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 2019-04: Oversight of the Controlled Unclassified Information (CUI) Program within Private Sector Entities

September 6, 2019

Authorities

1. Executive Order 13556, *Controlled Unclassified Information* (November 10, 2010); and

2. 32 Code of Federal Regulations 2002, *Controlled Unclassified Information* (September 14, 2016).

Applicability

3. CUI Program requirements apply to all executive branch departments and agencies, and to all private sector entities that handle, process, or store CUI through the use of agreements or arrangements (*See 32 C.F.R. Part 2002.4(c)).*

Purpose and Background

4. Federal agencies have made significant strides in implementing the CUI Program, established by Executive Order (E.O.) 13556, *Controlled Unclassified Information*, over the past 12 months. This progress allowed agencies to begin determining how they will effectively oversee the program not only within their agency, but with private sector entities that, through their agreements with the federal government, necessitate the handling of CUI.

5. The Director of the Information Security Oversight Office (ISOO) exercises Executive Agent (EA) responsibilities for the federal CUI Program. Through the program's implementing regulation at 32 Code of Federal Regulations (C.F.R.) Part 2002, ISOO has established the program's requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI. These requirements apply to all executive branch departments and agencies, and to all private sector entities that handle, process, or store CUI through agreements or arrangements. Agencies have requested that ISOO issue guidance to assist them as they begin conducting oversight of private sector entities that have entered into agreements or arrangements with them.

6. On January 24, 2018, The CUI Executive Agent issued CUI Notice 2018-01, Guidance for Drafting Agreements with Non-Executive Branch Entities involving Controlled Unclassified Information. This notice provides clarifying guidance and recommendations for conveying CUI Program requirements in information sharing agreements involving CUI. This guidance addresses agreements with non-executive branch entities and is not intended to provide guidance for sharing with foreign entities.

7. Throughout FY18 and FY19, ISOO worked closely with the General Services Administration (GSA), the National Aeronautical and Space Administration (NASA), and the Departments of Homeland Security (DHS) and Defense (DoD) to develop a subpart for the CUI Program

within the Federal Acquisition Regulation (FAR). Once published, the new subpart will standardize how executive branch agencies convey safeguarding requirements for CUI to private sector entities. ISOO anticipates the CUI Program will be incorporated in FAR in FY20.

8. The following sections provide guidance on overseeing implementation of the CUI Program within private sector entities for agencies, based on requirements in the CUI implementing regulation (32 C.F.R. Part 2002).

Oversight of Private Sector Entities

9. The agency CUI Senior Agency Official (SAO) is responsible for oversight of the agency's CUI Program implementation, compliance, and management. *See 32 C.F.R. Part 2002.8(b)(2)*. This should include adequate oversight over CUI entrusted to private sector entities through the use of agreements or arrangements. The agency CUI SAO may:

    a. Delegate internal component or sub-agencies with responsibilities related to the oversight of the handling of any CUI entrusted to private sector entities through the use of agreements or arrangements; and

    b. Enter into agreements with other executive branch agencies, authorizing or allowing oversight actions of any CUI-entrusted private sector entities through the use of agreements or arrangements.

Reciprocity

10. Agencies are encouraged to enter into interagency agreements and arrangements to avoid duplicative and unnecessarily burdensome oversight actions. Each agency is responsible for ensuring that security assessments and audit activities are held to the minimum necessary to effectively oversee compliance. Instances of duplicative or unnecessarily burdensome oversight actions should be reported by private sector entities to the applicable agency CUI program office. Private sector entities should inform the CUI EA should such instances remain unresolved.

CUI Oversight at the Department of Defense

11. As the Executive Agent for the National Industrial Security Program (NISP), the Department of Defense (DoD) has long exercised oversight of cleared defense contractors under that program to ensure the proper safeguarding of classified information. DoD also provides industrial security services to 33 other federal departments and agencies. The NISP's scope is limited to classified information, and the community of private sector entities handling CUI is broader and larger than those in the NISP. As a starting point for CUI oversight, DoD has elected to begin conducting assessments of major defense contractors that are contractually obligated to protect CUI under Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 7012 clause), or through other contractual obligations and agreements. DoD's authority to do so is based on its obligation to ensure effective oversight of the

agency's CUI Program and is restricted in scope to the CUI Program's regulatory requirements, and enforcement of the DFARS 7012 clause and other agreements and arrangements (as defined in 32 C.F.R. Part 2002.4(c)).

12. As agencies ramp up their CUI implementation efforts, the program's oversight landscape will continue to evolve; this is equally true for DoD as its program grows across the defense industrial base. Thus, we understand this is only a starting point, but an important one for private sector entities that handle CUI to ensure they protect this information adequately within the existing regulatory framework and pursuant to those requirements.

13. DoD should make every effort to streamline and consolidate its CUI oversight to reduce the time, burden, and cost on private sector entities. This should include appropriate coordination among DoD components that exercise oversight authorities to conduct such oversight jointly in order to limit the number of assessments and reduce the burden on private sector entities, whenever feasible. The methodology for these assessments should be consistent and shared, as appropriate, with stakeholders, including private sector entities. It is also highly recommended that planning and collaboration pertinent to the oversight and assessment process take place. Finally, DoD should promulgate a clear, concise, and centralized communication plan for the implementation and oversight of CUI programs of private sector entities.

Please direct any questions regarding this Notice to the CUI EA at cui@nara.gov.

Mark A. Bradley

MARK A. BRADLEY
Director