McKenna Government Contracts,
continuing excellence at Dentons

DENTONS

The NARA Rule and NIST SP 800-171

March 1, 2016

Phillip R. Seckman
Michael J. McGuinn

Overview

- Executive Order 13556
- NARA Controlled Unclassified Information Rules
- Protected Information Categories
- NIST SP 800-171 Requirements
- Proposed FAR Rule

Executive Order 13556

Executive Order 13556

- EO issued on November 4, 2010
- Underlying problem: agencies employed ad hoc, agency-specific policies and procedures, resulting in patchwork of inconsistent marking and safeguarding of documents
- Purpose was to establish a uniform program for “managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies,” excluding classified information
  - Referred to as “controlled unclassified information”
  - Aligns with DFARS CDI clause “catch-all” provision

Controlled Unclassified Information Program

- **EO designates the National Archives and Records Administration (NARA) as executive agent to implement the EO**
- **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"
  - NARA 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 will execute three steps:**
  - (1) A proposed rule regarding treatment of CUI
  - (2) NIST publication
  - (3) FAR clause

NARA CUI Rules

CUI Proposed Rule

- **Proposed Rule: Controlled Unclassified Information, 80 Fed. Reg. 26,501-01 (May 8, 2015)**
- **Purpose: establish required controls and marking for CUI government-wide**
  - Regulation needed to bind all executive branch agencies
- **Benefit for federal contractors**
  - Differing requirements and conflicting guidance from agencies for the same types of information
  - A single standard will simplify execution and reduce costs
  - NIST and OMB standards have been in effect prior to the proposed rule, so NARA claims it is merely codifying requirements with which contractors should already be in compliance
    - Recognizes that if companies are “substantially out of compliance,” the impact on those entities may be significant.

CUI Proposed Rule

- **Executive branch agencies must include a requirement to comply with Executive Order 13556 and the proposed NARA regulations (to be located at 32 C.F.R. § 2002.1 et. seq) in all contracts that require a contractor to handle CUI for the agency**
- **When feasible, rule requires executive branch agencies to enter into formal information-sharing agreements**
  - Any non-executive branch party to the agreement will be required to comply with the Order, proposed regulations, and the CUI Registry

CUI Proposed Rule: Safeguarding

- **“Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.”**
  - Agencies must safeguard CUI using one of two types of standards:
    - CUI Basic—default set of standards applicable to all CUI
    - CUI Specified—specific handling standards required or permitted by law, regulation, or policy
- **Safeguards authorized for classified information are sufficient to safeguard CUI**

CUI Proposed Rule: Safeguarding

- **Authorized holders must protect CUI from unauthorized access or observation**
  - Avoid conversations unauthorized individuals can overhear
  - Outside controlled environment, keep CUI under direct control or protected by at least one physical barrier
  - Federal information systems required to use security requirements and controls
    - FIPS Pub 199
    - FIPS Pub 200
    - NIST SP 800-53

CUI Proposed Rule: Safeguarding

- **Agencies should disseminate and permit access to CUI**
  - Impose controls only as necessary to abide by legal restrictions regarding access to CUI
  - Caution: "In order to disseminate CUI to a non-executive branch entity, you must have a reasonable expectation that the recipient will continue to control the information in accordance with the Order, this part, and the CUI Registry."
    - Written agreements preferred

Identifying Protected Information – UCTI vs. CDI vs. CUI

Prior DFARS Clause

- **Unclassified Controlled Technical Information (UCTI)**
  - Issued on November 18, 2013
  - New contract clause: DFARS 252.204-7012
    - Applied to any contractor information system that “may have” UCTI resident on or transiting through it
  - UCTI
    - Technical information
    - “Controlled” technical information
- **Safeguarding requirements**
  - 50+ security controls from NIST SP 800-53
- **Reporting of cyber incidents**
- **Flow down to subcontractors**

New Covered Defense Information Interim Rule

- **Replaced prior UCTI rule**
- **Issued on August 26, 2015**
- **Applies to all contractors with "covered defense information" (CDI) transiting their information systems**
  - Focus on CDI significantly expands the scope of the prior UCTI clause's safeguarding and reporting requirements
- **New safeguards**
  - Adequate security
  - NIST SP 800-171
- **Increased rapid reporting**
- **Cloud computing**

Covered Defense Information

- **(1) Unclassified information provided to contractor by or on behalf of DOD in connection with contractor performance**
- **(2) Information collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of contract performance, and**
- **(3) Information in one of these four categories:**
  - Controlled technical information
  - Critical information (operations security)
  - Export-controlled information
  - “Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies”

Relationship to CUI Proposed Rule

- **CDI definition includes CUI**
  - Unclassified information in connection with contract performance
  - Information in support of contract performance
  - Catch-all category; “requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies”
  - Expanded definition + broad flow down requirement means CDI clauses govern virtually all DOD contractors at both prime and subcontract levels
- **CDI interim rule in DFARS**
  - Limited to contracts governed by DFARS
  - CUI proposed rule is a backstop for non-DOD agencies
- **Move toward uniformity**
  - Revised CDI clause relies on NIST SP 800-171
  - DOD + NARA = shift toward consistency

NIST SP 800-171 Controls

Development

- **Two rounds of public comment**
- **Finalized in June 2015**
- **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

Don’t forget NFO Requirements!

Requirements – Catch-All

- **Other IS security protections required when contractor:**
  - "Reasonably determines"
    - Business discretion?
  - That additional IS security measures "may be required to provide adequate security in a dynamic environment"
    - "Adequate security:" protection commensurate with probability/consequences of loss, misuse, unauthorized access, or information modification
    - "Dynamic:" adequacy must be constantly assessed/updated
  - Based on an "assessed risk or vulnerability"
    - Requires an understanding of known risks
    - Look-back period?

NIST 800-171 Sets the Baseline

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
    - This is a **mandatory** proposal submission – no provision for seeking deviation once you’ve otherwise made DFARS 252.204-7008 proposal representation
- **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
- **Develop standard 30-day disclosure identifying non-compliances with NIST 800-171 update as appropriate (DFARS 252.204-7012(b)(ii))**

Will you be able to implement NIST 800-171 security requirements by December 31, 2017?

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**

Implementation Considerations – Relationship with UCTI Security Controls

- **CDI requirements from NIST 800-171 vs. UCTI clause requirements from NIST 800-53**
  - Certain UCTI clause requirements are not required by NIST 80-171 (e.g., PM-10)
  - Many CDI clause controls are not requirements of the UCTI clause
    - UCTI clause imposed approximately 60 security controls
    - NIST 800-171 has north of 250 (NFO included)
- **For purposes of implementation, consider treating two sets of requirements as complementary**
  - Can leverage existing UCTI compliance as appropriate
- **Consider contract modification for new contracts containing CDI clause by relying on existing UCTI security compliance to support "adequate security"**

Proposed FAR Rule

3 Stages Culminating with the FAR

- **In addition to the NARA proposed rule 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
- **Until the forthcoming FAR clause becomes operative, contracting officers and federal contractors may reference CUI requirements and NIST SP 800-171 in civilian contracts**
- **Final FAR rule currently with OIRA**

Questions?

Phillip R. Seckman

(303) 634-4338

phil.seckman@dentons.com

Michael J. McGuinn

(303) 634-4333

mike.mcguinn@dentons.com