-determined event or date occurs, as described in § 2002.20(g), unless law, regulation, or Government-wide policy requires coordination first.

(c) The designating agency may also decontrol CUI:

(1) In response to a request by an authorized holder to decontrol it; or

(2) Concurrently with any declassification action under Executive Order 13526 or any predecessor or successor order, as long as the information also appropriately qualifies for decontrol as CUI.

(d) An agency may designate in its CUI policies which agency personnel it authorizes to decontrol CUI, consistent with law, regulation, and Government-wide policy.

(e) Decontrolling CUI relieves authorized holders from requirements to handle the information under the CUI Program, but does not constitute authorization for public release.

(f) Authorized holders must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, releasing to the public, or donating it to a private institution. Otherwise, authorized holders do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

(1) Agency policy may allow authorized holders to remove or strike through only those CUI markings on the first or cover page of the decontrolled CUI and markings on the first page of any attachments that contain CUI.

(2) If an authorized holder uses the decontrolled CUI in a newly created document, the authorized holder must remove all CUI markings for the decontrolled information.

(g) Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and agency policies on the public release of information.

(h) Authorized holders may request that the designating agency decontrol certain CUI.

(i) If an authorized holder publicly releases CUI in accordance with the designating agency's authorized procedures, the release constitutes decontrol of the information.

(j) Unauthorized disclosure of CUI does not constitute decontrol.

(k) Agencies must not decontrol CUI in an attempt to conceal, or to otherwise circumvent accountability for, an identified unauthorized disclosure.

(l) When laws, regulations, or Government-wide policies require specific decontrol procedures, authorized holders must follow such requirements.

(m) The Archivist of the United States may decontrol records transferred to the National Archives in accordance with § 2002.34, absent a specific agreement otherwise 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.

§ 2002.20 Marking.

(a) *General marking policy.* (1) CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls. Agencies and authorized holders must, in accordance with the implementation timelines established for the agency by the CUI EA:

(i) Discontinue all use of legacy or other markings not permitted by this part or included in the CUI Registry; and

(ii) Uniformly and conspicuously apply CUI markings to all CUI exclusively in accordance with the part and the CUI Registry, unless this part or the CUI EA otherwise specifically permits. See paragraph (a)(6) of this section and §§ 2002.38, Waivers of CUI requirements, and 2002.36, Legacy materials, for more information.

(2) Agencies may not modify CUI Program markings or deviate from the method of use prescribed by the CUI EA (in this part and the CUI Registry) in an effort to accommodate existing agency marking practices, except in circumstances approved by the CUI EA. The CUI Program prohibits using markings or practices not included in this part or the CUI Registry. If legacy markings remain on information, the legacy markings are void and no longer indicate that the information is protected or that it is or qualifies as CUI.

(3) An agency receiving an incorrectly marked document should notify either the disseminating entity or the designating agency, and request a properly marked document.

(4) The designating agency determines that the information qualifies for CUI status and applies the appropriate CUI marking when it designates that information as CUI.

(5) If an agency has information within its control that qualifies as CUI but has not been previously marked as CUI for any reason (for example, pursuant to an agency internal marking waiver as referenced in § 2002.38 (a)), the agency must mark it as CUI prior to disseminating it.

(6) Agencies must not mark information as CUI to conceal illegality, negligence, ineptitude, or other disreputable circumstances embarrassing to any person, any agency, the Federal Government, or any of their partners, or for any purpose other than to adhere to the law, regulation, or Government-wide policy authorizing the control.

(7) The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable handling requirements as described in the Order, this part, and the CUI Registry.

(8) When it is impractical for an agency to individually mark CUI due to quantity or nature of the information, or when an agency has issued a limited CUI marking waiver, authorized holders must make recipients aware of the information's CUI status using an alternate marking method that is readily apparent (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) *The CUI banner marking.* Designators of CUI must mark all CUI with a CUI banner marking, which may include up to three elements:

(1) *The CUI control marking (mandatory).* (i) The CUI control marking may consist of either the word ''CONTROLLED'' or the acronym ''CUI,'' at the designator's discretion. Agencies may specify in their CUI policy that employees must use one or the other.

(ii) The CUI Registry contains additional, specific guidance and instructions for using the CUI control marking.

(iii) Authorized holders who designate CUI may not use alternative markings to identify or mark items as CUI.

(2) *CUI category or subcategory markings (mandatory for CUI Specified).* (i) The CUI Registry lists the category and subcategory markings, which align with the CUI's governing category or subcategory.

(ii) Although the CUI Program does not require agencies to use category or subcategory markings on CUI Basic, an agency's CUI SAO may establish agency policy that mandates use of CUI category or subcategory markings on CUI Basic.

(iii) However, authorized holders must include in the CUI banner marking all CUI Specified category or subcategory markings that pertain to the information in the document. If law, regulation, or Government-wide policy requires specific marking, disseminating, informing, distribution limitation, or warning statements, agencies must use those indicators as those authorities require or permit. However, agencies must not include these additional indicators in the CUI banner marking or CUI portion markings.

(iv) The CUI Registry contains additional, specific guidance and instructions for using CUI category and subcategory markings.

(3) *Limited dissemination control markings.* (i) CUI limited dissemination control markings align with limited dissemination controls established by the CUI EA under § 2002.16(b)(4).

(ii) Agency policy should include specific criteria establishing which authorized holders may apply limited dissemination controls and their corresponding markings, and when. Such agency policy must align with the requirements in § 2002.16(b)(4).

(iii) The CUI Registry contains additional, specific guidance and instructions for using limited dissemination control markings.

(c) *Using the CUI banner marking.* (1) The content of the CUI banner marking must apply to the whole document (*i.e.*, inclusive of all CUI within the document) and must be the same on each page of the document that includes CUI.

(2) The CUI Registry contains additional, specific guidelines and instructions for using the CUI banner marking.

(d) *CUI designation indicator (mandatory).* (1) All documents containing CUI must carry an indicator of who designated the CUI within it. This must include the designator's agency (at a minimum) and may take any form that identifies the designating agency, including letterhead or other standard agency indicators, or adding a ''Controlled by'' line (for example, ''Controlled by: Division 5, Department of Good Works.'').

(2) The designation indicator must be readily apparent to authorized holders and may appear only on the first page or cover. The CUI Registry contains additional, specific guidance and requirements for using CUI designation indicators.

(e) *CUI decontrolling indicators.* (1) Where feasible, designating agencies must include a specific decontrolling date or event with all CUI. Agencies may do so in any manner that makes the decontrolling schedule readily apparent to an authorized holder.

(2) Authorized holders may consider specific items of CUI as decontrolled as of the date indicated, requiring no further review by, or communication with, the designator.

(3) If using a specific event after which the CUI is considered decontrolled:

(i) The event must be foreseeable and verifiable by any authorized holder (*e.g.*, not based on or requiring special access or knowledge); and

(ii) The designator should include point of contact and preferred method of contact information in the decontrol

indicator when using this method, to allow authorized holders to verify that a specified event has occurred.

(4) The CUI Registry contains additional, specific guidance and instructions for using limited dissemination control markings.

(f) *Portion marking CUI.* (1) Agencies are permitted and encouraged to portion mark all CUI, to facilitate information sharing and proper handling.

(2) Authorized holders who designate CUI may mark CUI only with portion markings approved by the CUI EA and listed in the CUI Registry.

(3) CUI portion markings consist of the following elements:

(i) The CUI control marking, which must be the acronym ''CUI'';

(ii) CUI category/subcategory portion markings (if required or permitted); and

(iii) CUI limited dissemination control portion markings (if required).

(4) When using portion markings:

(i) CUI category and subcategory portion markings are optional for CUI Basic. Agencies may manage their use by means of agency policy.

(ii) Authorized holders permitted to designate CUI must portion mark both CUI and uncontrolled unclassified portions.

(5) 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, designators of CUI 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, or if the portion includes some CUI and some uncontrolled unclassified information, authorized holders should portion mark all segments separately to avoid improper control of any one segment.

(6) Each portion must reflect the control level of only that individual portion. 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.

(7) The CUI Registry contains additional, specific guidance and instructions for using CUI portion markings and uncontrolled unclassified portion markings.

(g) *Commingling CUI markings with Classified National Security Information (CNSI).* When authorized holders include CUI in documents that also contain CNSI, the decontrolling provisions of the Order and this part apply only to portions marked as CUI. In addition, authorized holders must:

(1) Portion mark all CUI to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information;

(2) Include the CUI control marking, CUI Specified category and subcategory markings, and limited dissemination control markings in an overall banner marking; and

(3) Follow the requirements of the Order and this part, and instructions in the CUI Registry on marking CUI when commingled with CNSI.

(h) *Commingling restricted data (RD) and formerly restricted data (FRD) with CUI.* (1) To the extent possible, avoid commingling RD or FRD with CUI in the same document. When it is not practicable to avoid such commingling, follow the marking requirements in the Order and this part, and instructions in the CUI Registry, as well as the marking requirements in 10 CFR part 1045, Nuclear Classification and Declassification.

(2) Follow the requirements of 10 CFR part 1045 when extracting an RD or FRD portion for use in a new document.

(3) Follow the requirements of the Order and this part, and instructions in the CUI Registry if extracting a CUI portion for use in a new document.

(4) 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.

(i) *Packages and parcels containing CUI.* (1) Address packages that contain CUI for delivery only to a specific recipient.

(2) Do not put CUI markings on the outside of an envelope or package, or

otherwise indicate on the outside that the item contains CUI.

(j) *Transmittal document marking requirements.* (1) When a transmittal document accompanies CUI, the transmittal document must include a CUI marking on its face (''CONTROLLED'' or ''CUI''), indicating that CUI is attached or enclosed.

(2) The transmittal document must also include conspicuously on its face the following or similar instructions, as appropriate:

(i) ''When enclosure is removed, this document is Uncontrolled Unclassified Information''; or

(ii) ''When enclosure is removed, this document is (control level); upon removal, this document does not contain CUI.''

(k) *Working papers.* Mark working papers containing CUI the same way as the finished product containing CUI would be marked and as required for any CUI contained within them. Handle them in accordance with this part and the CUI Registry.

(l) *Using supplemental administrative markings with CUI.* (1) Agency heads may authorize the use of supplemental administrative markings (*e.g.* ''Predecisional,'' ''Deliberative,'' ''Draft'') for use with CUI.

(2) Agency heads may not authorize the use of supplemental administrative markings to establish safeguarding requirements or disseminating restrictions, or to designate the information as CUI. However, agencies may use these markings to inform recipients of the non-final status of documents under development to avoid confusion and maintain the integrity of an agency's decision-making process.

(3) Agencies must detail requirements for using supplemental administrative markings with CUI in agency policy that is available to anyone who may come into possession of CUI with these markings.

(4) Authorized holders must not incorporate or include supplemental administrative markings in the CUI marking scheme detailed in this part and the CUI Registry.

(5) Supplemental administrative markings must not duplicate any CUI marking described in this part or the CUI Registry.

(m) *Unmarked CUI.* Treat unmarked information that qualifies as CUI as described in the Order, § 2002.8(c), and the CUI Registry.

§ 2002.22 Limitations on applicability of agency CUI policies.

(a) Agency CUI policies do not apply to entities outside that agency unless a law, regulation, or Government-wide policy requires or permits the controls contained in the agency policy to do so, and the CUI Registry lists that law, regulation, or Government-wide policy as a CUI authority.

(b) Agencies may not include additional requirements or restrictions on handling CUI other than those permitted in the Order, this part, or the CUI Registry when entering into agreements.

§ 2002.24 Agency self-inspection program.

(a) The agency must establish a self-inspection program pursuant to the requirement in § 2002.8(b)(4).

(b) The self-inspection program must include:

(1) At least annual review and assessment of the agency's CUI program. The agency head or CUI SAO should determine any greater frequency based on program needs and the degree to which the agency engages in designating CUI;

(2) Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;

(3) Formats for documenting self-inspections and recording findings when not prescribed by the CUI EA;

(4) Procedures by which to integrate lessons learned and best practices arising from reviews and assessments into operational policies, procedures, and training;

(5) A process for resolving deficiencies and taking corrective actions; and

(6) Analysis and conclusions from the self-inspection program, documented on an annual basis and as requested by the CUI EA.

Subpart C—CUI Program Management

§ 2002.30 Education and training.

(a) The CUI SAO must establish and implement an agency training policy. At a minimum, the training policy must address the means, methods, and frequency of agency CUI training.

(b) Agency training policy must ensure that 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.

(c) Agencies must train employees on these matters when the employees first begin working for the agency and at least once every two years thereafter.

(d) The CUI EA reviews agency training materials to ensure consistency and compliance with the Order, this part, and the CUI Registry.

§ 2002.32 CUI cover sheets.

(a) Agencies may use cover sheets for CUI. If an agency chooses to use cover sheets, it must use CUI EA-approved cover sheets, which agencies can find on the CUI Registry.

(b) Agencies may use cover sheets to identify CUI, alert observers that CUI is present from a distance, and serve as a shield to protect the attached CUI from inadvertent disclosure.

§ 2002.34 Transferring records.

(a) When feasible, agencies must decontrol records containing CUI prior to transferring them to NARA.

(b) When an agency cannot decontrol records before transferring them to NARA, the agency must:

(1) Indicate on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, 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.

(c) If the agency does not indicate the status as CUI on the TR or SF 258, NARA may assume the agency decontrolled the information prior to transfer, regardless of any CUI markings on the actual records.

§ 2002.36 Legacy materials.

(a) Agencies must review documents created prior to November 14, 2016 and re-mark any that contain information that qualifies as CUI in accordance with the Order, this part, and the CUI Registry. When agencies do not individually re-mark legacy material that qualifies as CUI, agencies must use an alternate permitted marking method (see § 2002.20(a)(8)).

(b) When the CUI SAO deems remarking legacy documents to be excessively burdensome, the CUI SAO may grant a legacy material marking waiver under § 2002.38(b).

(c) When the agency re-uses any information from legacy documents that qualifies as CUI, whether the documents have obsolete control markings or not, the agency must designate the newly-created document (or other reuse) as CUI and mark it accordingly.

§ 2002.38 Waivers of CUI requirements.

(a) *Limited CUI marking waivers within the agency.* 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) *Limited legacy material marking waivers within the agency.* (1) In situations in which the agency has a substantial amount of stored information with legacy markings, and removing legacy markings and designating or remarking it as CUI would be excessively burdensome, the agency's CUI SAO may approve a waiver of these requirements for some or all of that information while it remains under agency control.

(2) When an authorized holder re-uses any legacy information or information derived from legacy documents that qualifies as CUI, they must remove or redact legacy markings and designate or re-mark the information as CUI, even if the information is under a legacy material marking waiver prior to re-use.

(c) *Exigent circumstances waivers.* (1) In exigent circumstances, the agency head or the CUI SAO may waive the provisions and requirements established in this part or the CUI Registry for any CUI while it is within the agency's possession or control, unless specifically prohibited by applicable laws, regulations, or Government-wide policies.

(2) Exigent circumstances waivers may apply when an agency shares the information with other agencies or non-Federal entities. In such cases, the authorized holders must make recipients aware of the CUI status of any disseminated information.

(d) *For all waivers.* (1) The CUI SAO must still ensure that the agency appropriately safeguards and disseminates the CUI. See § 2002.20(a)(7);

(2) The CUI SAO must detail in each waiver the alternate protection methods the agency will employ to ensure protection of CUI subject to the waiver;

(3) All marking waivers apply to CUI subject to the waiver only while that agency continues to possess that CUI. No marking waiver may accompany CUI when an authorized holder disseminates it outside that agency;

(4) Authorized holders must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it outside the agency unless otherwise specifically permitted by the CUI EA; and

(5) When the circumstances requiring the waiver end, the CUI SAO must reinstitute the requirements for all CUI subject to the waiver without delay.

(e) The CUI SAO must:

(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.

§ 2002.44 CUI and disclosure statutes.

(a) *General policy.* The fact that an agency designates certain information as CUI does not affect an agency's or employee's determinations pursuant to any law that requires the agency or the employee to disclose that information or permits them to do so as a matter of discretion. The agency or employee must make such determinations according to the criteria set out in the governing law, not on the basis of the information's status as CUI.

(b) *CUI and the Freedom of Information Act (FOIA).* Agencies must not cite the FOIA as a CUI safeguarding or disseminating control authority for CUI. When an agency is determining whether to disclose information in response to a FOIA request, the agency must base its decision on the content of the information and applicability of any FOIA statutory exemptions, regardless of whether an agency designates or marks the information as CUI. There may be circumstances in which an agency may disclose CUI to an individual or entity, including through a FOIA response, but such disclosure does not always constitute public release as defined in this part. Although disclosed via a FOIA response, the agency may still need to control the CUI while the agency continues to hold the information, despite the disclosure, unless the agency otherwise decontrols it (or the agency includes in its policies that FOIA disclosure always results in public release and the CUI does not otherwise have another legal requirement for its continued control).

(c) *CUI and the Whistleblower Protection Act.* This part does not change or affect existing legal protections for whistleblowers. The fact that an agency designates or marks certain information as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority, and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, or executive order or directive.

§ 2002.46 CUI and the Privacy Act.

The fact that records are subject to the Privacy Act of 1974 does not mean that agencies must mark them as CUI. Consult agency policies or guidance to determine which records may be subject to the Privacy Act; consult the CUI Registry to determine which privacy information must be marked as CUI. Information contained in Privacy

Act systems of records may also be subject to controls under other CUI categories or subcategories and the agency may need to mark that information as CUI for that reason. In addition, when determining whether the agency must protect certain information under the Privacy Act, or whether the Privacy Act allows the agency to release the information to an individual, the agency must base its decision on the content of the information and the Privacy Act's criteria, regardless of whether an agency designates or marks the information as CUI.

§ 2002.48 CUI and the Administrative Procedure Act (APA).

Nothing in the regulations in this part alters the Administrative Procedure Act (APA) or the powers of Federal administrative law judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor do the regulations in this part impose requirements concerning the manner in which ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

§ 2002.50 Challenges to designation of information as CUI.

(a) Authorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the disseminating agency of this belief. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency.

(b) If the information at issue is involved in Government litigation, or the challenge to its designation or marking as CUI arises as part of the litigation, the issue of whether the challenger may access the information will be addressed via the litigation process instead of by the agency CUI program. Challengers should nonetheless notify the agency of the issue through the agency process described below, and include its litigation connection.

(c) CUI SAOs must create a process within their agency to accept and manage challenges to CUI status. At a minimum, this process must include a timely response to the challenger that:

(1) Acknowledges receipt of the challenge;

(2) States an expected timetable for response to the challenger;

(3) Provides an opportunity for the challenger to define a rationale for belief that the CUI in question is inappropriately designated;

(4) Gives contact information for the official making the agency's decision in this matter; and

(5) Ensures that challengers who are authorized holders have the option of bringing such challenges anonymously, and that challengers are not subject to retribution for bringing such challenges.

(d) Until the challenge is resolved, authorized holders should continue to safeguard and disseminate the challenged CUI at the control level indicated in the markings.

(e) If a challenging party disagrees with the response to a challenge, that party may use the Dispute Resolution procedures described in § 2002.52.

§ 2002.52 Dispute resolution for agencies.

(a) When laws, regulations, or Government-wide policies governing the CUI involved in a dispute set out specific procedures, processes, and requirements for resolving disputes, agencies must follow those processes for that CUI. This includes submitting the dispute to someone other than the CUI EA for resolution if the authority so requires. If the CUI at issue is involved in litigation, the agency should refer the issue to the appropriate attorneys for resolution through the litigation process.

(b) When laws, regulations, and Government-wide policies governing the CUI do not set out specific procedures, processes, or requirements for CUI dispute resolution (or the information is not involved in litigation), this part governs.

(c) All parties to a dispute arising from implementing or interpreting the Order, this part, or the CUI Registry should make every effort to resolve the dispute expeditiously. Parties should address disputes within a reasonable,

mutually acceptable time period, taking into consideration the parties' mission, sharing, and protection requirements.

(d) If parties to a dispute cannot reach a mutually acceptable resolution, either party may refer the matter to the CUI EA.

(e) The CUI EA acts as the impartial arbiter of the dispute and has the authority to render a decision on the dispute after consulting with all affected parties. If a party to the dispute is also a member of the Intelligence Community, the CUI EA must consult with the Office of the Director of National Intelligence when the CUI EA receives the dispute for resolution.

(f) Until the dispute is resolved, authorized holders should continue to safeguard and disseminate any disputed CUI at the control level indicated in the markings, or as directed by the CUI EA if the information is unmarked.

(g) Parties may appeal the CUI EA's decision through the Director of OMB to the President for resolution, pursuant to section 4(e) of the Order. If one of the parties to the dispute is the CUI EA and the parties cannot resolve the dispute under paragraph (c) of this section, the parties may likewise refer the matter to OMB for resolution.

§ 2002.54 Misuse of CUI.

(a) The CUI SAO must establish agency processes and criteria for reporting and investigating misuse of CUI.

(b) The CUI EA reports findings on any incident involving misuse of CUI to the offending agency's CUI SAO or CUI Program manager for action, as appropriate.

§ 2002.56 Sanctions for misuse of CUI.

(a) To the extent that agency heads are otherwise authorized to take administrative action against agency personnel who misuse CUI, agency CUI policy governing misuse should reflect that authority.

(b) Where laws, regulations, or Government-wide policies governing certain categories or subcategories of CUI specifically establish sanctions, agencies must adhere to such sanctions.

APPENDIX A TO PART 2002—ACRONYMS

CNSI—Classified National Security Information
Council or the Council—The CUI Advisory Council
CUI—Controlled unclassified information
EA—The CUI Executive Agent (which is ISOO)
FOIA—Freedom of Information Act
FRD—Formerly Restricted Data
ISOO—Information Security Oversight Office at the National Archives and Records Administration
NARA—National Archives and Records Administration
OMB—Office of Management and Budget within the Office of Information and Regulatory Affairs of the Executive Office of the President
PM—the agency's CUI program manager
RD—Restricted Data
SAO—the senior agency official [for CUI]
TR—Transfer Request in NARA's Electronic Records Archives (ERA)

PART 2003—INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL (ISCAP) BYLAWS, RULES, AND APPEAL PROCEDURES

Subpart A—Bylaws

Sec.

Subpart B—Appeal Procedures

AUTHORITY: E.O. 13526, 75 FR 707, 75 FR 1013, 3 CFR, 2010 Comp., p. 298