BILLING CODE: 7515-01U

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2002

[FDMS No. NARA-15-0001; NARA-2015-037]

RIN 3095-AB80

Controlled Unclassified Information

AGENCY: Information Security Oversight Office, NARA

ACTION: Proposed rule

SUMMARY: As the Federal Government's Executive Agent for Controlled Unclassified Information (CUI), the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) implements the Federal Government-wide CUI Program. As part of that responsibility, ISOO proposes this rule to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program.

DATES: Submit comments on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by RIN 3095-AB80, by any of the following methods:

- *Federal eRulemaking Portal:* http://www.regulations.gov. Follow the instructions for submitting comments.

- *Email:* Regulation_comments@nara.gov. Include RIN 3095-AB80 in the subject line of the message.
- *Fax:* 301-837-0319. Include RIN 3095-AB80 in the subject line of the fax cover sheet.
- *Mail* (for paper, disk, or CD-ROM submissions. Include RIN 3095-AB80 on the submission): Regulations Comment Desk, Strategy Division (SP); Suite 4100; National and Archives Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001
- *Hand delivery or courier:* Deliver comments to front desk at the address above.

Instructions: All submissions must include NARA's name and the regulatory information number for this rulemaking (RIN 3095-AB80). We may publish any comments we receive without changes, including any personal information you include.

FOR FURTHER INFORMATION CONTACT: Kimberly Keravuori, by email at regulations_comments@nara.gov, or by telephone at 301-837-3151. You may also find more information about the CUI Program, and some FAQs, on NARA's website at http://www.archives.gov/cui/.

SUPPLEMENTARY INFORMATION: Background. The President is committed to making the Government more open to the American people, as outlined in his January 21, 2009, memorandum to the heads of executive branch agencies. However, the Government must still protect some unclassified information, pursuant to and consistent with applicable laws, regulations, and Government-wide policies. This information is called Controlled Unclassified Information (CUI).

Prior to Executive Order 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010) (the Order), 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, and unnecessarily restricted information-sharing.

As a result, the Order established the CUI Program to standardize the way the executive branch handles information that requires safeguarding or dissemination controls (excluding information that is classified under Executive Order 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.

To develop policy and provide oversight for the CUI Program, the Order also appointed NARA as the CUI Executive Agent. NARA has delegated this authority to the Director of ISOO, a NARA component.

Regulatory analysis

Review under Executive Orders 12866 and 13563

Executive Order 12866, Regulatory Planning and Review, 58 FR 51735 (September 30, 1993), and Executive Order 13563, Improving Regulation and Regulation Review, 76 FR 23821 (January 18, 2011), direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). This proposed rule is "significant" under section 3(f) of Executive Order 12866 because it sets out a new program for Federal agencies. The Office of Management and Budget (OMB) has reviewed this regulation.

Review under the Regulatory Flexibility Act (5 U.S.C. 601, *et seq.*)

This review requires an agency to prepare an initial regulatory flexibility analysis and publish it when the agency publishes the proposed rule. This requirement does not apply if the agency certifies that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities (5 U.S.C. 603). NARA certifies, after review and analysis, that this proposed rule will not have a significant adverse economic impact on small entities. However, information on the number of small entities contracting, or wishing to contract, with the executive branch that have not already implemented appropriate information systems standards for handling CUI is unreported and difficult to collect, in part because it could reflect adversely on a contractor in other ways. As a result, while NARA believes from all available information that the economic impact would be minimal, if any, we are opening this issue to public comment in addition to the content of the proposed rule, in case reviewers have additional information to the contrary that was not available to NARA.

The CUI Program provides a unified system for handling unclassified information that requires safeguarding or dissemination controls, and sets consistent, executive branch-wide standards and markings for doing so. The CUI Program has established controls pursuant to and consistent with already-existing applicable law, Federal regulations, and Government-wide policy. However, because those authorities, as well as *ad hoc* agency policies and practices, were often applied in different ways by different agencies, the CUI Program also establishes unambiguous policy, requirements, and consistent standards.

The Order establishes that the CUI Executive Agent, designated as NARA, "shall develop and issue such directives as are necessary" to implement the CUI Program (Section 4b). NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO). Consistent with this tasking, and with the CUI Program's mission to establish uniform policies

and practices across the Federal Government, NARA is issuing a regulation, to establish the required controls and markings Government-wide. There is no viable alternative to a rule for meeting the Order's mandate to establish consistent information security standards Government-wide. A regulation binds agencies throughout the executive branch to uniformly apply the Program's standard safeguards, markings, and disseminating and decontrol requirements.

The proposed rule contains a consistent program that NARA developed in consultation with affected stakeholders, including private industry and Federal agencies. While developing this program, NARA conducted working group discussions and surveys, consolidated and streamlined current practices, and developed initial drafts that underwent both formal and informal agency comment and CUI Executive Agent comment adjudication for individual policy elements.

NARA believes that this proposed rule will benefit industry that contracts with the Federal Government, including small businesses. In the present contractor environment, differing requirements and conflicting guidance from agencies for the same types of information gives rise to confusion and inefficiencies for contractors working with more than one agency or handling information originating from different agencies. A single standard that de-conflicts requirements for contractors or potential contractors when contracting with multiple Government agencies will be simpler to execute and reduce costs. Because the regulation's uniform controls derive from already-required laws, regulations, and Government-wide policies, the standards are already ones with which businesses should be complying and the impact of the rule should be minimal or non-existent.

Those entities that currently do not implement information systems security controls for CUI consistent with requirements contained in the regulation will need to make changes and

implement new practices, which could therefore have an impact on such businesses. Consistent with the Order, these requirements are based on applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology (NIST), and applicable policies established by OMB (Section 6a3). These standards, which OMB and NIST established, have been in effect for some time, and were not created by this proposed rule. Rather, the proposed rule requires use of these standards in the same way throughout the executive branch, thereby reducing current complexity for agencies and contractors. The potential impact on businesses currently not in compliance with these standards arises from the possibility that some might need to take actions to bring themselves into compliance with already-existing requirements if they are not already. From all available information, NARA believes this impact will be minimal, but reporting on non-compliance with these OMB and NIST standards is limited. If any businesses are not in compliance with these requirements, or are substantially out of compliance, the impact on those entities may be significant.

NARA has taken steps, however, to alleviate the difficulty for contractors and small businesses of complying with information systems requirements, whether they already comply or will need to comply in future. Many of the security controls contained in the NIST guidelines are specific to Government systems, and thus have been difficult for contractors to implement with their own already-existing systems. This has also limited some businesses from competing for Federal contracts. Non-Federal systems are often built using different processes from the Government-specific ones outlined in the NIST guidelines, even while achieving the same standard of protection as set forth in the Federal Information Processing Standards (FIPS). NARA has therefore partnered with NIST to develop a special publication on applying the information systems security requirements in the contractor environment. Doing so should make it easier for

businesses to comply with the standards using the systems they already have in place, rather than trying to use the Government-specific approaches currently described. This publication has already undergone one round of public comment as NIST SP-800-171 and is undergoing a second round of public comment until May 12, 2015; we expect to finalize it in June 2015.

The CUI Executive Agent is also planning a single Federal Acquisitions Regulation (FAR) clause that will apply the requirements of the proposed rule to the contractor environment and further promote standardization to benefit a substantial number of businesses, including small entities that may be struggling to meet the current range and type of contract clauses. In the process of this three-part plan (rule, NIST publication, standard FAR clause), businesses will not only receive streamlined and uniform requirements for any unclassified information security needs, but will have information systems requirements tailored to contractor systems, allowing the businesses to help develop the requirements and to be in compliance with Federal uniform standards with less difficulty than currently. Businesses that currently meet all standards will have a clearer and easier time doing so in the future with virtually no negative impact, and businesses that do not currently meet standards will be able to bring themselves into compliance more easily as well, thus reducing the potential impact coming into compliance would have on them.

Despite all of this, there may still be a significant impact on small businesses, related to bringing themselves into compliance with existing standards that will be applied uniformly under this rule. NARA does not have data on how many small businesses may be impacted by this rule, or to what degree, because such information on compliance with the standards involved is not tracked for small businesses. NARA therefore opens this topic for input from small businesses during the public comment period.

Review under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501*et seq.*)

This proposed rule does not contain any information collection requirements subject to the Paperwork Reduction Act.

Review under Executive Order 13132, Federalism, 64 FR 43255 (August 4, 1999)

Review under Executive Order 13132 requires that agencies review regulations for Federalism effects on the institutional interest of states and local governments, and, if the effects are sufficiently substantial, prepare a Federal assessment to assist senior policy makers. This proposed rule will not have any direct effects on State and local governments within the meaning of the Executive Order. Therefore, no Federalism assessment is required.

List of Subjects in 32 CFR Part 2002

Administrative practice and procedure, Archives and records, Controlled unclassified information, Freedom of information, Government in the Sunshine Act, Information, Information security, National security information, Open Government, Privacy.

For the reasons stated in the preamble, NARA proposes to amend 32 CFR, Chapter XX, by adding part 2002 to read as follows:

PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Subpart A—General Information

Sec.

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.

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 sensitive 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 the Atomic Energy Act of 1954 (42 U.S.C. 2011, *et seq*), as amended.

(c) 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.

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

(e) This part applies to all executive branch agencies that designate or handle information that meets the standards for CUI. This part also applies, by extension, to agency practices involving non-executive branch CUI recipients, as follows:

(1) Contractors handling CUI for an agency. Executive branch agencies must include a requirement to comply with Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267) (the Order), and this part in all contracts that require a contractor to handle CUI for the agency. The contractual requirement must be consistent with standards prescribed by the CUI Executive Agent.

(2) Other non-executive branch entities. When feasible, executive branch agencies should enter formal information-sharing agreements and include a requirement that any non-executive branch party to the agreement comply with the Order, this part, and the CUI Registry. When an agency's mission requires it to disseminate CUI without entering into an information-sharing agreement, the agency must communicate to the recipient that because of the sensitive nature of the information, the Government strongly encourages the non-executive branch entity to protect CUI consistent with the Order, this part, and the CUI Registry.

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

(g) 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.

(h) Nothing in this part alters, limits, or supersedes a requirement stated in laws, regulations, or Government-wide policies. Where laws, regulations, or Government-wide policies articulate the requirements for protection of unclassified information, this part accommodates and recognizes those requirements as "CUI Specified." However, where agency-specific policy or *ad hoc* practices articulate requirements for protection of unclassified information, the CUI Executive Agent has the authority under the Order to establish control policy. In such cases, this part would override such agency-specific or *ad hoc* requirements if they are in conflict.

§ 2002.2 Definitions.

Agency includes 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.

Authorized holder is an individual, organization, or group of users that is permitted to designate or handle CUI, consistent with this part.

Classified information is information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or the Atomic Energy Act of 1954, as amended, requires to have classified markings and protection against unauthorized disclosure.

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

Control level is a general term that encompasses the category or subcategory of specific CUI, along with any specific safeguarding and disseminating requirements.

Controlled Unclassified Information (CUI) is information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information (see definition of classified information, above).

CUI Basic is the default, uniform set of standards for handling all categories and subcategories of CUI. CUI Basic differs from CUI Specified in that, although laws, regulations, or Government-wide policies establish the CUI Basic information as protected, it does not specifically spell out any handling standards for that information. The CUI Basic standards therefore apply whenever CUI Specified standards do not cover the involved CUI.

CUI categories and subcategories are those types of information for which laws, regulations, or Government-wide policies requires safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.

CUI category or subcategory markings are the markings approved by the CUI Executive Agent for the categories and subcategories listed in the CUI Registry.

CUI Executive Agent 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).

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.

CUI Program manager is an agency official, designated by the agency head or CUI senior agency official, to serve as the official representative to the CUI Executive Agent on the agency's day-to-day CUI Program operations, both within the agency and in interagency contexts.

CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than this part. Agencies and authorized holders must follow the requirements in the CUI Registry. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, and sets out handling procedures.

CUI senior agency official 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 senior agency official is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI Executive Agent.

CUI Specified are the sets of standards that apply to CUI categories and subcategories that have specific handling standards required or permitted by authorizing laws, regulations, or Government-wide policies. Only CUI categories and subcategories the CUI Executive Agent approves and designates in the CUI Registry as CUI Specified may use the specified standards rather than CUI Basic standards. Agencies must apply CUI Basic standards to all CUI that is not included in a CUI Specified category in the Registry, or when a CUI Specified authority is silent

on any aspect of handling the involved CUI. CUI Specified standards 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 standards for CUI Specified categories and does not for CUI Basic ones.

Decontrolling occurs when an agency removes safeguarding or dissemination controls from CUI that no longer requires such controls.

Designating occurs when an authorized holder determines that a CUI category or subcategory covers a specific item of information and then marks that item as CUI.

Designating agency is the executive branch agency that designates a specific item of information as CUI.

Disseminating occurs when authorized holders transmit, transfer, or provide access to CUI to other authorized holders through any means.

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, 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, and the labels on them, 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.

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

Lawful Government purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities.

Legacy material is unclassified information that was marked or otherwise controlled prior to implementation of the CUI Program.

Limited dissemination is any type of control on disseminating CUI approved for use by the CUI Executive Agent.

Misuse of CUI occurs when someone uses CUI in a manner inconsistent with the policy contained in the Order, this part, and the CUI Registry, or any of the laws, regulations, and Government-wide policy that establish CUI categories and subcategories. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI.

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, local, or foreign government elements; and private or international organizations, including contractors and vendors.

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, including those within slide presentations.

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

Public release occurs when an agency makes information formerly designated as CUI available to members of the public through the agency's official release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release; nor does releasing information to an individual pursuant to the Privacy Act of 1974.

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 contract, license, certificate, or grant.

Re-use means incorporating, disseminating, restating, or paraphrasing CUI from its originally designated form into a newly created document.

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

Unauthorized disclosure occurs when individuals or entities that do not have a lawful Government purpose to access the CUI gain access to it. Unauthorized disclosure may be intentional or unintentional.

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

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

§ 2002.3 CUI Executive Agent.

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

(b) NARA's Director of the Information Security Oversight Office (ISOO) performs the duties assigned to NARA as the CUI Executive Agent.

§ 2002.4 Roles and responsibilities.

(a) The CUI Executive Agent:

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

(2) Consults with affected agencies, State, local, Tribal, and private sector partners, and representatives of the public on matters pertaining to CUI.

(3) Establishes, convenes, and chairs the CUI Advisory Council (the Council) to address matters pertaining to the CUI Program. The CUI Executive Agent 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 before agencies issue them 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 the Office of Management and Budget (OMB).

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

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

(9) Standardizes forms and procedures to implement the CUI Program.

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

(11) 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 Executive Agent.

(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 Executive Agent.

(2) Designate a CUI senior agency official responsible for ensuring agency implementation, management, and oversight of the CUI Program.

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

(c) CUI senior agency officials:

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

(2) Direct and oversee the agency's CUI Program;

(3) Designate a CUI Program manager;

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

(5) Implement an education and training program pursuant to § 2002.20 of this part;

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

(7) Develop and implement the agency's self-inspection program;

(8) Establish a process to accept and manage challenges to CUI status, consistent with existing processes based in laws, regulations, and Government-wide policies; and

(9) Establish processes and criteria for reporting and investigating misuse of CUI.

(d) The Director of National Intelligence: After consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this part with respect to the protection of intelligence sources, methods, and activities. Such directives must be consistent 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 Executive Agent maintains the CUI Registry, which serves as the central repository for all information, guidance, policy, and requirements on handling CUI, including authorized CUI categories and subcategories, associated markings, and applicable decontrolling procedures.

(b) The CUI Registry:

(1) Is the sole authoritative repository for information on CUI except the Order and this part;

(2) Is publicly accessible;

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

(4) Notes any sanctions or penalties for misuse of each category or subcategory of CUI that are included in applicable statutes or regulations.

§ 2002.11 CUI categories and subcategories.

(a) CUI categories and subcategories are the exclusive means of designating CUI throughout the executive branch. They identify unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable laws, regulations, and Government-wide policies. Agencies may not control any unclassified information outside of the CUI Program.

(b) Agencies must designate CUI only by use of a category or subcategory approved by the CUI Executive Agent and published in the CUI Registry.

§ 2002.12 Safeguarding.

(a) General safeguarding policy. (1) Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.

(2) Agency personnel must comply with policy in the Order, this part, and the CUI Registry, and review their agency's CUI policies for additional instructions. For categories designated as CUI Specified, employees must also follow the procedures in the underlying laws, regulations, or Government-wide policies that established the specific category or subcategory involved.

(3) Safeguarding measures that are authorized or accredited for classified information are also sufficient for safeguarding CUI.

(4) Pursuant to the Order and this part, and in consultation with affected agencies, the CUI Executive Agent issues safeguarding standards in the CUI Registry, and updates them as needed.

(b) CUI safeguarding standards. Agencies must safeguard CUI using one of two types of standards:

(1) CUI Basic. CUI Basic is the default set of standards agencies must apply to all CUI unless the CUI Registry annotates the relevant information as CUI Specified.

(2) CUI Specified. (i) Agencies safeguard CUI using CUI Specified standards only when the involved information falls into a category or subcategory designated in the CUI Registry as CUI Specified. In such cases, agencies should apply the specified set of standards required by the underlying authorities, as indicated in the CUI Registry.

(ii) When the authorizing laws, regulations, or Government-wide policies for a specific CUI Specified category or subcategory is silent on a safeguarding or disseminating

requirement, agencies must handle that requirement using the CUI Basic standards, unless this results in any treatment that is inconsistent with the CUI Specified authority. If such a conflict occurs, agencies follow the CUI Specified authority's requirements.

(c) Protecting CUI under the control of an authorized holder. (1) Authorized holders must have access to controlled environments in which to protect CUI from unauthorized access or observation.

(2) When discussing CUI, you must reasonably ensure that unauthorized individuals cannot overhear the conversation.

(3) When outside a controlled environment, you must keep the CUI under your direct control or protect it with at least one physical barrier. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.

(4) Agencies must protect the confidentiality of CUI that is processed, stored, or transmitted on Federal information systems consistently with the security requirements and controls established in FIPS Publication 199, FIPS Publication 200, and NIST SP 800-53.

(d) Protecting CUI not under control of an authorized holder. (1) You may use the United States Postal Service or any commercial delivery service when you need to transport or deliver CUI to another organization.

(2) We encourage you to use in-transit automated tracking and accountability tools when you send CUI.

(3) You may use interoffice or interagency mail systems to transport CUI.

(4) Mark packages that contain CUI to indicate that they are intended for the recipient only and should not be forwarded.

(5) Do not put CUI markings on the outside of an envelope or package.

(e) Reproducing CUI. (1) You may reproduce (*e.g.*, copy, scan, print, electronically duplicate) CUI in furtherance of a lawful Government purpose.

(2) When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, you must ensure that the equipment does not retain data or you must otherwise sanitize it in accordance with NIST SP 800-53.

(f) Destroying CUI. (1) You may destroy CUI when:

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

(ii) Records disposition schedules published or approved by NARA or other applicable laws, regulations, or Government-wide policies no longer require your agency to retain the records.

(2) When destroying CUI, including in electronic form, you must do so in a manner that makes it unreadable, indecipherable, and irrecoverable, using any of the following:

(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;

(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; or

(iii) Any specific destruction methods required by laws, regulations, or Government-wide policies for that item.

(g) Information systems that process, store, or transmit CUI.

(1) Agencies must apply information system requirements to CUI that are consistent with already-required NIST standards and guidelines and OMB policies. The Federal

Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 3541, et seq., requires all Federal agencies to apply the standards in FIPS Publication 199 and FIPS Publication 200. FIPS Publication 200 and OMB Memorandum-14-04, November 18, 2013, require all Federal agencies to also apply the appropriate security requirements and controls from NIST SP 800-53. All three sets of publications are free and available from the NIST website at http://www.nist.gov/publication-portal.cfm.

(2) Consistent with this already-established framework governing all Federal information systems, CUI is categorized at the moderate confidentiality impact level in accordance with FIPS Publication 199. Likewise, agencies must also apply the appropriate security requirements and controls from FIPS Publication 200 and NIST SP 800-53 consistently with any risk-based tailoring decisions. Agencies may increase the confidentiality impact level above moderate and apply additional security requirements and controls only internally; they may not require anyone outside the agency to use a higher impact level or more stringent security requirements and controls.

§ 2002.13 Accessing and disseminating.

(a) General policy. (1) 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 Executive Agent; and,

(iv) Is not otherwise prohibited by law.

(2) Agencies should impose controls only as necessary to abide by restrictions on access to CUI. Agencies may not impose controls that unlawfully or improperly restrict access to CUI.

(3) Prior to disseminating CUI, you must mark CUI according to marking guidance issued by the CUI Executive Agent.

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

(5) In order to disseminate CUI to a non-executive branch entity, you must have a reasonable expectation that the recipient will continue to control the information in accordance with the Order, this part, and the CUI Registry.

(6) When feasible, agencies should enter into a written agreement with any intended non-executive branch entity. At a minimum, such agreements must specify that:

(i) CUI remains under the legal control of the Federal Government and its misuse is subject to penalties permitted under applicable laws, regulations, or Government-wide policies;

(ii) Non-executive branch entities must handle CUI consistently with the Order, this part, and the CUI Registry; and

(iii) The non-executive branch entity must report any non-compliance with handling requirements to the disseminating agency's CUI senior agency official. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency.

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

(2) CUI Specified. You may disseminate and allow access to CUI Specified as permitted by the authorizing laws, regulations, or Government-wide policies that established that category or subcategory of CUI Specified.

(i) The CUI Registry annotates CUI categories and subcategories that contain Specified controls.

(ii) In the absence of specific dissemination restrictions, agencies may disseminate and allow access to the CUI as they would for CUI Basic.

(3) Limited dissemination. (i) You may place limits on disseminating CUI only through the use of limited dissemination controls approved by the CUI Executive Agent and published in the CUI Registry.

(ii) Use of limited dissemination controls to unnecessarily restrict access to CUI is contrary to the stated goals of the CUI Program. You may therefore use these controls only when it serves a lawful Government purpose, or you are required by laws, regulations, or Government-wide policies to do so.

(iii) You may apply limited dissemination controls to any CUI that is required or permitted to have restricted access by or to certain entities.

(iv) You may combine the approved limited dissemination controls listed in the CUI Registry to accommodate necessary practices.

(c) Methods of disseminating CUI. (1) Before disseminating CUI, you must reasonably expect that all intended recipients are authorized to receive the CUI. You may then disseminate the CUI by any method that meets the safeguarding requirements of this part and ensures receipt in a timely fashion, unless the laws, regulations, or Government-wide policies that govern that category or subcategory of CUI requires 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), you must do so consistently with the moderate confidentiality value set out in the FISMA-mandated FIPS Publication 199, FIPS Publication 200, and NIST SP 800-53.

§ 2002.14 Decontrolling.

(a) Agencies may decontrol CUI that they have designated:

(1) When laws, regulations or Government-wide policies no longer require its control as CUI;

(2) In response to a request by an authorized holder to decontrol it, if the agency is the designating agency;

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

(4) When the agency releases it in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA);

(5) Consistent with any declassification action under Executive Order 13526 or any predecessor or successor order; or

(6) When a pre-determined event or date occurs, as described in the decontrol indicators section of this part.

(b) Decontrolling may occur automatically upon the occurrence of one of the conditions in paragraph (a) of this section, or through an affirmative decision by the designating agency.

(c) Only personnel that an agency authorizes may decontrol CUI.

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

(e) Agencies should decontrol any CUI designated by their agency that no longer requires CUI controls as soon as practicable.

(f) You must remove or strike through with a single straight line all CUI markings when restating, paraphrasing, re-using, releasing to the public, or donating CUI to a private institution. Otherwise, you are not required to mark, review, or take other actions to indicate the CUI is no longer controlled.

(1) Agencies may establish policy that allows holders to remove or strike through only those markings on the first or cover page of the CUI.

(2) If you use the decontrolled CUI in a newly created document, you 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 existing agency policies on the public release of information.

(h) You may request that the designating agency decontrol certain CUI. Agency heads or the CUI senior agency official must establish processes for handling CUI decontrol requests submitted by authorized holders.

(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) You must not decontrol CUI in an attempt to conceal, circumvent, or mitigate an identified unauthorized disclosure.

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

(m) The Archivist of the United States may decontrol records transferred to the National Archives in accordance with § 2002.26 of this part, absent a specific agreement otherwise with the originating 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.

§ 2002.15 Marking.

(a) General marking policy. (1) CUI markings listed in the CUI Registry are the only control markings authorized to designate unclassified information requiring safeguarding or dissemination controls. You must mark CUI exclusively in accordance with this part and the CUI Registry.

(2) You must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it unless otherwise specifically permitted by the CUI Executive Agent or as provided below.

(3) The CUI Program prohibits using markings or practices not included in this part or the CUI Registry. Agencies must take active measures to discontinue use of any other markings, in accordance with guidance from the CUI Executive Agent. Agencies may not modify CUI Program markings or deviate from the method of use prescribed by the CUI Executive Agent in an effort to accommodate existing agency marking practices, except in extraordinary circumstances approved by the CUI Executive Agent.

(4) The designating agency determines that the information qualifies for CUI status and applies the appropriate CUI marking at the time of designation.

(5) You 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 partners thereof.

(6) The CUI Program does not require agencies to redact or re-mark documents that bear legacy markings. However, agencies must mark as CUI any information they derive from such documents and re-use in a new document, if the information qualifies as CUI.

(7) When marking is excessively burdensome, an agency's CUI senior agency official may approve waivers of all or some of the marking requirements for CUI designated within that agency. However, all CUI must be marked when disseminated outside of that agency.

(i) When CUI senior agency officials grant such waivers, they must still ensure that the agency appropriately safeguards and disseminates the CUI.

(ii) The CUI senior agency official must detail in each waiver the alternate protection methods the agency must employ to ensure protection of the CUI in question.

(iii) All such waivers apply to CUI only while in possession of employees of that agency.

(8) The lack of a CUI marking on information does not exempt the information from applicable handling requirements set forth in laws, regulations, or Government-wide policies.

(b) The CUI banner marking. You 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). You may not use alternative markings to identify or mark items as CUI.

(ii) If you include in the banner marking other authorized CUI markings in addition to the CUI control marking (as set out below), separate those elements from the CUI control marking by a single slash ("/").

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

(ii) The CUI senior agency official may approve optional use of CUI category and subcategory markings for CUI Basic, through agency policy. The policy may also address whether to include these markings in the CUI banner marking. When the CUI senior agency official has approved CUI Basic category or subcategory markings through agency policy, you may include those markings in the CUI banner marking when multiple categories or subcategories are present.

(iii) You must use CUI category and subcategory markings for CUI Specified. If laws, regulations, or Government-wide policies require specific marking, disseminating, informing, or warning statements, you must use those indicators as required by those authorities. However, you must not include these additional indicators in the CUI banner marking or portion markings.

(iv) Include in the CUI banner marking all CUI Specified category or subcategory markings; other category or subcategory markings that may apply are optional.

(v) List category or subcategory markings in alphabetical order, using the approved abbreviations listed in the CUI Registry, and separate multiple categories or subcategories from each other by a single slash ("/").

(3) Limited dissemination control markings. (i) CUI limited dissemination control markings align with limited dissemination controls established under § 2002.13(b)(3) of this part.

(ii) Designating agencies must establish agency policy that includes specific criteria for when, and by whom, they will allow the use of limited dissemination controls and control markings, and ensure the policy aligns with the requirements in § 2002.13(b)(3) of this part.

(iii) In accordance with its policy, the designating agency may apply limited dissemination control markings when it designates information as CUI and may approve later requests by authorized holders to apply them. Authorized holders may apply limited dissemination control markings only with the approval of the designating agency.

(iv) When including limited dissemination control markings in the CUI banner marking, use a double slash ("//") to separate them from the previous element of the CUI banner marking (*e.g.* "CUI//NOFORN" or "CONTROLLED/LEI//NOFORN").

(v) List limited dissemination control markings in alphabetical order, using the approved abbreviations listed in the CUI Registry, and separate them from each other by a single slash ("/").

(c) Using the CUI banner marking. (1) The content of the CUI banner marking must apply to the whole document (*e.g.*, inclusive of all CUI within the document) and must be the same on every page on which you use it.

(2) The CUI banner marking must appear, at a minimum, at the top center of each page containing CUI.

(3) For non-document formats, the container or portion of the item that is first visible must carry the banner.

(d) CUI designation indicator (mandatory). (1) All media containing CUI must carry an indicator of who designated the CUI within it. This should include:

(i) The designator's agency (at a minimum); and

(ii) If not otherwise evident, the designating agency or office via 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.

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

(2) When used, decontrolling indicators must use the format: "Decontrol On:" followed by a date or name of a specific event.

(3) If using a specific decontrolling date, list it in the format "YYYYMMDD."

(i) Decontrol is presumed at midnight local time on the date indicated.

(ii) 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.

(4) 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);

(ii) State the event title in bullet format rather than a narrative statement; and

(iii) 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.

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

(2) You may mark CUI only with portion markings approved by the CUI Executive Agent 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); and

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

(4) When using portion markings:

(i) You must 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)."

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

(iii) You must portion mark both CUI and uncontrolled unclassified portions. Indicate the uncontrolled unclassified portions by using a "(U)" immediately preceding the portion to which it applies.

(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, you 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, you must portion mark all segments separately to avoid improper control of any one segment.

(6) Each portion 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.

(g) Commingling CUI markings with classified information. (1) When you include CUI in documents that also contain classified information, you must make the following changes to the CUI marking scheme:

(i) Portion mark all CUI to ensure that CUI portions can be distinguished from portions containing classified and uncontrolled unclassified information;

(ii) Include CUI Specified category and subcategory markings in the overall banner marking;

(iii) Include the CUI control marking ("CUI") in the overall marking banner directly before the CUI category and subcategory markings (e.g., "CUI/SP-PCII"). This applies only when CUI category and subcategory markings are included in the banner;

(iv) Separate category and subcategory markings from each other by a single slash (e.g. "CUI/SP-PCII/SP-UCNI");

(v) Include all CUI limited dissemination controls with each CUI portion and in the CUI section of the overall classified marking banner, if applicable. Separate limited dissemination markings from each other by a single slash ("/"); and

(vi) Separate the entire CUI marking string for the CUI banner marking from other parts of the overall classified marking banner by using a double slash ("//") on either end.

However, if the CUI marking string is the final portion of the overall classified marking banner, do not use an ending double slash ("//").

(2) Commingling restricted data (RD) and formerly restricted data (FRD) with CUI. (i) 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, this part, and the CUI Registry, as well as the marking requirements in 10 CFR part 1045, Nuclear Classification and Declassification.

(ii) The decontrolling provisions of the Order do not apply to portions marked as containing RD or FRD.

(iii) Add "Not Applicable (or N/A) to RD/FRD portions" to the "Decontrol On" line for commingled documents.

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

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

(vi) 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.

(h) 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) "Upon Removal of Enclosure, This Document is Uncontrolled Unclassified Information"; or

(ii) "Upon Removal of Enclosure, This Document is (Control Level)."

(i) Working papers. Mark working papers containing CUI as required for any CUI contained within them and handle them in accordance with this part and the CUI Registry.

(j) Using supplemental administrative markings with CUI. (1) Agency heads may authorize the use of supplemental administrative markings (*e.g.* "Pre-decisional," "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.

(3) To be eligible for use with CUI, agencies must detail use and requirements for supplemental administrative markings in agency policy that is available to anyone who may come into possession of CUI carrying these markings.

(4) Do not incorporate or include supplemental administrative markings in the CUI markings.

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

(k) Unmarked CUI. Treat unmarked information that qualifies as CUI as described in the Order, this part, and the CUI Registry.

§ 2002.16 Waivers of CUI requirements in exigent circumstances.

(a) In exigent circumstances, the agency head or the CUI senior agency official may waive the requirements established in this part or the CUI Registry for any CUI within the

agency's possession or control, unless specifically prohibited by applicable laws, regulations, or Government-wide policies.

(b) When the circumstances requiring the waiver end, the agency must reinstitute the requirements for all CUI covered by the waiver.

§ 2002.17 Limitations on applicability of agency CUI policies.

(a) Agency policies pertaining to CUI do not apply to entities outside that agency unless the CUI Executive Agent approves their application and publishes them in the CUI Registry.

(b) Agencies may not include any requirements on handling CUI other than those contained in the Order, this part, or the CUI Registry when entering into contracts, treaties, or other agreements with entities outside of that agency.

Subpart C – CUI Program Management

§ 2002.20 Education and training.

(a) The agency head or CUI senior agency official must establish policies that address the means, methods, and frequency of agency CUI training.

(b) At a minimum, agencies must ensure that personnel who have access to CUI receive training on creating CUI, relevant CUI categories and subcategories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures. Agencies must ensure that it trains employees on these matters when the employees first begin working for the agency and at least once every two years thereafter, at a minimum.

(c) The CUI Executive Agent may review agency training materials to ensure consistency and compliance with the Order, this part, and the CUI Registry.

§ 2002.21 Agency self-inspection program.

(a) Agency heads must establish and maintain a self-inspection program to ensure compliance with the principles and requirements of the Order, this part, and the CUI Registry.

(b) The self-inspection program must include no less than annual periodic review and assessment of the agency's CUI program. The agency head or CUI senior agency official should determine frequency based on program needs and the degree of designation activity.

(c) The self-inspection program must include:

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

(2) Formats for documenting self-inspections and recording findings, when not prescribed by the CUI Executive Agent;

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

(4) A process for resolving deficiencies and taking corrective actions in an accountable manner; and

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

§ 2002.22 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 should notify the designating agency of this belief.

(b) Agency CUI senior agency officials 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 their 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 are not subject to retribution for bringing such challenges.

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

(d) If a challenging party disagrees with the response to their challenge, that party may use the Dispute Resolution procedures described in § 2002.23 of this part.

§ 2002.23 Dispute resolution.

(a) All parties to a dispute arising from implementation or interpretation of the Order, this part, or the CUI Registry should make every effort to resolve the dispute expeditiously. Disputes should be resolved within a reasonable, mutually acceptable time period, taking into consideration the mission, sharing, and protection requirements of the parties concerned.

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

(c) The CUI Executive Agent is the impartial arbiter of the dispute and has the authority to render a decision on the dispute after consultation with all affected parties, unless laws, regulations, or Government-wide policies otherwise specifically govern requirements for the involved category or subcategory of information. If a party to the dispute is also a member of the Intelligence Community, the CUI Executive Agent must consult with the Office of the

Director of National Intelligence beginning when the CUI Executive Agent receives the dispute for resolution.

(d) Until the dispute is resolved, continue to safeguard and disseminate any disputed CUI at the control level indicated in the markings.

(e) Per section 4(e) of the Order, parties may appeal the CUI Executive Agent's decision through the Director of OMB to the President for resolution.

§ 2002.24 Misuse of CUI.

(a) CUI senior agency officials establish agency processes and criteria for reporting and investigating misuse of CUI.

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

§ 2002.25 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 establishes sanctions, agencies must adhere to such sanctions.

§ 2002.26 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, place the appropriate CUI marking on the outside of the container to indicate that it contains information designated as CUI.

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

§ 2002.27 CUI and the Freedom of Information Act (FOIA).

(a) The mere fact that information is designated as CUI has no bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion.

(b) Accordingly, agencies must ensure that:

(1) They do not cite the FOIA as a CUI safeguarding or disseminating control authority for CUI; and

(2) Agency FOIA reviewers use FOIA release standards and exemptions to determine whether or not to release records in response to a FOIA request; they do not use CUI markings and designations as a dispositive factor in making a FOIA disclosure determination.

§ 2002.28 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 guidance to determine which records may be subject to the Privacy Act. However, information contained in Privacy Act systems of records may be subject to controls under other CUI categories or subcategories and the agency may need to mark that information as CUI for that reason.

Dated: April 27, 2015

DAVID S. FERRIERO

Archivist of the United States.

[FR Doc. 2015-10260 Filed: 5/7/2015 08:45 am; Publication Date: 5/8/2015]