The FAR Basic Safeguarding Rule

Erin B. Sheppard, Partner
Michael J. McGuinn, Counsel

December 8, 2016

Agenda

- Regulatory landscape
- FAR Rule
  - History
  - Requirements
  - Harmonization
  - Subcontract issues
- What's next?

Regulatory Landscape

- Contractors faced with patchwork of legal requirements
  - FISMA
  - Industry/agency-specific requirements (e.g., DOD, NASA, GSA, DOE)
  - SEC disclosures for material cyber incidents
  - HIPAA requirements
  - FTC treatment of breaches as unfair trade practice
  - State-specific breach notification laws
  - International requirements
  - Private sector requirements (e.g., PCI DSS, subcontract requirements)

The Proposed FAR Safeguarding Rule

- Proposed rule (77 Fed. Reg. 51,496 (Aug. 24, 2012))
  - Done under authority of FISMA
  - Proposed rule intended to be broadly applicable to information systems containing non-public information provided by or generated for the government
- Rule contained security standards applicable to various information security areas:
  - Use of public computers or websites
  - Transmission of electronic information
  - Transmission of voice/fax information
  - Physical and electronic barriers
  - Sanitization
  - Intrusion protection
  - Transfer limitations
- Basis for security controls unclear

The Final FAR Safeguarding Rule

- Effective June 15, 2016 (81 Fed. Reg. 30,439 (May 16, 2016))
- Intended to establish a basic level of safeguarding for all federal government contractors
- "Intent is that the scope and applicability of this rule [will] be very broad."
  - Prime and subcontract level
  - Commercial items (but not COTS)
  - Small businesses

Applicability

- Applies to contractor information systems that process, store, or transmit “federal contract information”
  - Nonpublic information “that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government”
    - Contract must be for development or delivery of product or services
    - Information need not be
- No marking requirements

Applicability (cont.)

- Information “provided by” the government would include any government-furnished information
- Information “generated for” the government would cover:
  - Any information required by a CDRL
  - Technical data
  - Cost data (labor rates, indirect costs)
  - Project controls reporting/EVMS data
- Does not include “simple transactional information, such as necessary to process payments”

Requirements

- Intended to create a baseline of controls for federal contractors
  - Other controls (e.g., DOD) will overlay
- Imposes 15 different security requirements on contractors
  - Selected from NIST 800-171 “basic and derived” controls
  - Compliance with all 100+ controls not required
  - Controls are static, not cross-referenced to NIST 800-171
- No grace period for implementation; controls mandatory at the time of award

Requirements (cont.)

- Required controls:
  - Limit system access to authorized users
  - Limit system access to the types of transactions/functions users are permitted to execute
  - Verify/control/limit connections to external systems
  - Control publicly accessible information
  - Identify users, devices, or processes
  - Authenticate or verify user identifies prior to permitting access to information systems
  - Sanitize or destroy information system media
  - Limit physical access to authorized individuals
  - Escort visitors and monitor visitor activity; maintain audit logs of access

Requirements (cont.)

- Required controls (cont.):
  - Monitor and protect organization communications at external and key internal boundaries
  - Implement subnetworks for publicly accessible system components that are physically/logically separated from internal networks
  - Identify, report, and correct information and information system flaws in a timely manner
  - Protect from malicious code
  - Update malicious code protection mechanisms
  - Perform periodic/real-time scans of information system and files

The FAR Safeguarding Rule – Requirements (cont.)

- Controls do not include:
  - Security policies and procedures
  - Training requirements
  - Multi-factor authentication
  - Incident response plans
  - Tracking of incidents internally and externally
  - Control of removable media/prohibition on use of portable storage devices
  - Personnel screening
  - Security assessments
  - Prohibition of password reuse

Relationship to DOD Rule

- DFARS CDI clause requires compliance with all 15 FAR clause requirements
  - Contractors should prioritize implementation of FAR controls in any implementation plan
- FAR rule more limited than DFARS rule
  - No cyber incident reporting
  - No grace period
  - No pre-award representation of compliance/use of alternative approaches
  - No post-award disclosures of non-compliances
  - No broad government audit/access right

Supply Chain Issues

- Prime contractor responsible for flowing down clauses – but who will government hold responsible for incident?
- Possible prime contractor approaches:
  - Conduct some form of system verification through audit
  - Require subcontractor representation of compliance
  - Establish contract mechanisms for system audit rights, NDA and indemnification for breaches/challenges
  - Educate suppliers
  - Flow down clause and do nothing more

Supply Chain Issues (cont.)

- If contractor learns that subcontractor cannot/will not comply with clause requirements, prime should:
  - Find a compliant subcontractor
  - Preclude subcontractor from handling federal contract information (if possible)
  - 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

Supply Chain Issues (cont.)

- Subcontractor “avoidance” options:
  - Determine whether you are in fact a subcontractor
  - Assess whether you need/will have federal contract information
  - Attempt to resist inclusion of clause or reach agreement that it is inapplicable
  - Clarify existence of covered defense information (if applicable)
  - Limit/control covered defense information locations (if applicable)
- Self-assess compliance with FAR clause controls and develop implementation plan
  - FAR rule likely the first step
  - “A prudent business person would employ this most basic level of safeguarding, even if not covered by this rule.”

Consequences of Noncompliance

- Source selection impacts
  - *But see Discover Technologies LLC,* GAO B-412773
- Breach of contract
  - Termination for default
  - FCA liability (no express certification currently required)
  - Negative past performance evaluations
  - Declination of options (USIS)
  - Suspension and debarment

Final Considerations

- Know what data/information you have and applicable requirements
- Obtain management buy-in, proactive approach
- Have a plan providing guidance if crisis develops
- Consider supply chain considerations/partner
- Document risk management decisions and compliance efforts
- More developments coming
- Read your contracts!

What's Next?

- Additional FAR rule forthcoming in conjunction with NARA program for controlled unclassified information (CUI)
  - Final NARA rule (32 C.F.R. Part 2002) confirms that a forthcoming FAR clause will extend the federal CUI security controls to contractors
  - The FAR rule will require contractors dealing with CUI to implement at least some subset of the NIST SP 800-171 controls
  - FAR Council will look to NIST SP 800-171 as source for any mandatory controls for CUI basic and CUI specified information, as established in the CUI Registry
  - The timeline of the forthcoming FAR rule remains uncertain
- Contractors would be wise to prepare a plan for implementation of both the CUI basic and CUI specified controls

Questions?

Erin B. Sheppard
202-496-7533
erin.sheppard@dentons.com

Michael J. McGuinn
303-634-4333
michael.mcguinn@dentons.com

Thank you

Dentons US LLP
1900 K Street, NW
Washington, DC 20006-1102
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.