NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2002

[FDMS No. NARA–15–0001; NARA–2016–048]

RIN 3095–AB80

Controlled Unclassified Information

AGENCY: Information Security Oversight Office, NARA.

ACTION: Final rule.

SUMMARY: As the Federal Government's Executive Agent (EA) for Controlled Unclassified Information (CUI), the National Archives and Records Administration (NARA), through its Information Security Oversight Office (ISOO), oversees the Federal Government-wide CUI Program. As part of that responsibility, ISOO is issuing 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. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.

DATES: This rule is effective November 14, 2016. The Director of the Federal Register approves the incorporation by reference of certain publications listed in the rule as of November 14, 2016.

FOR FURTHER INFORMATION CONTACT: Kimberly Keravuori, by email at *regulation_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 Web site at *http://www.archives.gov/cui/.*

SUPPLEMENTARY INFORMATION:

Background

In November 2010, the President issued Executive Order 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010) (the Order) to ''establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls.'' Prior to that time, 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 Controlled Unclassified Information (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 EA. 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 final 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.)

Although this rule is not subject to the Regulatory Flexibility Act, *see* 5 U.S.C. 553(a)(2), 601(2), NARA has considered whether this rule, if promulgated, would 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 rule will not have a significant adverse economic impact on a substantial number of small entities.

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

This final 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 rule will not have any direct effects on state and local governments within the meaning of the Executive Order. Therefore, the regulation requires no Federalism assessment.

Public Comments

General

NARA published a proposed version of this rule in the **Federal Register** on May 5, 2015 (80 FR 26501), with a 60-day public comment period ending on July 7, 2015. We received 29 written responses, totaling 245 individual comments, and numerous phone calls, email questions, and requests for information or clarification. Comments came from individuals, contractors, businesses, non-government organizations, academic and research organizations, state organizations, Federal agencies, and Representative Bennie G. Thompson, ranking member of the House Committee on Homeland Security. Most commenters, including Congressman Thompson, were in support of the CUI Program and the goals and structure of the regulation. Most also offered suggestions to clarify or revise provisions or had questions or confusion regarding particular provisions. Of particular concern to a number of commenters was the distinction between contractors and other non-executive branch entities, and the distinction between what is set out in the regulation and what will instead be contained in written agreements with agencies. We have made a number of changes to the regulation to address these and other similar topics.

Several commenters recommended we establish more stringent controls on CUI, and some commenters recommended we impose less stringent controls. We have declined to make either change. The CUI Program must balance two goals that may sometimes compete with each other—ensuring standardized controls to the extent necessary to protect information, and ensuring standardized controls to enable authorized sharing of information. We must also balance between some agencies' needs for free exchange of information with multiple partners in a wide variety of circumstances and other

agencies' needs for limitations on access to protected information, and balance the desired end result against the potential burden of re-marking documents, training staff, and similar activities. Therefore, the controls established for CUI are between the two ends recommended in many comments. However, we have revised several sections of the rule in response to both public and agency comments to more clearly explain how the different levels of CUI interact, the basis for CUI controls, what levels of control agencies may impose within the agency and outside the agency, the rules governing written agreements and information sharing, CUI marking and how to treat legacy information, destruction options, controls on dissemination, and other similar subject areas also expressed by the commenters.

CUI Security Standards and Application Outside the Federal Government

We received a few comments, primarily from academic and research entities, asserting that the safeguarding requirements required by the proposed regulation, and the guidance in the new National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations, would be too extreme and burdensome, and would cost these entities potentially a great deal of money to implement. These commenters were unable to determine a more specific estimated cost without prolonged study and assessment. However, their concerns arose primarily from the nature of their current systems—which apparently do not comply with statutory and other information security controls that already applied to Federal information before this rule was drafted, and continue to apply. Apparently, the systems are also heavily decentralized, unmonitored, and open, to enable people to work with the information across a wide range of locations and to share information and resources freely. These commenters suggested providing additional public response time to assess the burden of implementing this regulation and NIST SP 800–171 because one standard comment period was insufficient time for them to consider all the impacts of implementing the NIST standards. They also suggested lower controls or exceptions to controlling the information when in the hands of such entities, and other reductions in the security requirements for CUI while in their hands. We have declined both suggestions for the reasons described below.

The Federal Government receives a great deal of information from individuals, businesses, and other entities that it is required to protect. This is not an optional set of requirements and the burden on the Federal Government of meeting these requirements is huge. It costs the Government billions of dollars to keep its information, systems, and facilities secure. But the American people expect their Government to appropriately safeguard sensitive information, and with good reason. When the Government provides controlled information to a non-executive branch entity, sometimes pursuant to a contract or other agreement, it does not make sense for the protection requirements to disappear or lessen just because the Government has shared the information. In fact, the protection requirements do *not* disappear or lessen. The Federal Government remains obligated to ensure that the information remains protected. It would be nonsensical to require the Government to protect and control information but to simultaneously allow others to leave the same information unprotected. The dispositive issues are not who protects the information, whether it is difficult or costly to protect it, or even how one goes about protecting it; the dispositive issue is that certain laws or similar authority require the Government, and by extension, those who handle or receive it, to protect this information.

Agencies must be able to provide protected information to law enforcement organizations to facilitate criminal investigations, provide people who served in the military (or their authorized relative) with copies of their military records so they can seek benefits, provide technological specifications or demographic and other personal information to contractors and researchers developing technology or conducting studies, share information on infectious diseases and epidemics with other health organizations locally or around the world to engage in joint efforts to contain them, and more. These information-sharing needs must still occur within the parameters permitted by the laws, regulations, or Government-wide policies that govern access to the information, and must be balanced by protection requirements. Sharing that information with non-executive branch entities is easier and can occur more extensively if those entities are complying with the same levels of protection controls. As a result of these reasons, and others set out in comment responses below, we decline to reduce or eliminate this rule's protection controls for information agencies share with non-executive branch entities.

Most of these comments on burden and time did not cite burdens arising from the rule itself. Instead, they cited the burden of implementing the recently published NIST SP 800–171.

The NIST SP 800–171, incorporated by reference in this final rule, establishes guidance for protecting CUI in non-Federal systems: (1) When the CUI is resident in non-Federal information systems and organizations; (2) when the information systems where the CUI resides are not used or operated by contractors of Federal agencies or other organizations on behalf of those agencies; and (3) when the authorizing law, Federal regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory does not prescribe specific safeguarding requirements for protecting the CUI's confidentiality.

Federal Information Systems Modernization Act (FISMA), 44 U.S.C. 3541, et seq, Information Security Requirements, NIST and FIPS Standards, This Regulation, and Moderate Confidentiality Impact Value

With regard to the information security standards incorporated by reference in the rule, the framework established by FISMA requires most Federal agencies to apply the standards in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. FIPS Publication 200 requires most agencies to use NIST SP 800–53, Security and Privacy Controls for Federal Information Systems and Organizations, as the means by which agencies assess security risks to Federal information systems and select appropriate security controls and assurance requirements for them. Non-executive branch entities that manage information systems on behalf of covered agencies are subject to these rules and requirements as though they are part of the agency.

FIPS Publication 199, FIPS Publication 200, NIST SP 800–53, NIST SP 800–88, and NIST SP 800–171 are incorporated by reference into this final rule. They are free and available for download from the NIST Web site at *http://www.nist.gov/publication-portal.cfm.* FIPS Publication 199 requires covered Federal agencies to categorize their information systems in each of the security objectives of

confidentiality, integrity, and availability, including rating each system as low, moderate, or high impact in each category. This CUI rule does not mandate the use of FIPS Publication 199; FISMA establishes the requirement to use FIPS Publication 199. Nor does it incorporate the extensive standards set out in FIPS Publication 199 for how agencies go about categorizing and rating their systems, which are beyond the scope of this rule. Instead, within that already-established framework governing Federal information systems, this regulation requires agencies to secure CUI (that is on information systems) by storing and using it only on information systems the agency categorizes at no less than the moderate confidentiality impact level (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for that CUI category or subcategory prescribes specific safeguarding requirements for protecting the confidentiality of that CUI).

NIST SP 800–53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800–88, Guidelines for Media Sanitization, are also incorporated by reference because they set out methods by which agencies may sanitize equipment like photocopiers or destroy CUI to the appropriate degree.

When agencies design and manage Federal information systems, they apply the FISMA. This rule informs them that, if their systems include CUI, they must incorporate the requirement to safeguard CUI at no less than the moderate confidentiality impact value into their design and management actions (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for that CUI category or subcategory prescribes specific safeguarding requirements for protecting the confidentiality of that CUI).

Comments

Sec. 2002.1 Purpose and Scope

We received numerous comments on § 2002.1. Some asked us to clarify certain provisions, like whether the regulation applies to contractors; whether there is a difference between contractors and non-executive branch entities; when agencies must enter into contracts or other written agreements; what the difference is between contracts and written agreements, if any; whether the provisions apply to other forms of agreements, such as grants, licenses, certificates, cooperative agreements, etc.; and what recourse contractors have when handling CUI for an agency, to include sharing that information with other non-executive branch entities.

We determined from the number and scope of the comments that we needed to thoroughly revise this section to make it clearer. This section merely spells out that the regulation's scope of impact will include non-executive branch entities by means of the requirement on agencies to include contract or agreement provisions regarding CUI, when relevant. Accordingly, we have revised the language to not only state that the rule applies to only agencies directly, but to also show that by the organization of the section. We have revised the structure of § 2002.1(e) [and § 2002.16(a)(5)] to more clearly reflect this, and to clarify what agencies should do when they cannot enter into a written agreement containing a CUI handling provision of this kind.

The rule now says that it applies only to executive branch agencies, but that, in written agreements (including contracts, grants, licenses, certificates, and other agreements) that involve CUI, agencies must include provisions that require the non-executive branch entity to handle the CUI in accordance with this rule, the Order, and the CUI Registry. These written agreement provisions will also help ensure that non-executive branch entities are aware of requirements associated with handling CUI, as appropriate.

Information that non-executive branch entities generate themselves and that they do not create, collect, or possess for the Federal Government by definition does not constitute Federal CUI, nor would it fall within the provisions of a contract or information-sharing agreement covering CUI. We have slightly revised the definition of CUI under § 2002.4 to make this clearer. We agree that contracts or solicitations for projects in which CUI will not be involved should not include requirements for handling CUI. This will be handled through the FAR case and other contracting practices, rather than through this regulation. If a contractor feels CUI requirements are included erroneously, they may object through normal contracting channels. Such subjects are outside the scope of this regulation.

In response to comments regarding CNSS policies, we do not list particular applicable laws, regulations, or Government-wide policies in the regulation because listing some would create confusion regarding any not listed, and the list would be too long and would have to be updated whenever one was added, revised, or rescinded, which is not practical. However, the CUI Registry lists the categories and subcategories of CUI that laws, regulations, and Government-wide policies create or govern. When we determine whether to include a particular Government-wide policy in the CUI Registry, the primary consideration is whether that policy contains requirements for control of unclassified information. CNSS policies do not; they pertain only to classified national security information. There is no such thing as unclassified national security information, although national security systems may also contain information designated as CUI. As a result, the provision of the CUI rule regarding conflict does not apply to CNSS policies, even though they are arguably Government-wide policies. CUI policies neither require an agency to stop using the CNSS policy in deference to the CUI regulation, nor permit agencies to apply CNSS requirements to CUI outside the agency or in decisions to share the CUI.

In contrast to Government-wide policies, agency-specific policies are ones that a particular agency has promulgated for its own use and the use of those who deal with that agency (including its contractors), and that are not codified in the U.S. Code, Code of Federal Regulations, or as a Government-wide policy. However, the rule does not prohibit agencies from promulgating agency-specific policies. Agencies are still able to set out agency policies and practices within their own documents and programs, and are, in fact, expected to promulgate CUI Program implementing policies within their agency to carry out the regulation's requirements. This provision makes it clear, however, that those agency-specific policies can not conflict with the regulation, the Order, or the CUI Registry.

We also responded to comments about §§ 2002.1(i), 2002.13(d) (now 2002.16), and 2002.28 (now 2002.46), with regard to restrictions on disclosure set forth in this rule that readers could override policies that implement discovery obligations in litigation, whistleblower protections, and other lawful disclosures. The comment further expressed concern about the lack of whistleblower protection in the rule. In response to these concerns, we have revised § 2002.27 (now § 2002.44) to state that 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. We also included a Whistleblower Protection Act provision

in that same section, and we revised § 2002.22 (challenges to CUI designation; now § 2002.50) (b)(5) to allow people the option of bringing challenges to CUI designation anonymously, and to prohibit retribution for bringing such challenges.

Sec. 2002.2 Definitions (Now § 2002.4)

We received comments on several definitions within this section. One comment asked if there are restrictions on who may be an ''authorized holder,'' and pointed to provisions where it was not clear if an authorized holder should be the actor. We clarified throughout the regulation whether authorized holders or agencies are the actors. However, the rule does not specify who may be an authorized holder and we decline to add specific criteria. There are no simple, universal rules for authorized holders such as those the comment suggests (U.S. citizens, those with clearances, etc.), and the factors applicable are too multiple and cumbersome to include in a regulation. For some types of CUI, certain laws, regulations, or Government-wide policies establish who may be an authorized holder. Authorized holders may include people outside an agency who have a lawful Government purpose to have, transport, store, use, or process CUI, but also include people within an agency who must handle, process, store, or maintain CUI in the course of their jobs. Agencies differ widely in structure and size, so do not always have the same sets of staff positions or offices; designating particular people within agencies as authorized holders would thus not be practical. Lawful purposes to have CUI outside an agency also vary greatly with the differing missions of agencies and would be equally impractical to list. Agencies must therefore have the discretion to determine who is an authorized holder within the context of that agency's structure, missions, and governing authorities, and in compliance with the CUI EA's policies on handling CUI, including the requirements in this rule.

We received a number of comments on the definitions of ''CUI,'' ''CUI Basic,'' and ''CUI Specified.'' While the comments raised concerns with a variety of aspects of the definitions, they all involved confusion about the relationship of the two groupings of CUI—Basic and Specified. As a result, we have revised all three definitions to more directly explain what each kind is and how they relate to each other. We have developed a clear set of requirements for CUI Basic that is the least burdensome and superfluous possible to uniformly cover all CUI that doesn't have a law, regulation, or Government-wide policy requiring different controls. The controls for CUI Specified categories are not something we can change because they are set by the governing law, regulation, or Government-wide policy, but by ensuring that every agency applies them consistently, we reduce burdens on agencies and external partners alike. The requirements for CUI Basic do not rise to the level of requirements for classified information, and if a given type of CUI Specified has classified-level controls, those are imposed by the information's governing authority, not by the CUI Program.

Some comments expressed concern about certain categories of information that are subject to laws and Federal regulations that set out specific and detailed protection requirements for that information, and were worried that designating them as CUI would undermine those specific requirements and subject agencies and entities to legal penalties for not meeting them.

We understand the concerns raised in these comments and agree that the penalties and consequences for failing to adequately protect CUI of some types may differ significantly from failure to protect CUI of other types. That being said, we cannot adjust the definition of CUI to exclude export controlled or other protected information; the Executive Order's definition of CUI is clear and includes *all* unclassified information that laws, regulations, and Government-wide policies require to have safeguarding or dissemination controls. However, this very concern is the reason why the CUI Program includes both CUI Basic and CUI Specified groups. When we reviewed all the types of protected unclassified information that existed across the Government, and reviewed all the authorities giving rise to each type, we were very aware that some types of protected information had specific protection requirements spelled out in laws—export-related information subject to confidentiality requirements under the Export Administration Act of 1979, as amended (EAR), being one, the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) being another—and they thus could not be handled in the same manner as the vast majority of other CUI types.

CUI Basic covers the kinds of CUI that have a general requirement for safeguarding or disseminating controls, and sets a uniform set of handling requirements for all agencies to use on all types of CUI Basic. All CUI that does not have specific protections set out in a law, regulation, or Government-wide policy falls into CUI Basic categories. All CUI Basic categories will be controlled by the same standard—no less than 'moderate' confidentiality, the lowest possible control level above the 'low' standard already applied to all information systems without CUI. CUI Basic requirements are the baseline default requirements for protecting CUI, and apply to the vast majority to CUI.

However, some CUI categories and subcategories may have higher, or different, requirements from the baseline ones if a law, regulation, or Government-wide policy requires or permits other controls for safeguarding or disseminating that information. CUI Specified, in contrast to CUI Basic, recognizes the types of CUI that have required or permitted controls included in their governing authorities, and each CUI Specified category or subcategory applies those other controls as required or permitted by the governing law, regulation, or policy.

A number of CUI Specified categories are governed by laws with specific requirements and with higher penalties for failing to protect the information. We cannot exclude all of them from the definition of CUI, but we created the CUI Specified concept to reflect that these types of CUI have special requirements and should be differentiated from all other CUI.

The regulation already provides for the CUI EA to consult with industry and other private sector partners on CUI matters, at § 2002.8(a)(2), which says, ''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.'' However, we believe the comments are based in part on a misunderstanding of the CUI Registry, which already lists the categories and subcategories that constitute CUI. It is not an agency determination whether certain types of information qualify as CUI; the EA determines that a type of information qualifies as CUI when a law, regulation, or Government-wide policy requires that information's protection. That information is listed on the CUI Registry as a CUI category or subcategory and then qualifies as CUI for all agencies. Information, such as vendor proprietary information, that is not listed on the Registry does not qualify as CUI.

The authorities that establish CUI categories and subcategories were in existence before the CUI Program and this regulation, and this regulation does not change those already-existing requirements or any categories created subsequent to this rule's promulgation. Agencies and their contractors should

already be complying with the authorities governing CUI. This rule gathers a majority of CUI under one set of consistent requirements (CUI Basic), and standardizes how agencies comply throughout the executive branch, both of which reduce the cost of complying with controlled information requirements. This structure, the CUI Registry, NIST standards, and oversight functions by the CUI EA are designed to restrain over-broad application of controls on information. In addition, the CUI EA is developing a Federal Acquisition Regulation (FAR) case through the normal FAR process, for agencies to use in contracts, which will further reduce chances of overreach. However, we have revised language throughout the regulation to strengthen the admonition against over-broad application and to better distinguish between CUI Basic and CUI Specified and the types of controls applied for each.

Additional comments recommended revisions to ''misuse of CUI,'' ''non-executive branch entity,'' and ''unauthorized disclosure.'' We have accepted these comments and revised the definitions to address the concerns raised, with the exception of adding a separate definition for ''contractors and vendors'' because those entities are treated the same way as other non-executive branch entities. We declined to accept the suggestion that we remove the term ''uncontrolled'' from the definition ''uncontrolled unclassified information.'' We understand the concern that the term seems to be the same as ''unclassified information'' so the addition of ''uncontrolled'' isn't necessary and could cause confusion. However, we added the 'uncontrolled' in response to comments from other agencies that 'unclassified information' in the context of CUI was confusing. Any information that is not classified information qualifies as 'unclassified' information. However, some unclassified information qualifies as controlled information under CUI and some does not. A piece of information might be classified and uncontrolled as CUI, unclassified but controlled as CUI, or unclassified and uncontrolled as CUI. This definition refers to only that last group, so it is necessary to label it in a way that identifies that it is both unclassified and uncontrolled.

Sec. 2002.4 Responsibilities (Now § 2002.8)

A few commenters suggested revisions to the EA responsibilities under § 2002.4(a) (now § 2002.8). These recommendations included adding responsibilities such as advising appropriate Federal officials who manage and monitor the application of the CUI Program in Federal contracts, continuously engaging with NIST to ensure standards applicable to contractors remain current and minimally burdensome, and maintaining the CUI Registry so it is current. Commenters also recommended adding a provision on the CUI Advisory Council under Subpart C; formally including a representative of the Federal contracting community as a member of the CUI Advisory Council, along with representatives of other non-executive branch entities; and adding a provision that, if the EA and an agency cannot reach agreement on agency policies, the issue can be raised through OMB to the President, if necessary.

We agree with the intent of the recommendations, and the CUI EA already consults with the suggested organizations (Federal contracting officials, NIST, etc.), but we decided to combine them into one reference. Therefore, we have revised § 2002.8(a)(2) to add ''Government-wide policy bodies'' to the list of organizations with which the CUI EA consults on CUI matters. We also revised § 2002.8(a)(8) to read, ''Maintains and updates the CUI Registry as needed.''

We also accepted the recommendation to address situations in which the EA and a party cannot resolve a dispute. This contingency is fully covered in the Order and is not limited to any specific area of CUI. Rather, it applies to any issue that arises with regard to implementing the Order. Section 2002.52, Dispute resolution, already sets out the resolution process when there are disputes and includes an agency's option to appeal through the Director of OMB, to the President. However, in light of this comment, we have revised 2002.52(g) to add a provision about how to proceed if there is a conflict with the EA.

We revised the language of § 2002.8(b)(2) to require agencies to include the CUI senior agency official in agency contact listings. The agency is tasked with designating both a CUI senior agency official and a CUI Program manager. Between them, these two roles oversee the agency's entire CUI planning and implementation program, including necessary training. Agencies have already been able and encouraged to designate these positions for more than a year, in part to enable them to plan ahead for necessary training so that it will occur in a timely manner.

Sec. 2002.10 CUI Registry, and 2002.11 (Now § 2002.12) CUI Categories and Subcategories

One commenter suggested that allowing the CUI Registry to be publicly accessible could compromise security by allowing others to know about handling procedures for protected information. Another felt that the CUI Registry should not be listed as the central repository for CUI information and guidance because they believe the Registry is currently an incomplete skeleton with no useful information. And a third comment raised a concern with § 2002.12's provision that agencies may not control any unclassified information outside the CUI Program, which might mean law enforcement agencies could be prevented from establishing basic dissemination controls on their law enforcement investigative information.

The CUI Advisory Council extensively discussed and deliberated about the potential security risk of a public CUI Registry, but decided that the current approach with the CUI Registry does not present such a risk. The CUI Registry does not set out the details of how agencies implement the prescribed CUI handling requirements. It instead points to the requirements (and permissible implementation options) that exist in governing authorities or standards publications. Most, if not all, of the information in the CUI Registry is already, or will be, publicly available through laws, regulations, Government-wide policies, NIST published standards, OMB memos, agency Web sites, Freedom of Information Act (FOIA) and similar requests, public contracts and the upcoming FAR case, agency policies implementing the CUI Program, and other similar sources.

While it is true that currently the CUI Registry is incomplete in a few areas, that will change once this CUI implementing regulation becomes effective. The CUI Registry will be the central repository, as described, and the place for agencies to find up-to-date information related to carrying out CUI requirements and implementing the CUI Program.

The provision in § 2002.12 is correct as drafted. As provided in the Order, and with limited exception, agencies may not control unclassified information except consistently with the CUI Program. A law enforcement agency may control dissemination of sensitive investigative information if a law, regulation, or Government-wide policy requires or permits controls on dissemination of that kind of

information. If such authority exists, the information qualifies as CUI and the agency accordingly must (or may, if the authority permits discretion) implement controls on dissemination only to the extent and in the way required or permitted by the standards covering that kind of information. If an agency has sensitive investigative information that does not qualify as CUI—which means there is no law, regulation, or Government-wide policy that requires or permits controls on that information—then the agency cannot place controls on its dissemination. This is a question of whether the agency's authority to withhold the information is also reflected in laws, regulations, or Government-wide policies, not a question of the agency's substantive authorities or the CUI EA's authority. The EA's authority is to create a program that encompasses all the types of information a law, regulation, or Government-wide policy already requires or permits to be controlled and to establish a standardized way in which those controls are implemented across the executive branch. The CUI EA does not create the authority to control certain kinds of information; law, regulation, or Government-wide policy does.

Sec. 2002.12 Safeguarding (Now § 2002.14)

Commenters requested clarification on whether CUI Basic is the minimum for handling CUI and on the minimum requirements for physically safeguarding CUI, including the definition of a controlled environment; suggested adding the word ''timely'' to § 2002.14(a)(1); recommended revising systems ''authorized or accredited for classified information are also sufficient for safeguarding CUI'' in § 2002.14(a)(3); and asked if the terms ''CUI Basic'' and ''CUI Specified'' are required in § 2002.14(b) since the regulation references NIST SPs 800–53 and 800–171.

We have revised the language in the § 2002.4 definition of CUI, CUI Basic, and CUI Specified to clarify the distinction between CUI Basic and CUI Specified, when the requirements of each apply, and whether agencies may apply more restrictive controls. We have also revised the language of § 2002.14(a)(1) to add in the word 'timely' as recommended.

We have also revised the language in 2002.4's definition of ''controlled environment'' as recommended. However, we decline to spell out specific detailed physical requirements beyond those already included in the regulation. Instead, we have set out in the CUI Registry the requirements for CUI Basic, while applicable laws, regulations, or Government-wide policies set out the requirements for CUI Specified.

Agencies have the discretion to choose different ways to meet the single physical barrier requirement to physically safeguard a given category or subcategory of CUI. The standard requires only that it be protected in a manner that minimizes the risk of unauthorized disclosure. In addition, another comment expressed concern about meeting the requirements for a controlled environment because many contractors have moved to open workstation environments and hoteling systems, where employees working on contracts for multiple agencies whose information must be protected are in the same space. This concern is likely due to a misunderstanding of what constitutes a controlled environment. To meet the requirement for a controlled environment, any separation from unauthorized people will suffice. In a cubicle situation with employees working on different contracts, each employee's cubicle would constitute a controlled environment for purposes of preventing visual access to the CUI as long as the CUI is under that employee's control. Such cases do not require additional construction for the visual aspect; the cubicle walls are sufficient. If an unauthorized person enters the cubicle, the authorized holder can close the CUI file or trigger a screen saver to block access to the CUI. If the authorized holder leaves their cubicle within an office environment where unauthorized people may also be working, they can appropriately secure the CUI within their cubicle, for example by placing it in a locked drawer or locking their computer screen so the information is not visible. However, discussions about CUI must also not be overheard by unauthorized people. Again, this does not require construction in open work environments or hoteling systems. For example, in hoteling environments separate rooms are still made available to employees for when ''sensitive discussions'' need to take place (performance appraisals, procurement or contracting discussions, medical-related discussions, etc). However, in other cases it might be appropriate for agencies to segregate some employee operation units from others and construction (more than a cubicle wall) could be necessary. The threshold is not burdensome, and permits agencies a variety of options by which to achieve it. The standard does not necessitate construction, although in some cases construction might be the way an agency achieves the controlled environment.

With regard to the question whether we need the CUI Basic and Specified concepts in the regulation if NIST SP 800–53 or 800–171 apply, we believe we do need those terms. The regulation explains the CUI Program and the structure that includes CUI Basic, CUI Specified, the CUI Registry, and categories and subcategories. These are terms that are part of the new CUI Program. The NIST publications set out standards and details for agencies to use when they are implementing certain information security controls, regardless of what type of information is involved. The CUI Program distinguishes between CUI Basic and CUI Specified, and informs agencies of what level of protection those kinds of information need. Agencies may then meet that requirement by implementing standards spelled out in the NIST publications.

We received five comments on § 2002.14(c) and (d). We have adopted the suggestion to include an overarching statement that an authorized holder must take reasonable precautions, and to include § 2002.14(c)(1)–(4) as examples of reasonable precautions, albeit required ones. In § 2002.14(c) and (d), we decline to change optional language into requirements. Some of these items are options agencies may use, and are not required. Not all agencies have the same resources or systems, so this section informs agencies of what they may do where there are options, what they must do when there are requirements, and encourages them to do some things that are not required (such as automated tracking systems), that may not be available in all cases but that aid in better securing the CUI.

In response to the question about intelligence information, this provision in the regulation relates to section 6(d) of the Order. Section 6(d) authorizes the Director of National Intelligence to issue policy directives and guidance necessary to implement the CUI Program for the intelligence community; it does not connect with CUI categories and subcategories. The Director of National Intelligence is, in this regard, functioning for the intelligence community in a role akin to an overarching agency head who may approve agency policies to implement the CUI Program within that ''agency.''

We received several comments on § 2002.14(e) and (f), about destroying and sanitizing CUI or equipment that contained CUI. Primarily, the suggestions were to make destroying

and sanitizing methods and requirements optional, required only when practicable, or to allow alternative methods, although one comment requested that the regulation include a specific list of acceptable destruction methods. We decline these suggestions. However, due to the confusion that the comments indicated, we have revised the language on destroying CUI to more clearly articulate the required standard and the different sets of methods from which agencies may choose. The requirement is that agencies must destroy the CUI in a manner that renders it indecipherable, unreadable, and unrecoverable. Agencies must also follow any requirements for destroying CUI that are set out by laws, regulations, or Government-wide policies applicable to a given type of CUI. These are not optional or up to an agency's discretion.

However, agencies may, if no applicable authority sets out specific requirements for destroying the type of CUI involved, choose to destroy the CUI by methods contained in any of the standards cited in this subsection—those in NIST SP 800–88, those in NIST SP 800–53, or classified destruction methods. These documents are updated to be in accord with the most technologically acceptable means to render a broad range of media indecipherable, unreadable, and unrecoverable, based on its confidentiality level. These cited standards documents are sufficiently flexible to allow agencies a variety of methods for destroying CUI, while ensuring that agencies meet the underlying requirement to render the information indecipherable, unreadable, and unrecoverable.

A couple of commenters said that the rule seems to require the costly equipment needed to destroy classified information—such as equipment with memory wiping functions and designated shredders—or that agencies must destroy CUI using classified methods, particularly with regard to paper. However, this appears to be based on a misunderstanding of the provision. The required standard is to render the CUI indecipherable, unreadable, and unrecoverable. That standard does not require classified-level specialized equipment or methods required for destroying classified information, although agencies may use classified information methods if they choose. Due to issues in the past with information remaining on equipment such as copiers (which are usually leased and thus must be returned to vendors), most, if not all, agency contracts for copiers and other similar equipment that can save information on internal drives or other mechanisms must now include provisions for destroying those mechanisms or otherwise purging/sanitizing them of the information so the information is indecipherable, unreadable, and unrecoverable. That practice has become the norm for most agency equipment already, and does not require costly or specialized equipment that is required for classified information. It is also a reasonable practice to better safeguard CUI, so we decline to remove or make the indecipherable, unreadable, and unrecoverable requirement optional. The current language in the regulation provides agencies with options other than classified destruction methods. In addition to methods prescribed by any applicable law, regulation, or Government-wide policy that specifies a requirement for destroying a particular type of information, agencies may use methods in NIST SP 800–88 or methods in NIST SP 800–53. NIST SP 800–88 has clear guidance on destroying hard copy (paper and microfilms). The guidance sets out a specific particle size for cross-cut shredders, along with a particle size when an agency elects to pulverize or disintegrate paper.

The information systems requirements set out in § 2002.14(g) received a number of comments. The comments were primarily divided between concerns about application of NIST guidelines and standards, including to whom, how, and when they apply, and concerns about the moderate confidentiality impact value being applied to all CUI (some requesting that lower or higher values be allowed and others suggesting that agencies be permitted to make their own risk-based assessments on the level of protection). An additional comment recommended we clarify language in § 2002.14(g) from ''existing'' to ''applicable'' so that future laws and policies will be included. We have made this change to this provision and others within the regulation.

The purpose of the CUI Program is to provide a uniform and consistent system for protecting CUI throughout the executive branch. The baseline standard for protecting CUI Basic is moderate confidentiality. Given the need to protect CUI, a baseline of moderate confidentiality makes sense, because such protection is greater than low, the minimum requirement for all systems under the FISMA.

For situations in which agencies share CUI with non-executive branch entities that are not operating an information system on behalf of the agency, agencies should establish understandings and agreements with those entities prior to sharing CUI.

In accordance with the FISMA, *all agency heads* are responsible for ensuring the protection of Federal information and Federal information systems (''information systems 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)).

The term ''on behalf of'' means 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. To protect such systems and information, agencies must prescribe appropriate security requirements and controls from FIPS Publication 200 and NIST SP 800–53 in accordance with any risk-based tailoring decisions they make.

When non-executive branch entities are not using or operating an information system or maintaining or collecting federal information ''on behalf of'' an agency, the agency must prescribe the requirements of NIST SP 800–171 in agreements to protect the confidentiality of the CUI, unless the agreement establishes higher security requirements.

A final comment on this section noted the statement in § 2002.14(g)(2) that, ''Agencies may increase the confidentiality impact level above moderate and apply additional security requirements and controls only internally or by agreement between agencies; they may not require anyone outside the agency to use a higher impact level or more stringent security requirements and controls,'' was unclear with regard to whether it applied to CUI Basic only or both CUI Basic and CUI Specified. We have revised the provision and the definitions of CUI Basic and Specified under § 2002.4 to clarify that the moderate confidentiality level applies to CUI Basic and is a baseline level; agencies must use no less than the moderate confidentiality level for CUI Basic, and may use the high level for CUI Basic within the agency or pursuant to agreements.

By contrast, CUI Specified information may be handled at higher confidentiality levels if the authorities establishing and governing the CUI Specified category or subcategory allow or require a higher confidentiality level or more specific or stringent controls. If they do not, then the no-less-than moderate confidentiality level established for CUI Basic applies to the

CUI Specified information as well. This also holds true for other controls—if the authorities specifying controls for a given type of CUI Specified are silent or do not set out a specific standard on any aspect of safeguarding or disseminating controls, the standards and the limited dissemination controls for CUI Basic apply to that aspect of handling the CUI Specified. CUI Basic standards, including no-less-than moderate confidentiality impact value, are the default standards for CUI in the absence of an appropriate authority and CUI Specified category or subcategory listed on the CUI Registry that specifies alternative standards.

Sec. 2002.13 Accessing and Disseminating (Now § 2002.16)

Several comments on this section involved recommendations that we set out more specific criteria governing when agencies must permit access to CUI (some were concerned we would be permitting too much access and others were concerned agencies would unduly restrict access). Other commenters expressed concern or confusion about what constitutes a lawful Government purpose, similar concerns about whether it would be applied too strictly or too over-broadly, and concerns about whether an authorized holder could guarantee that dissemination would actually further the lawful Government purpose.

The rule does not require agencies to share CUI—the rule states that agencies ''should'' share CUI in certain circumstances, but recognizes agencies' broad discretion to determine whether or not to do so. Section 2002.16(a) also does not state that they should share it whenever there is a lawful Government purpose to do so and disregard all other considerations. The subsection states that agencies should share CUI if it furthers a lawful Government purpose to do so AND doing so abides by the requirements and policies contained in the authorities that established that information as CUI, and it is not otherwise prohibited by law, and the information is not restricted by an authorized limited dissemination control. One of the purposes of the CUI Program is to enable more sharing and access to protected information—when it is appropriate, given the need to protect that information to a particular degree or in particular ways—because in the past, much information that could be appropriately shared was not, due to overly applied restrictions (*see, e.g.,* Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information (August 5, 2009), pp. 7–11)). The CUI Program does not give rise to situations in which a requesting agency must be given complete access to another agency's CUI just because the requestor can cite any lawful Government purpose. But if there is a lawful Government purpose and the other restrictions, considerations, and authorities do not prohibit it, then the purpose is to enable that sharing to occur.

However, as in most areas, the rule must balance between the goal of disseminating, the goal of uniform handling, the goal of protecting information as required, and the burden and cost of implementing the Program. One aspect of that balancing act is agency mission authority. Agency heads are granted by Congress the authority to manage their agencies and to take actions to carry out their missions within the scope of the various statutes giving rise to the mission. As a result, although we are working to implement a uniform system across agencies, and agencies are by and large in support of that goal, we must also still avoid establishing policies that could interfere with an agency head's authority to run the agency and carry out the mission.

Although NARA agrees with commenters that the absence of a firm across-the-board requirement to share CUI creates some potential for unclassified information to be ''siloed'' within agencies, we do not believe that such an across-the-board requirement would be consistent with our mandate under the Order, other agencies' statutory and other authorities and responsibilities, or the broad range of decisions that agencies face daily on whether and how to share information. Agencies have expressed concern about such an across-the-board requirement.

As a result, we changed the language from a requirement to disseminate CUI as the default state so long as a lawful government purpose exists, to an option. However, we have tried to keep the balance and to minimize unnecessarily restrictive policies and practices by setting out a framework of rules within which agencies may exercise their discretion, and by providing for CUI EA review of agency policies as a means by which to reduce chances of unnecessarily restrictive dissemination policies. The rule allows challenges to designation of information as CUI as another means of reducing the chance of unnecessarily restrictive policies. Although no procedure is ever implemented completely uniformly or consistently, this regulation establishes requirements that promote significantly greater consistency than already exists. In the long run, with additional guidance and oversight on the part of the CUI EA, as the CUI program develops, the Program will be able to bring about increasing uniformity in phases and some of the current balancing difficulties will evolve into practices that more completely fulfill the Program's goals.

The rule also does not require that an authorized holder must be able to guarantee that dissemination will actually further the lawful Government purpose. It is sufficient that the person disseminating it *believes* it furthers a lawful Government purpose.

With regard to a recommendation that we revise § 2002.16(a)(2) to limit when agencies may impose controls to restrict access to CUI, we have accepted the recommendation, but not the suggested language because it was too broad and could result in agency-by-agency decisions to apply controls based on their own risk tolerance, defeating the CUI Program's purpose of establishing a uniform system. The intent is for agencies to use controls only as necessary to abide by restrictions and none that are unlawful or improper. We have revised the language in 2002.16(a)(2) to more clearly reflect this and to address other concerns raised by the commenters. It now reads, ''Agencies must impose 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.''

We also accepted a recommendation to move § 2002.16(a)(4) to another section because it addresses non-executive branch entities, not agency tasks, which is the subject of the rest of paragraph (a). We have moved the provision to § 2002.16(b)(3) under controls on disseminating CUI.

We declined to accept suggestions that allow agencies to create their own limited dissemination controls, recommendations that we revise the access requirements to require compliance with Privacy Act, PII, and protected health disclosure requirements, and a suggestion that we point to the CNSSI 1253 Privacy Overlay. The purpose of the CUI Program is to establish a uniform set of requirements for how each type of CUI is handled by every agency. Agencies may not create their own exceptions to those requirements or grant themselves agency-specific restrictions on dissemination. The CUI EA has the sole authority to determine if a limited dissemination control might be appropriate within the larger framework of CUI and the Program's purpose to establish a uniform system. The regulation already states that

dissemination and information sharing must be in accord with existing law, regulation, and Government-wide policy, so we decline to add a statement that it must be in accord with specific ones. However, the regulation also includes a section on CUI and the Privacy Act (2002.46), in which it spells out that the mere fact that information is marked CUI does not interfere with an agency making determinations about release of information protected by the Privacy Act; agencies must still abide by the Privacy Act requirements when making such determinations. The rule also includes a similar provision for FOIA, Whistleblower Protection Act, and other release authorities.

We also received several comments about § 2002.16(a)(6) (also connected with § 2002.1(e)) and the requirement to handle CUI in accord with the CUI Registry, especially when applied to contractors (as it could be through contract provisions), and a concern that contractors might receive improperly marked CUI. Compliance with the CUI Registry is woven as a requirement throughout the regulation, not just this section, as one commenter thought. The phrase ''consistent with'' or ''complies with'' and similar variations appears in several places with the phrase ''the Order, this part, and the CUI Registry.'' Anyone who is authorized to handle CUI is responsible for doing so in compliance with the requirements of the Order, this regulation, and the CUI Registry. If a contractor receives improperly marked CUI from an agency, the contractor is not responsible for having marked the CUI improperly, but the contractor could be responsible for knowing the types of CUI it receives from the agency pursuant to the contract, and for knowing which CUI Registry category the information falls into, the handling requirements for that type of CUI, and so forth. As a result, the contractor could, in some cases, also be held responsible for properly handling the CUI even if it is not marked properly when they receive it.

In § 2002.1(e) of this rule, we explain that agencies extend the controls for handling CUI to contractors by means of contract provisions (including forthcoming new FAR case on CUI), which include the requirement to abide by the rule, the Order, and the CUI Registry and which also include other provisions relating to the CUI and its controls. In Subpart C of this rule, we include a section on challenges to CUI designation and have clarified that this includes a party's belief it has received improperly marked or unmarked CUI. In addition, under § 2002.8, agencies must establish a process for recipients of CUI to raise questions of improper or no CUI markings and receive directions from the agency on what to do with the information. In some cases, the agency may be contracting for services in which the contractor would mark and otherwise manage the CUI for the agency. In such cases, the contract would very likely include provisions in which the contractor is responsible for the burden of properly marking. In other cases, the agreement would not include that provision if the task was not part of the contract.

Additional comments on § 2002.16(a)(6) included a recommendation that we note that the authorities setting out misuse of CUI or penalties are provided as part of the CUI Registry, and another that recommended we remove the reporting requirement for any incident of non-compliance with handling requirements. We decline both suggestions. Governing laws, regulations, or Government-wide policies apply to CUI and to misuse of CUI as described with those authorities. This was true prior to the CUI Program's inception, and it remains true if those authorities are not listed on the CUI Registry. However, the regulation defines the CUI Registry as the repository for agencies to find information on handling CUI, and states that the CUI categories and subcategories, along with their governing authorities, are listed there. Agencies or entities that handle a given type of CUI should make themselves familiar with the contents of the governing authorities, and the requirements for that kind of CUI, including any provisions about misuse of the CUI. And, while we agree that the reporting requirement should be included in the FAR case that is being drafted, we disagree that it should be removed from the regulation. This reporting requirement applies to anyone who handles CUI, not just contractors. Other entities would not be subject to the FAR case, so this section makes clear that a provision for that purpose must be included in any agreement, including contracts but not limited to them. The FAR case is a tool to help agencies achieve that purpose in contracts in a uniform way, but it does not establish the requirement for agencies to include that provision in their agreements. This regulation does.

Sec. 2002.14 Decontrolling (Now § 2002.18)

Several commenters asserted that, at times, decontrol is not optional, such as when the circumstances in law, regulation, or Government-wide policy that authorize information controls no longer apply to the information. We agree with these statements. While the rule requires agencies to actively manage decontrolling CUI as well as marking and handling it, and expects agencies to do so to the fullest extent they can, there are some circumstances in which they may not be able to take affirmative actions to decontrol information when it no longer qualifies as CUI. Some agencies have vast amounts of information stored in facilities or systems. In some situations, they may not have the resources to regularly sift through all of that information to determine which, if any, of it might no longer qualify as CUI. We have had to balance these competing concerns. However, this section did not clearly include automatic decontrol situations, so we have revised the language to clarify that in some circumstances, CUI may be decontrolled automatically, without review or an affirmative agency decision to decontrol the information. In such circumstances, the rule does not require agencies to take affirmative action to remove legacy markings from the information that no longer qualifies as CUI unless the agency re-uses, restates, paraphrases, releases, or donates that information.

One commenter requested that the section on removing decontrol statements be moved to § 2002.15 (now § 2002.20), under marking, as it seemed more appropriate there. We declined to do so, as we feel users will most easily find and apply all guidance on decontrol, including on removing decontrol markings, if it remains in the decontrol policy section.

One commenter requested clarification of the CUI Basic and Specified terms, in light of references made to NIST 800–53 and 800–171 guidance documents. We have revised the definitions of CUI Basic and CUI Specified in § 2002.2 (now § 2002.4), and the explanation of how they interact with NIST and FISMA requirements in § 2002.18(g), to better clarify the distinctions. The framework of CUI Basic and CUI Specified is part of the CUI Program; the NIST publications do not establish or describe it. Those publications already applied to agencies under the requirements of the FISMA before the CUI Program began, and they set out standards for information security of various types.

One commenter expressed concern about the provision prohibiting decontrol of CUI for the purpose of ''mitigating'' unauthorized disclosures. The commenter understood that this provision intended to prohibit the decontrol of CUI as a means of hiding unauthorized disclosures and avoiding

accountability for them, but suggested clarifying language to avoid certain unintended consequences with the language as it was written. We have adopted the suggested revisions.

Sec. 2002.15 Marking (Now § 2002.20)

We received a number of comments regarding the old, or legacy, marking aspects of this section in § 2002.20(a) and (b). Although the comments addressed different specific concerns, a large number of them demonstrated an underlying confusion about when agencies must remove legacy markings, when they must apply the new CUI markings, and when waivers may apply. As a result, we have substantially revised these sections to clarify the relationship between CUI markings, legacy markings, and marking waivers. A related subject concerned confusion between one provision that required designating agencies to mark CUI when designating and another provision that required agencies to mark prior to disseminating.

The basic rule is that Agencies must mark all CUI with CUI markings and must also remove all legacy markings (markings from before the CUI Program and this regulation, including FOUO, SBU, OUO, etc.) from everything. Designating agencies must mark CUI at the time they designate the information as CUI. However, marking upon designation does not address when to mark legacy information that has already been designated in the past as one of various types of controlled information (now gathered under CUI). As a result, § 2002.20(a)(1) and (3) together explain that agencies must also mark legacy information with new CUI markings, if it qualifies as CUI. In situations in which an agency has a significantly large amount of legacy material, it may waive the requirement to re-mark each item, as long as the legacy material remains within the agency, but it must still protect the information by alternate means. In addition, it must re-mark any portion of the material as CUI, if it qualifies, when the agency re-uses or disseminates information from legacy material.

We also received a comment recommending that we adopt a 'not-required-to-mark' policy for all CUI; that agencies do not have to mark CUI, but if they do, they must use the markings set out in the Program rather than agency-specific markings. The interagency review process extensively discussed marking policy and the option of not requiring marking. The conclusion was that going with a 'not-required-to-mark' policy would result in failure to properly identify unclassified information requiring control and would subject employees, contractors, partners, and other recipients of CUI to an increased likelihood of sanctions for mishandling information that laws, regulations, or Government-wide policies require them to handle as CUI.

The marking policy for CUI is not complex, however. The CUI rule allows for a simple marking of ''CUI'' or ''Controlled,'' if the CUI falls into a CUI Basic category or subcategory. The vast majority of CUI falls into CUI Basic categories and subcategories. As a result, this is the marking requirement for the vast majority of CUI. CUI Specified categories and subcategories incur additional marking requirements because they require controls that differ from all the other CUI, so the additional markings serve to identify that they are CUI Specified and what category or subcategory they belong to. As a result, authorized holders can tell at a glance that they have something that requires specific controls other than the default for CUI Basic, and what group the information falls into so they can determine what special handling that information requires. Most often, agencies that deal with CUI Specified information deal with it on a regular basis and are already intimately familiar with the requirements arising from law, regulation, or Government-wide policy for that type of information, since those requirements remain the same under this rule as in the past.

A number of comments on this section concerned waivers of the marking requirements (now re-located to their own section at § 2002.38). We recognize commenters' concerns that permitting waivers of the CUI marking requirements could affect the security of CUI and create confusion. We would prefer to keep the requirement absolute. However, some agencies already have internal storage and systems in which there is a substantial amount of information marked with legacy markings. In some cases, the number of items can be in the millions. Requiring the agency to re-mark all of that information with new CUI markings (which may also, if multiple types of legacy information are stored together, require them to go through each item to assess whether it qualifies as CUI, and which category or subcategory it falls into; not all information protected under various agency programs in the past qualifies as CUI or fits into the same groupings) may, in certain limited situations, be too burdensome for an agency's resources.

As a result, we have allowed agencies in these and similar rare circumstances to waive the requirement to re-mark that information with new CUI markings—but only as long as it remains within the agency's facilities or systems and as long as agency still safeguards the information to the required degree. However, when the agency disseminates a portion of that information outside the agency, or re-uses some of that information, it must remove legacy markings and mark that portion of the information with correct CUI markings. In § 2002.20(b)(7), the rule also requires agencies to document the waivers they implement and report them to the CUI EA. In this way, the CUI EA monitors implementation of the waiver option, may take steps to ensure waivers do not swallow the rule, and ascertains that the agencies are implementing other safeguarding practices so the protected information is not endangered.

Other comments addressed failure to mark CUI, or improperly marked CUI, and concerns that non-executive branch entities would not know that the information was CUI and would either be penalized or would have to assume a burden of control to oversee CUI marking in some manner. The requests included exempting non-executive branch entities from requirements to properly handle CUI if it isn't marked or marked properly, and creating a FAR case to address the issue. The comments raise a reasonable concern. However, we cannot exempt non-executive branch entities from the requirements to protect CUI, for the reasons explained in the beginning of the general comments discussion. The regulation does contemplate the possibility that some CUI may be unmarked or marked improperly. In such cases, agencies and non-executive branch agencies would still be subject to that CUI's governing law, regulation, or Government-wide policy's requirements, including any penalties or sanctions for not handling it properly in accord with those authorities or the connected CUI Program requirements. Entities that receive CUI from an agency should normally be on notice that they will be receiving that type of CUI information, pursuant to the terms of any contract or agreement between the two. As a result, if some of that information is not properly marked for some reason, the recipient entity should be aware that they receive certain types of CUI from the agency; the information is CUI; it falls within the agreed-upon type of CUI; and it is subject to the same handling requirements.

However, we have included in § 2002.8(c)(8) a requirement that agencies must establish a process to accept and manage challenges to CUI status (including improper or no

marking). 2002.20(m)(2) also requires agencies to establish a mechanism by which authorized holders can contact an agency representative for instructions when they receive unmarked or improperly marked information that the agency designated as CUI. We have also revised § 2002.50, Challenges to designation of information as CUI, subsection (a), to allow CUI authorized holders who believe they have received unmarked CUI to notify the designating agency of this belief through the challenge process. These provisions establish methods for reporting the improper marking or lack of marking, and will trigger the challenge process so that the situation is addressed. Misuse of CUI, as described in the definition in § 2002.4, may include no or improper marking, and subsection 2002.52 requires agencies to establish processes for reporting and investigating misuse of CUI, and requires them to report misuse of CUI to the CUI EA. This ensures agencies will look into causes of improper or lack of marking so that the causes can be addressed, and that the CUI EA can monitor trends like frequency, appropriate handling, recurring causes, etc., and determine if there is a systemic issue.

Other comments recommended including specific procedures in the rule for vetting or challenging CUI markings, allowing agencies to establish their own marking requirements, and clarifying whether agencies should mark CUI in accord with the CUI Registry or the regulation. Some commenters expressed concern that current marking technology would work for new CUI markings, and others requested we add an explanation of how markings for other types of data, such as ITAR- and EAR-controlled technical data, ''sensitive but unclassified,'' and ''for official use only (FOUO),'' will co-exist with the CUI Program. One comment requested an explanation of the status of information derived from CUI, and another suggested we add a requirement to mark the designating and disseminating agencies on all CUI.

There are competing interests inherent within the CUI Program—full consistency and uniformity vs. cost and burden. This rule attempts to balance these competing interests, and we engaged in extensive discussions with Federal agencies, state, local, and tribal groups, industry, and public interest groups as part of that balancing effort. The marking requirements were developed in consultation with the CUI Advisory Council, which gave serious consideration to the costs of implementing them. However, the marking requirements are necessary to ensure uniform handling across agencies and accomplish the goals of the Program. Agencies or others may incur costs for purchasing new marking tools, if new ones are necessary to implement the marking requirements. However, most information that requires control is already being marked in some manner, so in most cases, it would be a matter of aligning those tools with this policy.

The CUI Advisory Council considered a number of the same issues and concerns about over-broad marking as commenters raised, and determined that the kinds of suggested review procedures and practices were too onerous or were not in keeping with goals of the Program. However, there are some controls built into the program's structure. The CUI EA determines which information belongs in which categories and subcategories, whether those groupings are CUI Basic or CUI Specified, and articulates which controls or controlling authorities apply. This limits the kinds of information agencies can designate as CUI to only those vetted through that process and listed on the Registry. One set of uniform handling requirements applies to all CUI that falls into the CUI Basic category. This means that all agencies must use the same handling requirements for the vast majority of CUI, including marking. Individual agencies won't be able to establish special marking for information, so that should also help minimize over-broad marking. In addition, agencies must establish a mechanism for challenges to information they designate as CUI, so if someone believes the agency is marking over-broadly, they can raise the issue through the challenge process for scrutiny. They may make these challenges anonymously, so should not be discouraged from raising concerns. These structural elements, and other facets of the Program's structure, including CUI EA oversight of agency implementation and the ability to pursue challenges with the EA and above if not resolved at the agency level, address many of the commenters' concerns about over-broad marking and are designed in part to restrict agencies from over-broadly applying any CUI controls and policies.

The CUI EA mandates marking requirements, but agency policy implements those requirements within the agency. Agency policies that implement CUI can spell out detailed procedures when needed. However, the regulation must apply to a broad spectrum of agencies with different structures, staffing, and sizes, among other differences. As a result, detailed processes are better managed at the agency level, as long as they comply with the CUI Program's requirements and policies. In response to one commenter's suggestion that we add provisions on decontrol to the marking section, the regulation already contains a full section on decontrol of CUI and for unmarking it once it is decontrolled. We believe that marking aspects of decontrol are best addressed within the decontrol section so that all decontrol policies are easy to find in one place.

The CUI Program markings will replace other designations, such as SBU, FOUO, and OUO, and any agency-specific labels for CUI, which will all be discontinued. As a result, concerns about how they will integrate are moot. Some CUI qualifies as CUI Specified (such as export controlled information and confidential statistical information under the Confidential Information Protection and Statistical Efficiency Act) due to the existing statutory regime already established for controlling that type of information. While some types of CUI Specified may arise primarily in only one or a couple of agencies, those types of CUI do not become agency-specific types of CUI simply for that reason. The categories or subcategories for those types of CUI Specified have gone through CUI EA vetting, have underlying laws, regulations, or Government-wide policies establishing them, are listed on the CUI Registry, and include specified controls that apply uniformly throughout the executive branch, to any agency that has that type of information. This is different from an agency developing its own category of protected information, or its own policy or practice for handling protected information, such as the various SBU and FOUO regimes that currently exist from agency to agency.

Regarding the questions about derived CUI, the bottom line is that certain types of information qualify as CUI. If an item of information qualifies as CUI, it doesn't matter whether it is in some way also derived from another item of information that qualifies as CUI, and it should be marked as CUI either way. Its status as CUI depends upon the information itself and whether it meets the requirements in a law, regulation, or Government-wide policy that establish it as needing controls on safeguarding or disseminating. A document containing CUI that is derived from another document that contains CUI would also be CUI—because it contains controlled information, not simply because it is derived from a document that contains CUI. It is possible the original document contains both CUI and non-CUI and the derived document could therefore contain only information derived from

the non-CUI portions of the original document. In such a case, the derived document would not become CUI simply because the information was derived from a CUI document.

The fact that a certain item of CUI derives from another item of CUI becomes relevant primarily in the context of marking waivers for legacy CUI. This is because the rule states that an agency's waiver, for re-marking as CUI certain items of legacy information, ceases for one or more of those items when the agency re-uses them. So, if an agency is not re-marking certain legacy CUI because that CUI is under a marking waiver, and it then uses in another item some controlled information from within that legacy CUI—*i.e.* it derives CUI from the legacy item—then the new item containing the derived CUI does not fall under the waiver (even though the originating legacy CUI item does) and the agency must properly mark the derived item as CUI. A similar requirement would apply to CUI derived from an unmarked or improperly marked item of CUI as well, although in that case the original item should then be properly marked as well once it is clear it contains CUI.

With regard to suggestions that we add marking requirements for designating and disseminating agency information and dates, the regulation already includes a provision within § 2002.20 that requires marking the designating agency. We do not see a reason to add an extra marking for the disseminating agency. Likewise, we decline to require a date marking on all CUI, as another commenter suggested. This was previously discussed during the inter-agency development process, but not adopted. Practically speaking, much CUI will have a date apparent, though it is not required. However, there is no required decontrol time period, so this issue is much different in a CUI context than the need for a date within a classified information context.

Sec. 2002.16 Waivers of CUI Requirements in Exigent Circumstances (Now Part of § 2002.38)

Several commenters recommended that we add a provision requiring agencies to report any waivers to the CUI EA, both when the agency issues the waiver and when it rescinds it. We agree, and revised the section to require CUI senior agency officials to retain records on each waiver and use them to report the waivers to the CUI EA.

Another commenter expressed concern that waivers could be used over-broadly to avoid complying with CUI requirements and suggested we add a provision that limits waivers to the shortest period and narrowest scope necessary to account for the exigent circumstances. The comment also expressed concern that waivers could not accord with prescriptive language in 2002.12 CUI categories and subcategories. We accepted the idea of language limiting the waivers and revised the section to require agencies to reinstitute CUI requirements for all CUI covered by the waiver without delay when circumstances requiring the waiver end. However, we disagree that this section generally conflicts with the requirements of 2002.12 CUI categories and subcategories.

Sec. 2002.27 CUI and Information Disclosure Requests (Now § 2002.44)

One commenter questioned whether a CUI designation really has ''no bearing'' on decisions to release or not to release information in response to a FOIA request. The Order explicitly states that the mere fact that an item is CUI has no bearing on disclosure determinations under release statutes such as FOIA. Agencies make determinations about whether to release, or to exempt from release, under the FOIA solely on the basis of FOIA criteria and considerations. This rule, or the fact that something is CUI, does not change the basis upon which agencies must make FOIA determinations.

Agencies may determine that certain documents are exempt from release under FOIA that also qualify and are marked as CUI, but the CUI status does not cause or influence that determination. The FOIA allows Federal agencies to withhold information prohibited from disclosure by another Federal statute pursuant to exemption 3 in the FOIA (5 U.S.C. 552(b)(3)). In some cases, a given item of information may qualify as CUI on the basis of one of those same Federal statutes. However, the decision whether to release or withhold such information in response to a FOIA request would still be based on the requirements under which the FOIA exemption 3 may apply, rather than its status as CUI. Based on the comment, we have revised 2002.44 to better clarify this.

Sec. 2002.22 Challenges to Designation of Information as CUI (Now § 2002.50)

One commenter requested that we revise this section to include challenges about improperly marked or unmarked CUI and challenges to waivers. The commenter also sought clarification regarding whether the challenge procedures are available to recipients outside of the Government. We have revised this section to clarify that all authorized holders, whether within or outside of the Government, may challenge CUI designations, and to reflect that they may bring a challenge because they believe CUI is improperly marked or unmarked.

Conclusion

We have thoroughly and carefully considered all the comments and have attempted to clearly explain in this supplementary information section some of our reasoning and changes to the regulation since it was proposed, in hopes of better conveying the scope and nature of the CUI Program and its requirements to those who had questions or concerns. We appreciate the comments and the effort individuals and organizations made to craft them and to think about the CUI Program and the implications of the regulation's provisions. The comments helped us refine the rule into a much better regulation and one that more clearly explains the Program and its requirements. We realize any new program brings change, and that those changes can be confusing, can seem inconsistent or incompletely thought out, and can appear to be hugely burdensome or unnecessarily complicated at first encounter. We hope that we have alleviated much of those concerns by our responses to these comments and the changes to the regulation. However, if you have additional questions or would like more information, please visit our CUI Web site at *http://www.archives.gov/cui/* or contact us directly.

We have had to make compromises to the goal of complete or absolute uniformity in deference to the need to balance between several competing, legitimate interests and to develop a Program and requirements that can work for a variety of agencies and types of information, as well as those who receive CUI from agencies. However, we believe strongly that, in the course of those efforts and all the input, discussions, comments, and work contributed by our partners on the CUI Advisory Council and at NIST, agency and industry experts who generously consulted with us, and the many industry, business, organizational, and individual reviewers, we have been able to develop a sound CUI Program that significantly increases uniformity throughout the executive branch, appropriately protects CUI while encouraging sharing and access when appropriate, and does so with the least amount of burden, complexity, and change possible.

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, Incorporation by reference, Information, Information security, National security information, Open government, Privacy.

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

PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Subpart A—General Information

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

Subpart B—Key Elements of the CUI Program

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

Subpart C—CUI Program Management

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

Appendix A to Part 2002—Acronyms

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

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.* ''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. 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 re-marking 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 re-use) 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 re-marking 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)

Dated: August 30, 2016.

David S. Ferriero,

Archivist of the United States.

[FR Doc. 2016–21665 Filed 9–13–16; 8:45 am]

BILLING CODE 7515–01–P