NCMA *Wisconsin Chapter*

Cybersecurity Federal Acquisition Regulations

New and Updated

(January 2017)

By Jason Rathsack
Contractor Update 1/17/2017

DISCLAIMER: The views expressed are not necessarily representative of DCMA. I am here to present on behalf of NCMA, Wisconsin Chapter. Although all of the information contained within is public knowledge, any opinions expressed are those of the presenter alone. If you have any questions, feel free to contact Jason Rathsack at visn12jr@gmail.com

Agenda

A. History

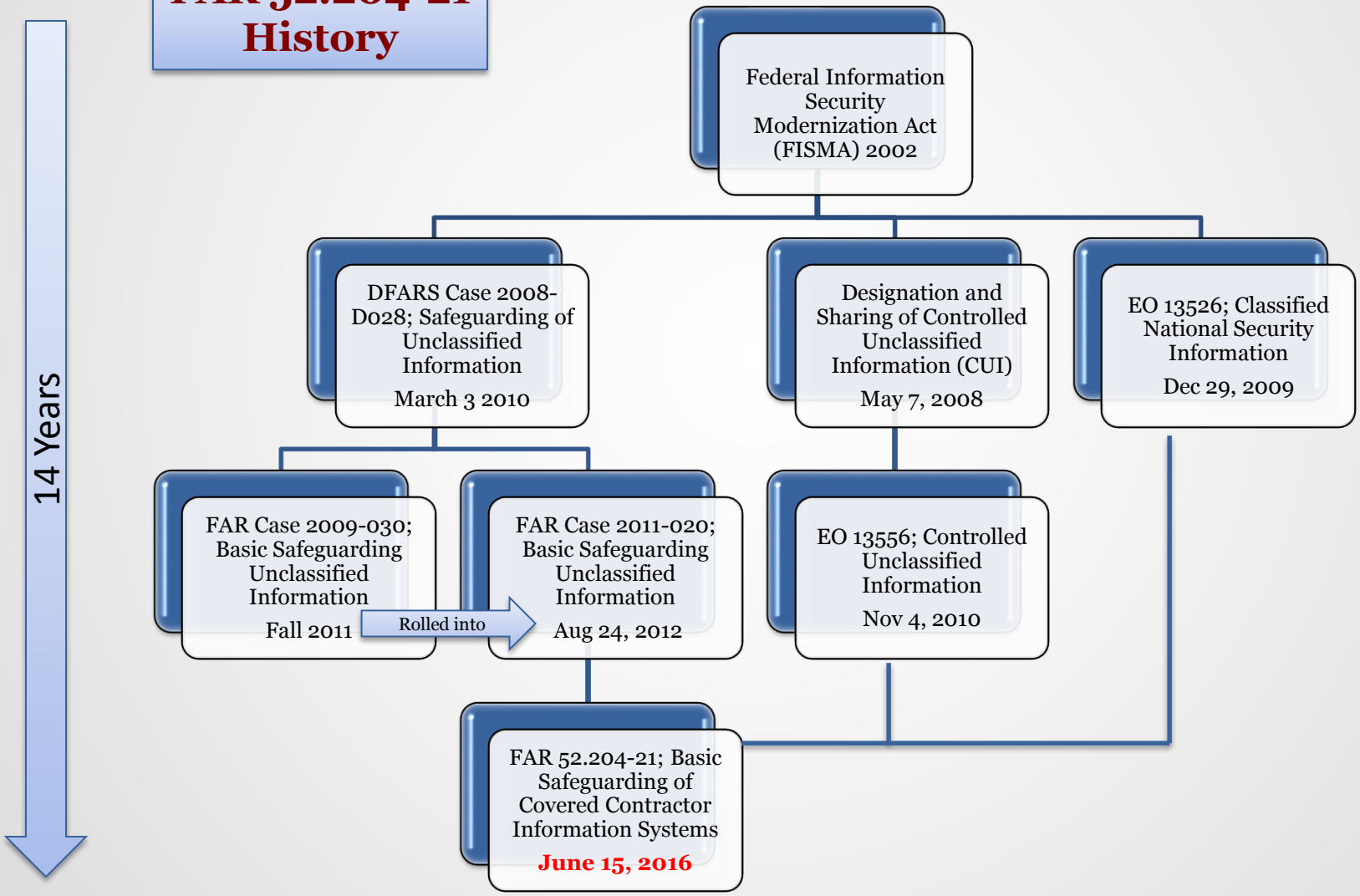
B. Regulations

   1. Prescription
   2. Clause
   3. Administration

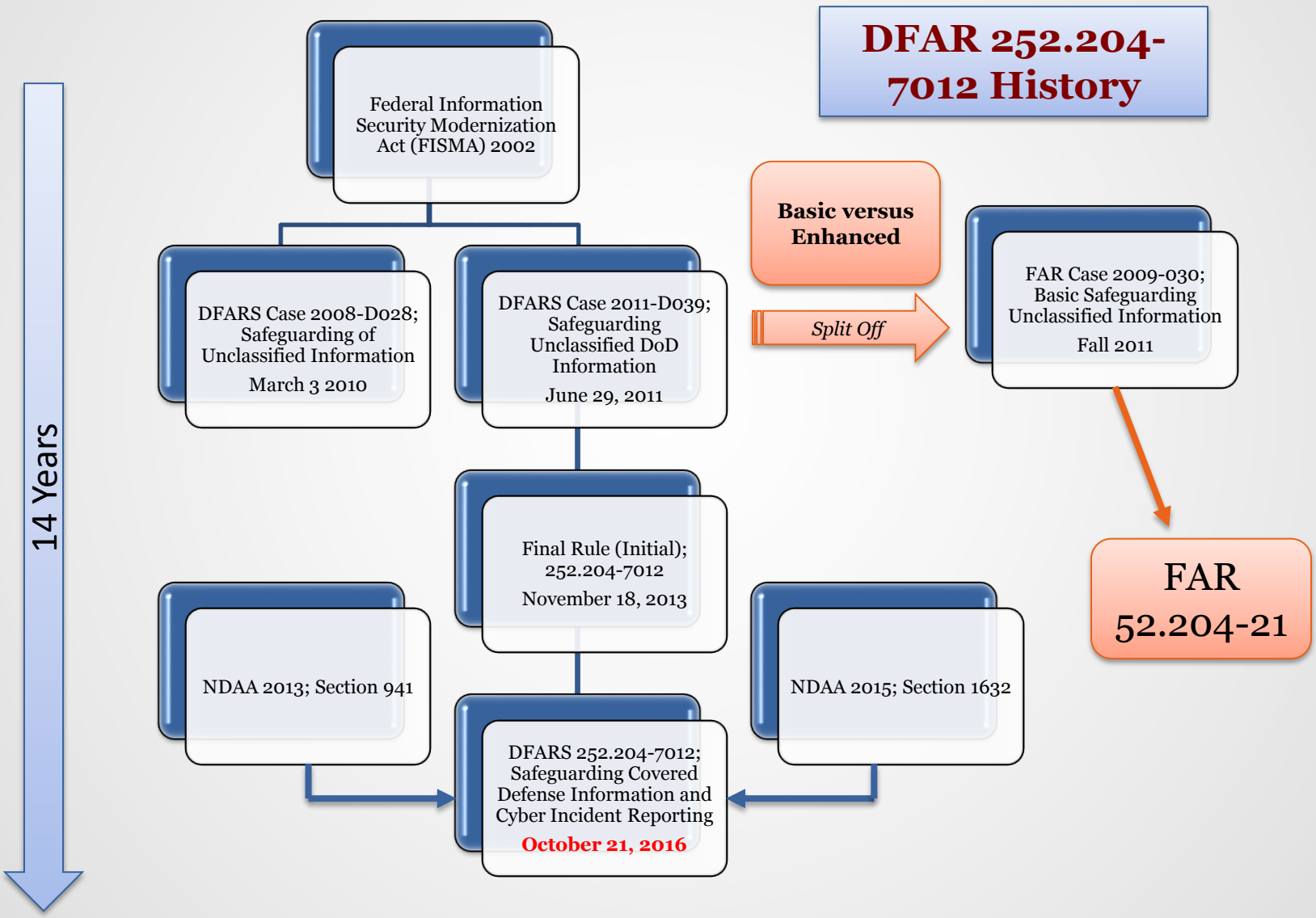
C. Resources

NCMA *Wisconsin Chapter*

FAR 52.204-21 History



NCMA *Wisconsin Chapter*



Provisions and Clauses

1) **52.204-21** – Basic Safeguarding of Covered Contractor Information Systems **(Clause)** **(June 2016)**

2) **252.204-7008** Compliance with Safeguarding Covered Defense Information Controls. **(Provision)** **(Oct 2016)**

3) **252.204-7009** Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. **(Applies to contracts for cyber security services)** **(Oct 2016)**

4) **252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting. **(Clause)** **(Oct 2016)**

Provisions and Clauses

1. **52.204-21** – Basic Safeguarding of Covered Contractor Information Systems (Clause) (June 2016)

2. 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls. (Provision)
3. 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. (Applies to contracts for cyber security services)

4. **252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting. (Clause) (Oct 2016)

Prescription: FAR 52.204-21

The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

Prescription: FAR 52.204-21

The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a ***subcontractor at any tier*** may have **Federal contract information** residing in or transiting through its *information system*.

Definitions: FAR 52.204-21

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Definitions: FAR 52.204-21

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but **not including information provided by the Government to the public (such as on public Web sites)** or simple transactional information, such as necessary to process payments.

Definitions: 52.204-21 – Federal Contract Information

Federal Register: The clause is prescribed for inclusion in the solicitation when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system. This does not require any specific knowledge of the contractor's existing information system. Generally, the person drafting the contract requirements/statement of work would know if contract performance will involve Federal contract information residing in or transiting through its information system. The contracting officer may not have the technical expertise to make this determination.

Definitions: 52.204-21 – Federal Contract Information

Federal Register: The clause is prescribed for inclusion in the solicitation when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system. This does not require any specific knowledge of the contractor's existing information system. Generally, the person drafting the contract requirements/statement of work would know if contract performance will involve Federal contract information residing in or transiting through its information system. **The contracting officer may not have the technical expertise** to make this determination.

Definitions: 52.204-21 – Information System

Federal Register: The intent is that the scope and applicability of this rule be very broad, because this rule requires only the most basic level of safeguarding. The focus of the final rule is shifted from the safeguarding of specific information to the basic safeguarding of certain contractor information systems. Therefore, it is not necessary to draw a fine line as to what information was "generated for the Government," when the information is received, or whether the information is marked. The requirements pertain to the information system itself. A prudent business person would employ this most basic level of safeguarding, even if not covered by this rule. This rule is intended to provide a basic set of protections for all Federal contract information, upon which other rules, such as a forthcoming FAR rule to protect CUI, may build.

Definitions: 52.204-21 – Information System

Federal Register: **The intent is that the scope and applicability of this rule be very broad**, because this rule requires only the most basic level of safeguarding. The focus of the final rule is shifted from the safeguarding of specific information to the basic safeguarding of certain contractor information systems. Therefore, it is not necessary to draw a fine line as to what information was "generated for the Government," when the information is received, or whether the information is marked. **The requirements pertain to the information system itself. A prudent business person would employ this most basic level of safeguarding, even if not covered by this rule.** This rule is intended to provide a basic set of protections for all Federal contract information, upon which other rules, such as a forthcoming FAR rule to protect CUI, may build.

Clause - 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

(b)(1) (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- 15 Safeguards (see handout) - **comparable security requirements from NIST SP 800-171**

1) Limit information system access to employees on an as needed basis
2) Document who has what devices and access to what systems
3) Federal Contract Information is a valued commodity – treat it as such
4) Physical security – escort and limit access
5) Segregate internal from external systems
6) IT Security Policies – develop, document, and practice

Flowdowns - 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

Federal Register: The final rule no longer focuses on the safeguarding of information, but of information systems. The requirement to flow the clause down to subcontractors accomplishes the objectives of the rule to require safeguarding of covered contractor information systems at all tiers.

Administration - 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

Federal Register: e. Noncompliance Consequences

Comment: One respondent was concerned that any inadvertent release of information could be turned into not only an information security issue but also a potential breach of contract.

Response: The refocus of the final rule on the safeguarding requirements applicable to the system itself should allay the respondent's concerns. Generally, as long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract.

Prescription: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

DFARS 204.7304

(a) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(c) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.

Prescription: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

204.7304

(a) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, **in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.**

(c) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, **in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.**

Prescription: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard **covered defense information** that resides in or transits through **covered contractor information systems** by applying specified network security requirements. It also requires reporting of cyber incidents.

- WIFCON Discussion – disagreement over application
- DPAP March 1, 2016 BBP Memorandum: **DFARS Clause 252.204-7012 is prescribed for use in all solicitation and contracts.**

Could the clause be included in the contract but not required to be implemented?

Q4: When must the requirements in DFARS clause 252.204-7012 be implemented? (DPAP Memo)

A4: The requirements in DFARS clause 252.204-7012 must be implemented when CDI is processed, stored, or transits through an information system that is owned, or operated by or for, the contractor, or when performance of the contract involves operationally critical support. The contracting officer shall indicate in the solicitation/contract when performance of the contract will involve, or is expected to involve, CDI or operationally critical support. All CDI provided to the contractor by the Government will be marked or otherwise identified in the contract, task order, or delivery order.

Could the clause be included in the contract but not required to be implemented?

Q4: When must the requirements in DFARS clause 252.204-7012 be implemented?

A4: The requirements in DFARS clause 252.204-7012 must be implemented **when CDI is processed, stored, or transits through an information system that is owned, or operated by or for, the contractor, or when performance of the contract involves operationally critical support.** The contracting officer shall indicate in the solicitation/contract when performance of the contract will involve, or is expected to involve, CDI or operationally critical support. **All CDI provided to the contractor by the Government will be marked or otherwise identified in the contract, task order, or delivery order.**

Definitions: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Definitions: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

"Covered defense information" means **unclassified controlled technical information** or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) **Marked or otherwise identified in the contract**, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) **Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.**

Definitions: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

"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.

Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Definitions: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

"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.

Controlled technical information would meet the criteria, if disseminated, for **distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.**

Clause: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

- 13 Parts – summarized below

(a) Definitions – covered

(b) CDI is subject to NIST 800-171 Requirements

1) Must be implemented by December 31, 2017

2) You may seek a waiver if you cannot meet the security requirements for any contract awarded prior to October 1, 2017

- **Issue #1: Do I need to seek a waiver for every contract until I meet the requirement?**

- **Issue #2: Old contracts versus new contracts? Prior NIST SP 800-53 versus current NIST 800-171**

Clause: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

(c-g) Cyber Incident Reporting

1. Rapidly report (72 hours) cyber incidents to http://dibnet.dod.mil
2. DoD reserves right to conduct their own forensic analysis - DoD Cyber Crime Center (DC3)
3. Requirements and instructions for preserving records and how to report

- **HINT: Familiarize yourself with:**
  - ✓ **Defense Industrial Base (DIB) Cybersecurity Program**
  - ✓ **DoD Cyber Crime Center (DC3)**
  - ✓ **Defense Industrial Base Collaborative Information Sharing Environment (DCISE)**

Clause: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

(h-j) Government versus Contractor rights with Proprietary Data

(k-l) Don't ignore other regulations (Classified Info and/or IT Service Contractors)

(m) Mandatory flowdown

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties.

- **CPSR Team Discussion and Federal Register Comment – Conflict?**
- **Cost to Small Biz?**

Administration: DFARS 252.204-7008 & 7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

Federal Register: A number of respondents commented on the lack of oversight and certification of compliance with the NIST controls in the rule. Several respondents requested clarification on the requirements for an organization to be considered compliant, as well as the intended means of verification, which organization will verify, how compliance will be assessed

Response: No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, then it can be accomplished through existing Federal Acquisition Regulation (FAR) and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require "certification" of any kind. By signing the contract, the contractor agrees to comply with the contract's terms.

❖ Resources and Government Players

- National Institute of Standards and Technology (NIST) – Computer Security Resource Center (CSRC) – Computer Security Division
- National Archives and Record Administration (NARA)
- Defense Industrial Base (DIB) Cybersecurity Program
- DoD Cyber Crime Center (DC3)
- Defense Industrial Base Collaborative Information Sharing Environment (DCISE)
- Office of Management and Budget (OMB) CIO
- Department of Homeland Security

❖ Take Aways

- Requirements are evolving and will continue to – IT Security is dynamic
- The Regulations are coming but administration guidelines are not here **YET**…
- There are a lot of Government players involved – get familiar
- Develop and **DOCUMENT** your basic safeguards
- Develop and **DOCUMENT** internal procedures for how to handle a cyber intrusion incident

Questions?

NCMA WI Chapter

Jason Rathsack

visn12jr@gmail.com