INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

CUI Notice 2018-01: Guidance for Drafting Agreements with Non-Executive Branch Entities involving Controlled Unclassified Information (CUI)

January 24, 2018

Purpose

This notice provides clarifying guidance and recommendations for conveying CUI Program requirements in information sharing agreements involving CUI that do not fall under the upcoming CUI Federal Acquisition Regulation (FAR). This guidance addresses agreements with non-executive branch entities and is not intended to provide guidance for sharing with foreign entities.

Authorities

32 CFR 2002, Controlled Unclassified Information, September 14, 2016; and

Executive Order 13556, Controlled Unclassified Information, November 10, 2010.

Background

The Director of the Information Security Oversight Office (ISOO), exercises Executive Agent (EA) responsibilities for the CUI Program. The CUI Federal regulation at 32 CFR 2002 implements Executive Order 13556 on CUI, and establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, including the following:

- When disseminating or sharing CUI with any non-executive branch entity, agencies should enter into written agreements or arrangements when feasible. These agreements or arrangements are to include CUI provisions. See §§ 2002.16(a)(5)-(6).

- When an agency entered into an information sharing agreement prior to implementation of the CUI requirements, the agency should modify any terms in that agreement that conflict with the CUI Program, when feasible. See §§ 2002.16(a)(5)(iv).

Definitions

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. See § 2002.4(c).

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. See § 2002.4(q).

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, 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. See § 2002.4(gg).

Content of Agreements

By regulation, agreements with non-executive branch entities must include provisions that state:

- Non-executive branch entities must handle CUI in accordance with Executive Order 13556, 32 CFR 2002, and the CUI Registry (see §§ 2002.16(a)(5)(i) and (6)(i));

- Misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies (see § 2002.16(a)(6)(ii)); and

- The non-executive branch entity must report any non-compliance with handling requirements to the disseminating agency using methods approved by that agency's CUI SAO. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency (See § 2002.16(a)(6)(iii)).

Recommendations

In addition to the regulation-required provisions listed in the section above, ISOO also recommends, as best practices, that non-executive branch entity agreements:

- Identify the categories or subcategories of CUI that the non-executive branch entity will be expected to handle or transmit in connection with the agreement, along with any specific handling, safeguarding, or dissemination requirements stipulated in the underlying laws, regulations, or Government-wide policies;

- Identify where agreement performance will take place (i.e., Government facilities or non-executive branch entity facilities);

- Identify the type of equipment (information systems, etc.) that will be used to process, store, or transmit the CUI, along with the applicable technical requirements that must also be used to protect the CUI:

    - Federal information system: Agency information systems are Federal information systems. When a non-executive branch entity operates an information system *on behalf of* an agency, that system is also a Federal information system and is subject to the requirements of 32 CFR 2002 as though it is the agency's system. Agencies

may require these systems to meet requirements the agency sets for its own internal systems. See § 2002.14(h)(1).

- Non-Federal information system: A non-Federal information system is any information system that does not meet the criteria for a Federal information system. 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. 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. See § 2002.14(h)(2).

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 defines the requirements necessary to protect CUI Basic on non-Federal information systems. 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). See § 2002.14(h)(2);

- Whether Government-furnished equipment will be used; and

- Any disposition or destruction requirements.

Mark A. Bradley

MARK A. BRADLEY
Director