A Brief Introduction to CUI and NIST 800-171

COGR

June 8, 2017
Where are we and how did we get here?

- EO 13556 (Nov, 2010)
- NIST 800-171 (June, 2015) with Dec 2016 revision
- 32 CFR 2002 (Dec, 2016)
- December 31, 2017 NIST 800-171 full implementation DFAR
- CUI Registry (2015)
- DFAR 252.204-7012 (Oct, 2016 revision)
- DHS proposed rule (Jan, 2017)
- FAR and other Agency clauses TBD
CUI Defined

- “Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.”
  - 23 categories and 84 subcategories
  - Basic and specific security levels dependent on category/subcategory (NIST 800-171)
  - Standardized Markings (information provided by government to contractors should be marked).

(https://www.archives.gov/cui/about)
CUI Categories

- Agriculture
- Controlled Technical Information
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Geodetic Product Information
- Information Systems Vulnerability Information
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- NATO
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- SAFETY Act Information
- Statistical
- Tax
- Transportation

This is not a Research Only Issue!
The CUI Control Marking is mandatory for all CUI and may consist of either the word "CONTROLLED" or the acronym "CUT" (at the designator's discretion). As an optional best practice, the CUI Banner Marking may be placed at the bottom of the document as well. Below are two examples showing the options for the CUI Banner Marking.

MANDATORY:
CUI Banner Markings must appear on the top portion of the page.

CONTROLLED

Department of Good Works
Washington, D.C. 20006

August 27, 2016
MEMORANDUM FOR THE DIRECTOR
From: Elliott Alderson, Chief
Robotics Division
Subject: Examples
We support President Walker by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Optional Best Practice: Also Placed Centered at Bottom

CUI

Department of Good Works
Washington, D.C. 20006

August 27, 2016
MEMORANDUM FOR THE DIRECTOR
From: Tyrell Wellick
Office of the CTO
Subject: Examples
We support President Walker by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

CUI Specified Category Marking

CONTROLLED/SP-SPECIFIED

Department of Good Works
Washington, D.C. 20006

August 27, 2016
MEMORANDUM FOR THE DIRECTOR
From: Gary Walsh
Chief, Cargo Division
Subject: Examples
We support President Walker by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

NOTE: The above examples use the words "SP-SPECIFIED" and "BASIC" as substitutes for CUI Category and Subcategory Markings. Consult the CUI Registry for actual CUI markings.

CUI Basic Category Marking (if authorized in agency policy)

CUI/BASIC

Department of Good Works
Washington, D.C. 20006

August 27, 2016
MEMORANDUM FOR THE DIRECTOR
From: Robert Loblaw, Esq
Office of the General Counsel
Subject: Examples
We support Congressman Love by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Reference: 32 CFR 202.20(b)(1)
NIST 800-171

- Establishes information security standards and guidelines for protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations

- Is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies), but not when nonfederal organizations are operating information systems on behalf of the government.

- Requirements apply only to components of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components.
14 families of Controls

- Access Controls
- Awareness and training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident response
- Maintenance
- Media Protection
- Personnel Security
- Physical protection
- Risk Assessment
- Security assessment
- Systems and communication protection
- System and information security

110 individual controls; many with high impact or resource intensive.
When is NIST 800-171 Applicable?

- Information is identified in NARA registry category or subcategory
- There is a federal nexus:
  - Contract (e.g., DFAR 252.204-7012 non-FRE contract)
  - Data Use Sharing Agreement
Identifying and Engaging Stakeholders

- IT (central and local)
- Provost office
- Sponsored Programs (contracting and costing)
- Student Services
- Immigration Services
- Business Services
- Others?