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