March 20, 2023

Cybersecurity Rules Under FAR & DFARS: Protecting Unclassified Information

α

AMADEO LAW FIRM

PROFESSIONAL LIMITED LIABILITY COMPANY

Introductions

Mark A. Amadeo

- Over 20 years experience as government counsel & law firm counsel
- LL.M. Georgetown University Law Center; J.D. University of Wisconsin Law School; B.A. Boston College
- Founder & Managing Partner of Amadeo Law Firm, PLLC
- Focus on Government Contracting & Technology
  - Drafting/Negotiating: Teaming, Subcontract, Joint Ventures
  - Government Contract & FAR/DFARS Compliance
  - Post-award Review and Negotiations
  - Technology: IP Preservation & Commercialization

March 20, 2023

Cybersecurity Rules Under FAR & DFARS: Protecting Unclassified Information

α

AMADEO LAW FIRM

PROFESSIONAL LIMITED LIABILITY COMPANY

Overview

FAR - Basic Safeguarding Rules (FCI) - DoD & Civilian Agency Contracts

- 15 basic requirements

DFARS - Additional Security Requirements (CDI) - DoD Contracts

- Adequate security
- Cyber incident & malicious software responses
- NIST SP 800-171 assessments

Coming Soon – DFARS - CMMC Verification – DoD Contracts

- Basic FAR safeguarding
- Additional DFARS safeguarding

FAR – Basic Safeguarding Rules

FAR: 52.204-21

Which Contracts/Solicitations?

When contractor or subcontractor will have Federal Contract Information (FCI) in information systems

What Conditions Trigger The Requirements?

Covered Contractor Information System (CCIS) – an IS that processes, stores, or transmits Federal Contract Information (FCI)

Federal Contract Information (FCI)

- Not intended for public release and
- Provided by Gov or generated for Gov under the contract

but not

Made public by Gov or transactional information

α

AMADEO LAW FIRM

PROFESSIONAL LIMITED LIABILITY COMPANY

FAR – Basic Safeguarding Rules

Basic Safeguarding Requirements – at a minimum – the following 15:

- Limit access to authorized users/devices
- Limit access to types of transactions and functions
- Verify/control/limit connections to and use of external information systems
- Control information posted or processed on publicly available systems
- Identify information system processes acting on behalf of users/devices
- Authenticate/verify identities of users/processes/devices before access
- Sanitize/destroy media before release/disposal
- Limit physical access to information systems, equipment and operating environments
- Escort/monitor visitors, maintain logs, control/manage physical access devices
- Implement subnetworks for publicly accessible system components
- Identify/report/correct information and flaws in a timely manner
- Provide malicious code protection
- Update malicious code protection with new releases
- Perform periodic scans of information systems + real time scans of files from external sources

DFARS – Additional Security Requirements

DFARS: 252.204-7008; 252.204-7012; 252.204-7019; 252.204-7020

Which Contracts/Solicitations?

All DoD solicitations/contracts except COTS

What Conditions Trigger The Requirements?

Covered Contractor Information System – an IS that processes, stores, or transmits Covered Defense Information (CDI)

DFARS – Additional Security Requirements

What Conditions Trigger The Requirements?

Covered Defense Information (CDI)

- **Unclassified Controlled Technical Information (CTI) or**
- **Controlled Unclassified Information (CUI), as described in National Archives CUI Registry (http://www.archives.gov/cui/registry/category-list.html)**

plus

- **Marked or identified in contract/order and provided to the contractor by DoD in support of contract performance, or**
- **Collected, developed, received, transmitted, used or stored by the contractor in support of contract performance**

α

Amadeo Law Firm

Professional Limited Liability Company

DFARS – Additional Enhanced Security Requirements

What Conditions Trigger The Requirements?

Controlled Technical Information (CTI)

- **Technical information with military or space application subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.**
  - **Technical Information: DFARS 252.227-7013 - Technical Data or Computer Software**
- **CTI would meet criteria for distribution statements (B through F) under DoD Instruction 5230.24 if disseminated**

But CTI does not include: Information made public with no restrictions

252.204-7000 Disclosure of Information

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

What Conditions Trigger The Requirements?
CTI

DoD Instruction 5230.24 (As of 2018)

- Administrative or Operational Use
- Contractor Performance Evaluation
- Critical Technology
- Export Controlled
- Foreign Government Information
- Operations Security
- Premature Dissemination (Patentable Information)
- Proprietary Information
- Test and Evaluation
- Software Documentation
- Specific Authority
- Vulnerability Information

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

What Conditions Trigger The Requirements?
CTI

DoD Instruction 5230.24 (As of 2023)

- CTI
- Contractor Performance Evaluation
- Critical Technology
- Direct Military Support
- Export Controlled
- Foreign Government Information
- International Agreements
- Operations Security
- Patents & Inventions
- Proprietary Business Information
- Small Business Innovation Research (SBIR)
- Software Documentation
- Test & Evaluation
- Vulnerability Information

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

What Conditions Trigger The Requirements?

Controlled Unclassified Information (CUI) (under National Archives Registry) - information that requires safeguarding or dissemination control under law, regulations or Gov policies (http://www.archives.gov/cui/registry/category-list.html)

20 Groupings	125 Categories
Critical Infrastructure	General Critical Infrastructure Information Physical Security
Defense	Controlled Technical Information DoD Critical Infrastructure Security Info
Export Controlled	Export Controlled
Patent	Patent Applications Inventions
Procurement	General Procurement and Acquisition Small Business Research and Technology
Proprietary Business Information	General Proprietary Business Information

α

Amadeo Law Firm

Professional Limited Liability Company

DFARS – Additional Security Requirements

Adequate Security Requirements
(DFARS 252.204-7012)

CCIS – Part of IT Service or System Government-Operated

- IT/System Not Cloud Computing – Requirements in the contract
- Cloud Computing Services – Must also meet DFARS 252.239-7010:
  - DoD's Cloud Computing Security Requirements Guide
    - FedRAMP and other requirements
  - Maintain data in US or outlying areas
  - Limitations on access to data
  - Cyber incident reporting
  - Malicious software
  - Media preservation
  - Records management/facility access

DFARS – Additional Security Requirements

Adequate Security Requirements
(DFARS 252.204-7012)

CCIS – Part of IT Service or System Operated By the Contractor

- Implementation of 110 NIST SP 800-171 Security Requirements
  - Unless DoD CIO has indicated requirement is not applicable or approved a request to vary the requirement
- If Contractor uses cloud-services for CDI (i.e., CUI or CTI)
  - Cloud service provider must be FedRAMP compliant
- Any other security measures the contractor determines necessary

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

Adequate Security Requirements (DFARS 252.204-7012)

CCIS – Part of IT Service or System Operated By the Contractor

Implementation of 110 NIST SP 800-171 Security Requirements

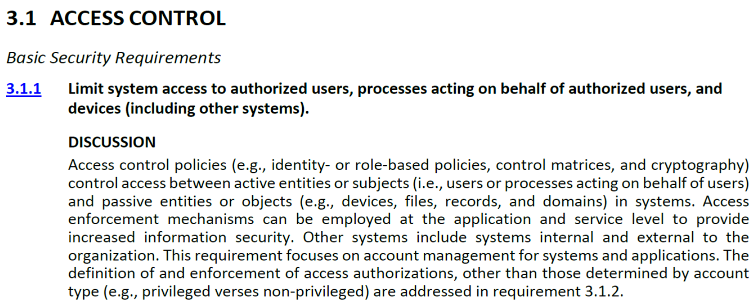
- **Implement all 110 security requirements; or**
- **System security plan (SSP) and plans of action (POA)**

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

Adequate Security Requirements (DFARS 252.204-7012)

NIST SP 800-171



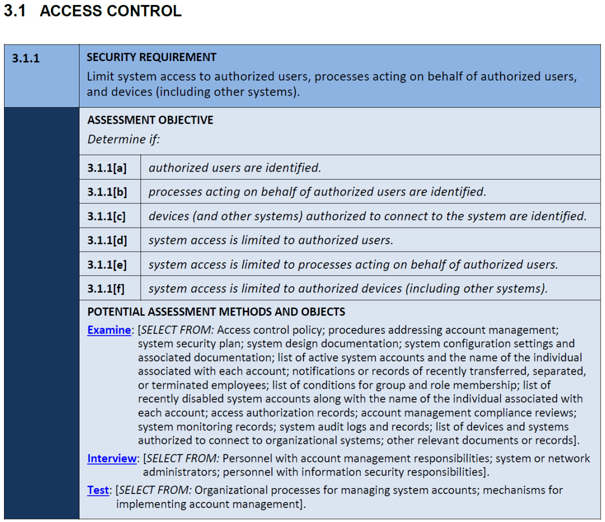
3.1 ACCESS CONTROL

Basic Security Requirements

3.1.1 **Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.



3.1 ACCESS CONTROL

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].	

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

DFARS – Additional Security Requirements

Cyber Incident & Malicious Software Responses (DFARS 252.204-7012)

- Cyber incident reporting (*https://dibnet.dod.mil*)
  - Must have a medium assurance certificate
- Malicious software submission
- Media preservation and protection
- Provide DoD access to information or equipment
- Marking data before submission to DoD

DFARS – Additional Security Requirements

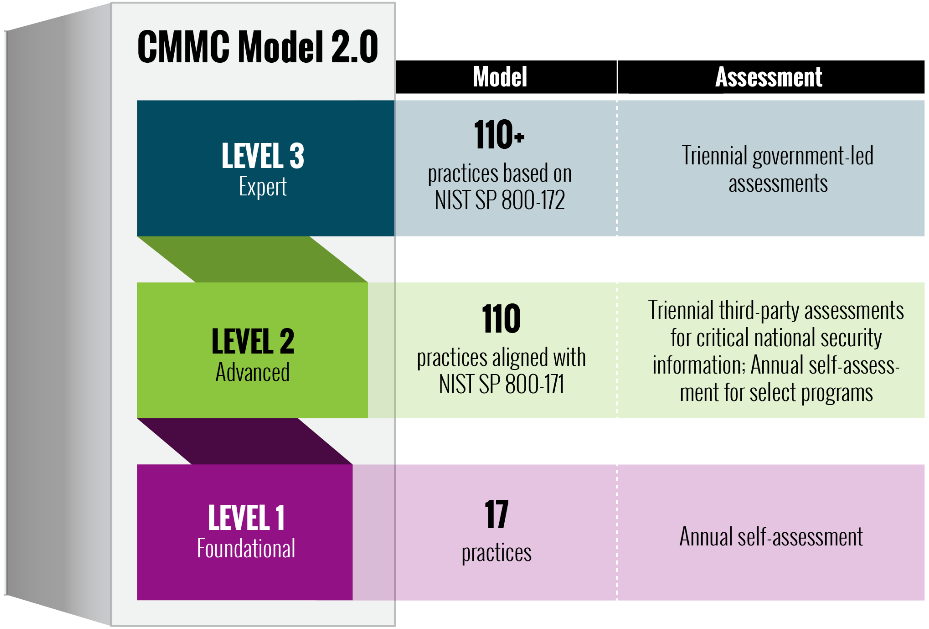
NIST SP 800-171 Assessments
(DFARS 252.204-7019, 252.204-7020)

- To receive a DoD award must have a current assessment for each CCIS
  - No more than 3 years old
  - NIST SP 800-171 DoD Assessment Methodology & SP 800-171A
    - Basic – self assessment
      - Based on review of SSP
    - Medium & High – Gov assessment
      - Review contractors Basic Assessment (M/H)
      - Thorough document review (M/H)
      - Discussions if addition info needed (M/H)
      - Verification, examination and demonstration of SSP (H)

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

Coming Soon – CMMC Verification Requirements

Certification Requirements (DFARS 252.204-7021)



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

Cybersecurity Rules Under FAR And DFARS

Last Thoughts

Flow down requirements

Expect gov-wide CMMC or similar requirements

Contractors should be proactive

Cybersecurity Rules Under FAR & DFARS: Protecting Unclassified Information

THANKS!

Any questions?

Mark Amadeo
(202) 640 - 2090
mamadeo@amadeolaw.com
www.amadeolaw.com

α
AMADEO LAW FIRM
PROFESSIONAL LIMITED LIABILITY COMPANY

Cybersecurity Rules Under FAR & DFARS: Protecting Unclassified Information

THANK YOU FOR JOINING OUR WEBINAR!

The Recorded Webinar Can Be Found Here:

https://www.amadeolaw.com/firm - resources/webinars

α

AMADEO LAW FIRM

PROFESSIONAL LIMITED LIABILITY COMPANY