Raytheon

IT DFARS CDI Clause and Cyber Reporting

Kathy O'Donnell, CISSP
Manager, Computer Systems Analysis
Integrated Defense Systems
Raytheon

What is the Requirement?

Raytheon

The Applicable Clause (DFARS 252.204-7012 (Dec 2016)

Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS Final Rule –

- Regulations Update:
  - 20 Dec 16: Final release of National Institute of Standards and Technology (NIST) Special Publication 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.
  - 11 Jan 17: Based on the final rule Frank Kendall - Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System
  - Provide "Adequate Security" for all "Covered Defense Information" on all covered contractor information systems that support performance of work under the contract

DFARS Cyber Clause Mandatory for DoD Contracts

What is “Adequate Security”?

Raytheon

- “Adequate Security” means meeting the NIST 800-171 security controls
- Defense contractors have until 31 December 2017 for full compliance to the NIST 800-171 controls
- NIST 800-171 imposes 109 Controls under 14 “families” of basic & derived security requirements
- Requirement for contractors to report (to the DOD-CIO- not the PCO) any current areas of non-compliance *within 30 days of contract award*

Non-compliance needs to be reported within 30 days of contract award

What is “Covered Defense Information”?

Raytheon

Covered Defense Information (CDI) is ***unclassified information*** that:

- Is provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or
- Is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract, and
- Falls within the four categories:
  - Controlled Technical Information
  - Critical Information
  - Export Controlled Information
  - Other information that requires safeguarding or dissemination controls

Unclassified and used in support of contract with DFARS clause

The 4 Categories of CDI

Raytheon

Controlled Technical Information

- Technical information subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination
- Distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents.

Critical Information

- Operations Security Process
- Friendly intentions, capabilities, and activities needed by adversaries to guarantee failure or unacceptable consequences for friendly mission

Export Control

- Unclassified information whose export could reasonably affect national security and nonproliferation objectives
- Includes: Dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

Other

- Other Information identified in the contract, that requires safeguarding or dissemination controls (e.g., privacy, proprietary business information)

Examples of Possible CDI- “Controlled Technical Information”

Raytheon

- From The DFARS Clause
  - 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
  - Computer software executable code and source code

KMO1

How to Protect CDI

- NIST Special Publication 800-171, Revision 1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Describes fundamental assumptions and methodology used to develop the security requirements for protecting CDI, format and structure of the requirements and the tailoring criteria applied to NIST standards
  - Describes 14 families of security requirements for protecting CDI
  - Supporting appendices provide additional information related to protecting CDI
    - General references
    - Definitions and terms
    - Acronyms
    - Mapping tables relating security requirements with security controls in NIST Special Publication 800-53 and ISO/IEC 27001
    - Explanation of tailoring actions employed on moderate security control baseline

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Slide 7

KMO1 Kathleen M O'Donnell, 6/27/2017

What are the NIST 800-171 Security Controls?

Raytheon

Family	Controls	Family	Controls
Access Control	22	Media Protection	9
Awareness & Training	3	Personnel Security	2
Audit & Accountability	9	Physical Protection	6
Configuration Mgt.	9	Risk Assessment	3
Identification & Authentication	11	Security Assessment	3
Incident Response	3	System & Communications Protection	16
Maintenance	6	System & Information Integrity	7
		Total	109

109 Controls under 14 “Families”

What types of security controls?

Raytheon

- What are the security controls we need to implement?
  - Physical controls
    - Hardware devices on your systems (physically and virtually plugged in)
    - Servers, routers, switches, and servers with firewalls, patches
    - Wireless access control and protection
  - Software controls
    - Only authorized software allowed
    - Ability to detect and remove unauthorized software and malicious code
  - Boundary defense
    - Interfaces between systems and with customers and suppliers
    - Physical security of company systems
    - Employee and the visitor badging and access controls

What types of security controls?

Raytheon

- Management Policies
  - Data recovery capability
  - Data encryption
  - Access control and monitoring of employee accounts
  - Vulnerability assessment and remediation
  - System maintenance and risk assessment

- Organization: an important part of your line of defense
  - Awareness training: prevent unauthorized website surfing, software, and devices; data encryption
  - Information security organization expertise

- Possible alternate but equally effective security controls

The key is documentation!

How to Get to Compliance

Raytheon

- System administrators apply technical controls
  - Operating system configuration settings described in 800-171
- Organization define and document policies to address non-technical controls
  - Configuration management plan
  - Access control list
  - Network diagrams
  - Vulnerability management plan
  - Audit log management plan
  - Disaster recovery plan
  - Hardware and software maintenance
    - All hardware and software must be supported
    - End-of-life operating systems are non-compliant since they are not supported

Helpful Links

Raytheon

- DoD DFARS Frequently Asked Questions (FAQs)
  - http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services.pdf
- DFARS – Safeguarding CDI
  - http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
- NIST 800-171
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
- NDIA Cybersecurity for Advanced Manufacturing Public Forum
  - https://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services.pdf
- Raytheon Foreground Security (RFS) and Forcepoint
  - Safeguarding users, data and networks against insider threats and outside attackers, in the cloud, on the road, in the office.
  - www.forcepoint.com
- Sysadmin, Audit, Network and Security (SANS) Institute
  - https://www.sans.org

Questions?

Raytheon