McKenna Government Contracts,
continuing excellence at Dentons

DENTONS

DOD's New Cyber Requirements:
Impacts on DOD Contractors and Subcontractors

Phil Seckman
Mike McGuinn
Quincy Stott

Dentons US LLP

Date: January 5, 2016

Agenda

- Regulatory landscape
- DOD’s covered defense information (CDI) interim rule
  - History
  - Requirements
  - Issues
  - Supply chain compliance
- Compliance and breach response final considerations

Regulatory Landscape

- Contractors faced with patchwork of legal requirements
  - Federal Information Security Management Act of 2002
    - Primarily applicable to government information systems, but also to contractors
    - Federal Information Security Modernization Act of 2014
      - Signed into law on Dec. 18, 2014
      - New requirements likely forthcoming regarding reporting of major incidents and agency breaches
  - Industry/agency-specific requirements (e.g., DOD (including CDI Clause), NASA, GSA, DOE)
  - SEC disclosures for material cyber incidents
  - HIPAA requirements
  - FTC treatment of breaches as unfair trade practices
  - State-specific breach notification laws
  - International requirements
  - Private sector requirements (e.g., PCI DSS)

Clause requirements overlay and increase compliance obligations

DFARS Unclassified Controlled Technical Information (UCTI) Clause

- Issued on Nov. 18, 2013 (78 Fed. Reg. 69,273)
  - Established new contract clause: DFARS 252.204-7012
- Clause included in all DOD contracts issued after Nov. 18, 2013
  - Applies to small business and commercial item contracts
  - Applies to any contractor information system that “may have” UCTI resident on or transiting through it
- UCTI
  - “Technical Information”
    - Technical data or computer software
  - “Controlled” Technical Information
    - Military or space application
    - Subject to controls on access, use, modification, release
    - Marked with required distribution statement pursuant to DOD Instruction 5230.24, Distribution Statements on Technical Documents

DFARS UCTI Clause Requirements

- (1) Safeguarding requirements:
  - Compliance with 50+ security controls from NIST SP 800-53
    - E.g., access control, awareness and training, incident response
  - Must otherwise explain
    - Why security control is inapplicable, or
    - An alternative control or protection achieves equivalent protection
- (2) Reporting of cyber incidents
- (3) Flow down to subcontractors

New DOD Covered Defense Information Rule

- Interim rule: Network Penetration Reporting and Contracting for Cloud Services
- Issued on Aug. 26, 2015 (80 Fed. Reg. 51,739-01)
  - New rule effective immediately
    - Per rule, all DOD contracts issued after Aug. 26, 2015 include the clause
  - Rule applies to commercial item and small business contractors
- Applies to all contractors with “covered defense information” transiting their information systems
- Second interim rule issued on December 30, 2015 (80 Fed. Reg. 81472-74) contains key clarifications to the CDI rule

Justifications for the Interim Rule

- Urgent need to protect covered defense information
- Lack of awareness of the full scope of cyber incidents committed against defense contractors
- Proliferation of cloud computing has increased vulnerability of DOD information on both DOD and DOD contractor systems
- Information gathering—through expanded reporting requirements—for future improvements in cybersecurity policy
- “Recent high-profile breaches of Federal information show the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts.”

Key Points from DOD Interim Rule

- (1) Scope
  - Covered defense information – definition significantly expands the scope of the prior UCTI clause's safeguarding and reporting requirements by focusing on all "covered defense information" (CDI)
- (2) New safeguards
  - Internal contractor information systems containing covered defense information subject to new safeguarding requirements
- (3) Increased reporting
  - Expanded cyber incident reporting obligations to DOD
- (4) Cloud computing
  - New requirements related to the acquisition of cloud computing services

Issue #1: Scope

- New clause “Safeguarding Covered Defense Information and Cyber Incident Reporting” (DFARS 252.204-7012) applies more broadly to all “covered defense information”
- Covered defense information means
  - (1) Unclassified information provided to contractor by or on behalf of DOD in connection with contract 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, and
    - “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 (e.g., privacy, proprietary business information)”
- Key point: the expanded definition, plus broad flow down requirement, means the revised clauses will apply to virtually all DOD contractors at both prime and subcontract levels.

Issue #1: Scope (cont.)

- Requirements of rule apply to “covered contractor information system”
  - Information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information
- Applies to contractor’s internal information systems
  - Contrast with contractor system operating on DOD’s behalf (e.g., data hosting services, cloud service providers), which are subject to more significant requirements
    - Contractor systems operated on behalf of DOD subject to specific contractual requirements (including DOD Risk Management Framework (formerly DIACAP))
  - OMB draft guidance issued in August 2015 provides further support for distinction between contractor internal systems vs. information systems operated on behalf of the government
    - OMB’s distinction was based on internal system used to provide product or service that is incidental to the product or service being provided
- Type of system drives the requirements imposed – CDI clause is the baseline

Issue #2: Safeguards

- The rule requires adequate security for all covered defense information
- Adequate security includes:
  - NIST SP 800-171 for covered contractor information systems
  - Other security measures when contractor reasonably determines they may be required to provide adequate security based on an assessed risk or vulnerability
- Compliance under first interim rule was required when contract is awarded
- DOD on December 30, 2015 issued a second interim rule (80 Fed. Reg. 81472)
  - Rule gives contractors until December 31, 2017 to fully implement NIST 800-171 controls
    - "As soon as practical, but no later than December 31, 2017."
  - Contractor to notify the DoD CIO, via email within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award

Issue #2: Safeguards (cont.)
NIST Standards Shift

- Prior UCTI regulations security controls were based on NIST SP 800-53
- The revised DFARS 252.204-7012 clause relies on NIST SP 800-171
  - NIST SP 800-171 is specifically tailored for protecting sensitive information residing in contractor information systems
    - Refines requirements from Federal Information Processing Standard (FIPS) 200
- NIST SP 800-171 maps substantially with NIST SP 800-53, but significant differences exist
- Benefits to NIST SP 800-171
  - Increases protections of government information in contractors' possession
  - Reduces contractors' burdens by eliminating some federal-centric requirements in NIST SP 800-53

Issue #2: Safeguards (cont.)
NIST Standards Shift

- New NIST standards adopted by DOD signal a shift towards consistency
- National Archives and Records Administration (NARA) issued a proposed rule in May 2015 that would adopt NIST SP 800-171 to safeguard controlled unclassified information
- Office of Management and Budget (OMB) recently proposed guidance that would adopt NIST SP 800-171

Issue #2: Safeguards (cont.)
Alternative to Non-Compliance

- DFARS clause, Compliance with Safeguarding Covered Defense Information Controls (DFARS 252.204-7008), requires contractors to make certain representations:
  - (1) Company will implement NIST 800-171 requirements not later than December 31, 2017
  - (2) If company proposes to vary from any NIST 800-171 requirements, submit a written explanation of:
    - (A) Why a particular requirement is not applicable
    - (B) How an alternative, but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection
  - Representative of DOD CIO will "adjudicate" contractor requests to deviate from NIST SP 800-171 prior to contract award

Issue #3: Reporting Requirements

- Contractors must “rapidly report” cyber incidents to DOD
- “Cyber incident” means “actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.”
- Contractors must
  - Report cyber incidents related to covered defense information
  - Report any cyber incident that may affect “operationally critical support”
  - Review any evidence that covered defense information was compromised
- Subcontractors must rapidly report cyber incidents directly to DOD and the prime
  - Second interim rule issued on December 30, 2015 does not change obligation to rapidly report

Issue #4: Cloud Computing

- Interim rule added DFARS Subpart 239.76 to implement policy for acquisition of cloud computing services
  - Importantly, DOD may only award contracts for cloud computing services to contractors with provisional authority to operate from the Defense Information Systems Agency (DISA)
- Contract clause “Representation of the Use of Cloud Computing” (DFARS 252.239-7009)
  - Allows contractor to represent its intention to utilize cloud computing services in performance of the contract
  - If a contractor later proposes use of cloud computing services—and did not indicate that in the offer prior to award—the contracting officer must approve
- Contract clause “Cloud Computing Services” (DFARS 252.239-7010)
  - Provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements

Consequences of Noncompliance

- Consequences of noncompliance include
  - Breach of contract
  - Termination for default
  - FCA liability (no express certification currently required)
  - Negative past performance evaluations
  - Declination of options (USIS)
  - Suspension and debarment
  - Purchasing system disapproval
- Government likely to review non-compliances in the context of a breach and with benefit of hindsight
  - Contractor reasonableness likely to be touchstone for penalties
  - Documentation of decision-making crucial
  - DOD likely to have concerns about implementation approach that begins with specific safeguarding controls before the audit/detection controls (evades reporting requirement)

Supply Chain Issues

- The following covered defense information contract clauses are mandatory flow downs in certain subcontracts, regardless of size
  - DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Information
  - DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- Subcontractors are also required to flow down the clauses to lower-tier subcontractors
- Many subcontractors may be unable or unwilling to comply with these requirements

Supply Chain Issues (cont.)

- Second interim rule issued on December 30, 2015 provides the clause must only be flowed down to *certain* subcontractors
  - Revises the DFARS § 252.204-7012(m) flow-down requirements to mandate inclusion of the clause in subcontracts where the subcontractor will be providing “operationally critical support” and/or where subcontract performance “will involve a covered contractor information systems.”
- Clause must be flowed down without alteration, except to properly identify the parties
- Subcontract reporting must occur directly to DOD and the prime contractor

Supply Chain Issues (cont.)

- Prime contractor responsibility for flowing down clauses
  - Clauses do not require prime contractor to conduct assessment or verify system adequacy of subcontractors
  - Obligation is on party receiving covered defense information to explain
    - Why security control is inapplicable OR
    - That an alternative control achieves equivalent protection
- Government likely to argue prime contractors are responsible for ensuring adequate protection of covered defense information, wherever located
  - Government Furnished Information ("GFI") under DFARS 252.227-7025 requires contractors to indemnify government and third parties for violations of GFI use and disclosure restrictions
    - Applies to any person/entity to whom contractor has released or disclosed GFI
  - Similar also to government property systems
    - FAR 52.245-1(f) makes contractors responsible for ensuring subcontractors have adequate property management systems in place for GP (including CAP)

Supply Chain Issues (cont.)

- Higher-Tier Contractor Options
  - Conduct some form of system verification through audit
    - Significant risks associated with approving subcontractor system compliance
  - Require subcontractor representation of compliance
    - Unlikely to get it, then what?
  - Require written explanation from sub consistent with DFARS 252.204-7008 and DFARS 252.204-7012 that
    - (1) security control is inapplicable or
    - (2) an alternative control achieves equivalent protection
  - Establish contract mechanisms for system audit rights, NDA and indemnification for breaches/challenges
    - DFARS 252.227-7025 as guide
  - Educate suppliers
    - Develop checklist or “target profile” of requirements and provide to subcontractors
    - Make resources available to subcontractors (DHS “C Cubed” program, SBA training)
  - Emphasize reporting requirements and preservation of data
  - Flow down clause and do nothing more

Supply Chain Issues (cont.)

- Higher-Tier Contractor Options (cont.)
  - If contractor learns that subcontractor cannot/will not comply with clause requirements, prime should
    - Find a compliant subcontractor
    - Preclude subcontractor from handling covered defense information
    - Identify/document the subcontractor's security capabilities and ask subcontractor to attest to the adequacy of those capabilities
      - Any other factors showing trustworthiness
      - Confirm prompt reporting is in place
  - Take care in integrating subcontractor cyber compliance into procurement system as you are likely to be audited to it

Touchstone will be reasonableness

Supply Chain Issues (cont.)

- Subcontractor Options
  - Determine whether you are in fact a subcontractor
    - Potentially difficult to support: ISPs and other external service providers are subcontractors according to preamble of the UCTI rule
  - Assess whether you need covered defense information for performance of your subcontract
    - Given the broad scope of the definition, unlikely to avoid
    - Attempt to resist inclusion of clause or reach agreement that it is inapplicable if covered defense information will not be provided/created
  - Clarify existence of covered defense information
    - Does this subcontract require me to receive or generate covered defense information?
    - Don’t assume – ask, and get specificity before award
  - Limit/control covered defense information locations
    - Centralize covered defense information in network with controls, no copies elsewhere
    - Hard copies
    - Possible to use higher-tier contractors networks directly?

Supply Chain Issues (cont.)

- Subcontractor Options (cont.)
  - Self-assess compliance with covered defense information controls
    - If not in compliance, do you have adequate controls in place to address your company's cyber risks?
    - Are these controls tied to covered defense information requirements? Focus on NIST SP 800-171
    - Can you reasonably and accurately represent that controls are inapplicable or that you have equivalent controls?
    - Avoid broad representations or over-promises of system compliance
  - Ensure disclosures are controlled
    - Limit prime contractor's ability to access systems for purposes of reporting cyber incident (government only)
    - Consider NDA with enforceable provisions to ensure information disclosed to the prime is protected from further disclosure outside of the covered defense information context

Cyber compliance likely to be significant competitive advantage for suppliers

Company Compliance: Final Considerations

- Know what data/information you have and the applicable requirements
- Obtain management buy-in, proactive approach
- Have a plan in place providing guidance if crisis develops
- Supply chain considerations
  - Symantec report: small businesses are “path of least resistance”
  - Required security profile vs. supplier’s current profile?
  - Are you protected from liability/indemnified for subcontractor issues?
  - Are supplier obligations to notify, respond, cooperate/share information properly defined?
- Commercial companies and small businesses likely not exempt
- Document risk management decisions and compliance efforts
- Read your contracts!

Questions?

- Phil Seckman
  - (303) 634-4338
  - phil.seckman@dentons.com

- Michael J. McGuinn
  - (303) 634-4333
  - mike.mcguinn@dentons.com

- Quincy Stott
  - (303) 634-4316
  - quincy.stott@dentons.com