The NARA Rule and NIST SP 800-171

Erin B. Sheppard
Phillip R. Seckman
J. Quincy Stott

March 9, 2017

Overview

- Executive Order 13556
- NARA's Controlled Unclassified Information Rule
- NIST SP 800-171 Requirements
- Status of the Upcoming Final FAR Rule

Executive Order 13556

Purpose of the Executive Order

- EO issued on November 4, 2010
- The Underlying Problem:
  - Agencies' ad hoc, agency-specific, policies and procedures
  - Result: patchwork of inconsistent marking and safeguarding of documents
- EO Purpose:
  - Establish a uniform program for managing information that requires safeguarding or dissemination controls
  - Excludes classified information
  - Referred to as "controlled unclassified information" (CUI)

Controlled Unclassified Information Program

- EO designates the National Archives and Records Administration (NARA) as executive agent
- CUI Program created to standardize how executive branch handles information that requires safeguarding or dissemination controls
  - Required each agency to review categories or marking used to designate unclassified information
  - Approved categories and subcategories of CUI "to be applied uniformly throughout the executive branch"
  - Authorized to develop and issue directives as are necessary to implement this order
    - "This order shall be implemented in a manner consistent with . . . applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology . . . ."
- NARA developed a CUI Registry reflecting CUI categories and subcategories

Three-Part Plan

- To carry out Executive Order 13556 and the CUI Program, NARA asked to complete three steps:
  - (1) A proposed rule regarding treatment of CUI
  - (2) NIST publication
  - (3) FAR clause

NARA's Controlled Unclassified Information Rule

Final Rule

- Issued September 14, 2016
- Regulations at 32 CFR Part 2002
  - Provides for safeguarding, accessing and disseminating, decontrolling, and marking of CUI
- Not directly applicable to government contractors
  - "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"
- Predictive of what contractors who handle CUI can expect in a
  - Future FAR clause or
  - Tailored clause in Sections H or I

Required Agreement Content

- At a minimum, agreements with non-executive branch entities must:
  - Require handling CUI in accordance with the EO, CUI regulations, and the CUI Registry
  - Provide for penalties as established in applicable laws, regulations, or Government-wide policies
  - Require reporting of any non-compliance with handling requirements
- Exceptions are unlikely to apply to government contractors

Definition of CUI

- "[I]nformation 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."
- Law, regulation, or government-wide policy must require or permit controls
  - Agencies cannot implement controls other than those consistent with the CUI Program

Designating CUI

- Requires an authorized holder to determine that a specific item of information falls into a CUI category or subcategory
  - Authorized holder is an individual, agency, organization, or group of users permitted to designate or handle CUI
  - Aimed at creating greater uniformity in classification
- Must make recipients aware of the information's CUI status
  - Through uniform marking convention (more on this later)

CUI Registry

- Authoritative central repository for all guidance, policy, instructions, and information on CUI
- Agencies and authorized holders must follow CUI Registry instructions
- Includes CUI categories and subcategories, markings, decontrolling procedures, and other guidance
  - Registry does not explicitly identify the required safeguarding obligations
  - Instead, it contains cross-references to the safeguarding/dissemination authority giving rise to its classification as CUI
  - Also identifies whether the category or subcategory is subject to basic or specified safeguarding requirements

CUI Basic and CUI Specified

- Law, regulation, or Government-wide policy may require or permit agencies to issue safeguarding or dissemination controls in 3 ways:
  - (1) CUI Basic: requiring or permitting agencies to control or protect the information, but providing no specific controls
    - Uniform set of controls in 32 CFR Part 2002 and CUI Registry based on NIST SP 800-171 (though not expressly requiring application of all 800-171 controls)
    - Agencies may not require controls for CUI Basic at a higher level when disseminating outside the agency
  - (2) CUI Specified: requiring or permitting agencies to control or protect the information and providing specific controls for doing so
    - CUI Registry indicates which laws, regulations, and Government-wide policies include specific requirements
    - May be more stringent or simply differ from CUI Basic controls (e.g., all 800-171 controls)
  - (3) Hybrid: specifying only some of the controls, which makes the information CUI Specified, but with CUI Basic controls where authority does not specify


NATIONAL ARCHIVES
Blogs · Bookmark/Share · Contact Us
Search Archives.gov
Search
RESEARCH OUR RECORDS
VETERANS' SERVICE RECORDS
EDUCATOR RESOURCES
VISIT US
AMERICA'S FOUNDING DOCUMENTS
Controlled Unclassified Information (CUI)
Home > Controlled Unclassified Information (CUI) > Registry - Categories and Subcategories
Controlled Unclassified Information
Use the CUI logo
Contact Us
About CUI
Key Elements of CUI
Chronology and History
FAQs
CUI Registry
Categories-Subcategories
Category-Subcategory Markings
Limited Dissemination Controls
Decontrol
Policy and Guidance
Glossary
CUI Reports
CUI Training
CUI Additional Tools
Registry - Categories and Subcategories
***** IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT *****
Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.
Search the Registry
GO
CUI Categories and Subcategories
• Select a Category or Subcategory to view associated detail information.
• An asterisk (*) indicates that Safeguarding, Dissemination, Marking and/or Decontrol measures that differ from General Guidelines are required by statute, regulation, or Government-wide policy for some or all control authorities..
• Unless noted, CUI may be controlled at the Category or the Subcategory level.
Category
Category Description

CUI Categories and Subcategories

- Select a Category or Subcategory to view associated detail information.
- An asterisk (*) indicates that Safeguarding, Dissemination, Marking and/or Decontrol measures that differ from General Guidelines are required by statute, regulation, or Government-wide policy for some or all control authorities..
- Unless noted, CUI may be controlled at the Category or the Subcategory level.

Category	Category Description
Agriculture	Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.
Controlled Technical Information*	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
Critical Infrastructure Subcategories: • Ammonium Nitrate • Chemical-terrorism Vulnerability Information* • Critical Energy Infrastructure Information • DoD Critical Infrastructure Security Information • Physical Security* • Protected Critical Infrastructure Information* • Water Assessments	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
Emergency Management	Related to information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.

CUI Registry: Controlled Technical Information

Category-Subcategory: **Controlled Technical Information**

Category Description: Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Subcategory Description: N/A

Marking: CTI

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012	Specified	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

Controlled Unclassified Information

Use the CUI logo
Contact Us

About CUI
- Key Elements of CUI
- Chronology and History
- FAQs

CUI Registry
- Categories-Subcategories
- Category-Subcategory Markings
- Limited Dissemination Controls
- Decontrol
- Policy and Guidance
- Glossary

CUI Reports
CUI Training
CUI Additional Tools

CUI Registry: Critical Infrastructure

Category-Subcategory:	**Critical Infrastructure**
Category Description:	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
Subcategory Description:	N/A
Marking:	CRIT

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
Presidential Policy Directive 21	Basic	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

Safeguarding

- CUI Registry provides safeguarding standards through CUI Basic, CUI Specified, or other hybrid/tailored requirements
  - Controlled technical information example: CUI Specified links to DFARS 252.204-7012, safeguarding covered defense information and cyber incident reporting
  - The Registry is a starting point for tracing necessary controls and may require multiple levels of review to ensure compliance
  - Like the DFARS rule, other authorizing rules may require specific, concrete controls that are identified only by cross reference in the CUI registry
- Goal: minimize risk of unauthorized disclosure, but allow timely access by authorized holders

Safeguarding cont.

- Authorized holders must take **reasonable precautions**
  - Establish controlled environments
  - Prevent access or observation of CUI by unauthorized individuals
  - Provide at least one physical barrier; protection when outside a controlled environment
  - Protect CUI processed, stored, or transmitted on federal information systems
- Additional CUI safeguarding requirements connected with
  - Shipping or mailing
  - Reproduction
  - Destruction

Safeguarding cont.

- Non-federal information systems
  - NIST 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
  - Exception: the CUI Registry provides specific safeguarding requirements
  - FAR Rule is likely going to be the source of uniformity across agencies (to the extent such uniformity is achieved)
    - Absent such an approach, contractors subjected to the rule will have to continue a fairly detailed agency-by-agency review process

NIST SP 800-171 Requirements

Development

- Two rounds of public comment
- Issued in June 2015
- Updated on December 20, 2016
  - Minor changes mostly; larger change regarding system security plans
- Focused on alleviating impact of requirements on nonfederal organizations
  - Specific to nonfederal information systems and organizations
  - Avoids government-specific approaches, while extracting transferable parts
    - FIPS Pub 199
    - FIPS Pub 200
    - NIST SP 800-53
- Includes security requirements using the systems and practices contractors already have in place
- NARA and NIST developed SP 800-171 collaboratively as part of CUI Program

Structure

- “Basic” security requirements—obtained from FIPS Pub 200, which includes the high-level and fundamental security requirements for federal information systems
- “Derived” security requirements—supplements to basic security requirements, taken from NIST SP 800-53’s security controls

Requirements—14 Families

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information security

Implementation Considerations

- Develop implementation plan
  - Prioritize “long lead” requirements
  - Utilize NIST 800-53 prioritization categories
  - Identify as soon as possible security controls that are inapplicable/otherwise addressed by compensating controls
- Designate a responsible POC for revising/updating plan
  - Utilize cross-functional team members (cyber, compliance, contracts, business development, legal) to address issues and track efforts

Implementation Considerations cont.

- Consider isolating into separate security domain information systems or components for processing, storing, and transmitting CUI
- Many controls allow for reasonable contractor discretion
  - 3.1.8 – Limit unsuccessful logon attempts
  - 3.4.8 – Blacklisting and whitelisting both permitted
  - 3.5.8 – prohibit password re-use for specified number of generations (neither number nor generation length set)
  - Double-edged sword
- Appendix D maps NIST 800-171 controls with NIST 800-53, use NIST 800-53 as guide as needed

Status of the Upcoming Final FAR Rule

3 Stages Culminating with the FAR

- In addition to the NARA final rule implemented at 32 CFR Part 2002 and NIST SP 800-171, NARA will issue a standard FAR clause
  - "NARA, in its capacity as the CUI Executive Agent, also plans to sponsor in 2016 a single Federal Acquisition Regulation (FAR) clause that will apply to requirements contained in the proposed federal CUI regulation and Special Publication 800-171 to contractors."
- Benefits
  - Provide clear direction to contractors
  - Promote standardization across agencies
- FAR 52.204-21 is likely to be supplanted
- Open Questions:
  - How will basic compare to current FAR Basic Safeguarding requirements
  - Will there be a low/moderate/high format, or just two levels of safeguarding

Questions?

Erin B. Sheppard

(202) 496-7533

erin.sheppard@dentons.com

Phillip R. Seckman

(303) 634-4338

phil.seckman@dentons.com

J. Quincy Stott

(303) 634-4316

quincy.stott@dentons.com