Quality People.
Quality Projects.

New FAR And DFARS Cybersecurity Requirements for Federal Contractors: What You Need to Know

Reginald M. Jones ("Reggie")
Chair, Federal Government Contracts Practice Group
rjones@foxrothschild.com; 202-461-3111
November 9, 2017

Today's Outline

We will:

- Walk through and explain the new DFARS Cybersecurity Requirements – Will break the requirements into three steps.
- Explain the FAR Requirements and how they relate to the new DFARS clause.
- Urge you to roll these new federal cybersecurity requirements into your existing FAR 52.203-13 ethics & compliance obligations.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- **History**: It's not a new rule. It has applied to federal agencies since at least 2013. It was updated in October 2016 to apply to contractors on Department of Defense contracts.
- **Not Retroactive**: It is not required to be applied retroactively, but a contracting officer may modify an existing contract to add the clause.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- **There are two DFARS clauses**
  - **DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls)** is the notice clause that accompanies the 7012 clause.

- **Subcontractor Flowdown Requirement**: Primes must flow this clause down to subcontracts for operationally critical support or for which subcontract performance will involve covered defense information.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- **Purpose**: To ensure that unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized through cyber incident reporting and damage assessment processes.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- **The Three Main Tasks**:
  - Figure out what information is covered,
  - Implement the cyber incident reporting requirements, **and**
  - Develop and document a System Security Plan/Plans of Action – all by December 31, 2017.

The Third Task - The System Security Plan

- **NIST 800-171, Rev. 1, Chapter 3 Requirements**
  - Describe in a ***system security plan***, how the specified security requirements are met or the plan for how they will be met.
  - Plan should describe the system boundary, the operational environment, how the security requirements are implemented, and the relationships with or connections to other systems.
  - Develop ***plans of action*** about how requirements will be met and risks mitigated.
  - SSP/POA separate or combined. No required format.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- Requires **Covered Contractor Information Systems** to comply with **NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)** in effect at the time the solicitation is issued.
  - NIST = Department of Commerce's National Institute of Standards and Technology.
- Don't get overwhelmed! 6 pages in Chapter 3 identify the requirements; the other 69 pages are just introduction and attachments.

NIST 800-171, Rev. 1, Chapter 3 Requirements

- Outline your SSP based on the 14 categories in Chapter 3:
  - Access Control
  - Awareness & Training
  - Audit & Accountability
  - Configuration Management
  - Identification and Authentication
  - Incident Response
  - Maintenance
  - Media Protection

NIST 800-171, Rev. 1, Chapter 3 Requirements

- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System & Communications Protection
- System & Information Integrity

DoD Guidance on Implementation

- DoD issued a guidance memo on September 21, 2017.
  - "There is no single or prescribed manner in which a contractor may choose to implement NIST 800-171, or to assess their own compliance with those requirements."

- DoD previously issued an updated Frequently Asked Questions on January 27, 2017 regarding the application and requirements of the new clause The FAQ is a helpful document for contractors working on implementation of DFARS 252.204.7012.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- Earlier versions of DFARS 252.204-7012 applied only to Federal systems and were based upon **NIST 800-53 (Security and Privacy Controls for Federal Systems and Organizations)**.

- NIST 800-171 includes Appendix D (Mapping Tables) to map out the basic security requirements.

- **<u>Do Not Use Appx. D As Anything Other Than a Loose Guide!</u>**

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- Before you can develop a System Security Plan or a Plan of Action, you first need to know what information is covered by the new clause.

DFARS 252.204-7012
(Safeguarding Covered Defense Information & Cyber Incident Reporting)

- The clause applies to "***covered contractor information systems***" that hold "***covered defense information***."

- Like any good FAR or DFARS clause, there are lots of confusing acronyms, so let's break it down like Mr. Potato Head.

"Covered Contractor Information System" (CCIS) means:

- An unclassified information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information.
- In other words, a CCIS is an unclassified information system that is owned or operated by a federal contractor and that process or stores **Covered Defense Information (CDI)**.

"Covered Defense Information" (CDI) means:

- Unclassified **Controlled Technical Information *or***
- Other information described in the **Controlled Unclassified Information (CUI)** registry published by the National Records and Archives (NARA); ***and that***
- Requires safeguarding or dissemination controls ***and*** is:
  - Marked or otherwise identified in the contract; **or**
  - Collected, developed, received, transmitted, used, stored, etc. by the contractor.

"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. It does not include information that is lawfully publicly available without restrictions. It means technical data or computer software as those terms are defined in DFARS 252.227-7013 (Rights in Technical Data - Noncommercial Items).

"Controlled Technical Information" means:

- Examples 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.

"Controlled Unclassified Information" (CUI) means:

- Any of the categories in the CUI Registry is considered covered defense information.

- Export control is a CUI Registry category and is considered CDI when it is (1) marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract **or** (2) collected, developed, received, transmitted, used, stored by or on behalf of the contractor in support of performance of the contract.

DFARS Cyber Incident Reporting

DFARS Cyber Incident Reporting

- When you discover a cyber incident that affects a CCIS or the CDI residing there, or that affects your ability to perform, you must:
- Conduct a review for evidence of compromise of CDI including identifying the compromised computers, servers, specific data, and user accounts; **and**
- **Rapidly reporting** (i.e., within 72 hours) the cyber incidents to DoD at http://dibnet.dod.mil.

DFARS Cyber Incident Reporting

- Must preserve and protect images of all known affected information systems for at least 90 days from the submission of the Cyber Incident Report.

- Must provide DoD with access to all information and equipment if DoD requests so DoD can conduct its own forensic analysis.

DFARS/FAR Comparison Guide

- Comparison to **DFARS Cybersecurity Provisions**
  - Many contractors will be subject to **both** the Final Rule and the DFARS Rule.

- DFARS requires far more extensive security controls and reporting requirements than the FAR clause.
  - Cyber Incident Reporting
  - Post-Incident Investigation (90 day preservation period from reporting to give DoD time to determine whether it wants to investigate and to give access to additional information and equipment)

DFARS/FAR Comparison Guide

- FAR Rule is more **limited and basic**
  - Steps a **reasonable** business should be taking irrespective of requirements
  - DFARS mandates "enhanced safeguarding," by comparison

- FAR Rule does **not** include mandatory cyber-incident reporting, incident response, or data collection
  - No forensic analysis requirement
  - Reporting and data collection elements of the DFARS cited as most troubling for DoD contractors

- FAR Rule does **not** include NIST 800-171 requirements
  - Standard covering most government systems and the DFARS

FAR 52.204-21
(Basic Safeguarding of Covered Contractor Information Systems)

- **Final Rule** Issued May 2016 (3+ years after interim rule first published)
    - Effective as of **June 15, 2016**

- Published by **DoD**, **GSA**, and **NASA**
  - But will apply to virtually all future Federal contracts

- Compliance Now **Mandatory** for All Contracts Including **Cybersecurity Clause**

FAR 52.204-21
(Basic Safeguarding of Covered Contractor Information Systems)

- New subpart (4.19) and contract clause (52.204-21) to the Federal Acquisition Regulation (FAR)

- Basic Safeguarding of Covered Contractor Information Systems

"**For the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information**."

FAR 52.204-21
(Basic Safeguarding of Covered Contractor Information Systems)

- Intent of the Rule is to establish **basic** safeguarding measures as part of the contractor's "**routine**" business practice.
- Basic Jumping Off Point for Contractor Compliance
  - Think in terms of your **Business Ethics and Compliance Program**
- Does **Not** Impact Other Federal Safeguarding Requirements:
  - **DFARS 252.204-7012** (Safeguarding Covered Defense Information and Cyber Incident Reporting) (2016)
  - Requirements Relating to **Classified** or **Controlled Unclassified Information**

FAR 52.204-21
(Basic Safeguarding of Covered Contractor Information Systems)

- The Rule imposes **15 "basic" security controls** for contractors
- The Rule applies to "**covered contractor information systems**" (contractor systems that process, store, or transmit "Federal contract information")
- **Federal contract information** means information provided by **or** generated for the Government under a contract to develop or deliver a product or service for the Government, but does not include: (1) publicly available information, or (2) basic transactional information (like information required to process contractor payment applications)

The 15 Security Controls

1. Limit access to **authorized users**.
2. **Limit information system access** to the types of transactions and functions that authorized users are permitted to execute.
3. **Verify controls** on connections to external information systems.
4. **Impose controls** on information that is posted or processed on publicly accessible information systems
5. **Identify information system users and processes** acting on behalf of users or devices

The 15 Security Controls

6. **Authenticate or verify the identities of users, processes, and devices** before allowing access to an information system

7. **Sanitize or destroy** information system media containing Federal contract information before disposal, release, or reuse.

8. **Limit physical access** to information systems, equipment, and operating environments to authorized individuals.

9. **Escort visitors and monitor visitor activity**, maintain audit logs of physical access, control and manage physical access devices.

The 15 Security Controls

- 10. **Monitor, control, and protect organizational communications** at external boundaries and key internal boundaries of information systems.
- 11. **Implement sub networks** for publically accessible system components that are physically or logically separated from internal networks.
- 12. Identify, report, and correct information and information **system flaws** in a timely manner.
- 13. Provide protection from **malicious code** at appropriate locations within organizational information systems.

The 15 Security Controls

- 14. Update **malicious code protection** mechanisms when new releases are available.
- 15. Perform **periodic scans** of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. FAR 52.204-21(b).

Understand Cybersecurity in terms of Ethics & Compliance

- **Integrate the FAR and DFARS cybersecurity requirements into your ethics and compliance Program!**

- **FAR 52.203-13** Requires Contractors to:
  - Implement a **Contractor Code of Business Ethics and Conduct**.
  - Establish a **Business Ethics Awareness and Compliance Program**.
  - Establish an **Internal Control System**.
  - Inform the Office of Inspector General and Contracting Officer of "**Credible Evidence**" of any Violation.

Questions?