Cybersecurity Challenges

Protecting DoD's Unclassified Information

Implementing DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

SOFIC 2019

Outline

- Cybersecurity Landscape
- Protecting DoD's Unclassified Information on the Contractor's Internal Information System
- DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Implementation and Guidance
  - Compliance and Oversight
- Enhancing the Cybersecurity Measures Provided by DFARS Clause 252.204-7012 and NIST SP 800-171
- Resources

Cybersecurity Landscape

Cyber threats targeting government unclassified information have dramatically increased

The U.S. was the most targeted country in the past three years; accounting for 27% of all targeted attack activity

Internet Security Threat Report, Symantec 2018

Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%)

AT&T Cybersecurity Insights Vol. 4

53% of attacks result in damages of $500,000 or more

CISCO Annual Cybersecurity Report 2018

61% of breach victims are businesses with <1,000 employees

80% of breaches leverage stolen, weak, and/or guessable passwords

2017 Data Breach Investigations Report, Verizon

Cybercrime will cost businesses over $2 trillion by 2019

Juniper Research

In a study of 200 corporate directors, 80% said that cyber security is discussed at most or all board meetings. However, two-thirds of CIOs and CISOs say senior leaders in their organization don't view cyber security as a strategic priority.

NYSE Governance Services and security vendor Veracode

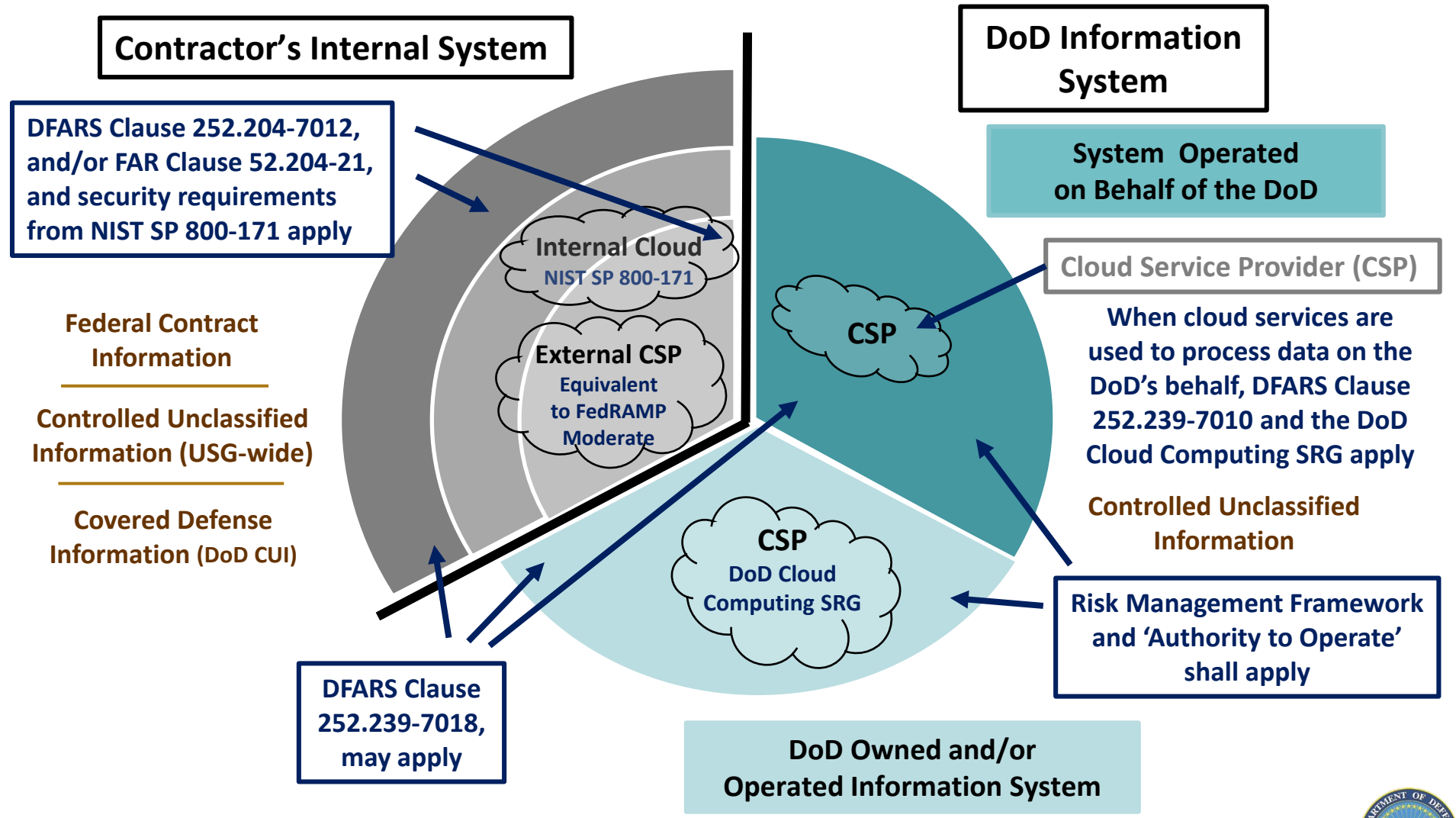
What DoD Is Doing

DoD is participating in a range of activities to improve the collective cybersecurity of the nation and protect U.S. interests:

- **Secure DoD's information systems and networks**
- **Implement contractual requirements to secure contractor systems and networks through the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS)**
- **Leverage National Institute of Standards and Technology (NIST) information security standards and guidelines for federal and nonfederal information systems**
- **Codify cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy**
- **Promote cyber threat awareness through information sharing opportunities**

The Department continues to focus on elevating cybersecurity in the DoD Supply Chain

Protecting the DoD's Unclassified Information



DFARS Clause 252.204-7012 - Requirements

Requires the program office/requiring activity to:

Mark or otherwise identify in the contract, task order, or delivery order covered defense information provided to the contractor by or on behalf of, DoD in support of the performance of the contract

Requires the contractor/subcontractor to:

- **Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network**
- **Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support**
- **Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center**
- **Submit media/information as requested to support damage assessment activities**
- **Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information**

DFARS Clause 252.204-7012 - Prescription and Flow down

DFARS Part 204.7304 Solicitation provision and contract clauses.

> **(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.**

DFARS Clause 252.204-7012 (m) Subcontracts.

> **The Contractor shall (1) Include this clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer…**

If a subcontractor does not agree or is unable to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not reside on the subcontractor ’s information system

Mark / Identify Covered Defense Information

Covered defense information – Term used to identify information that requires protection under DFARS Clause 252.204-7012

Covered defense information means:

- **Unclassified controlled technical information (CTI) or other information as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is –**
  1) **Marked or otherwise identified in the contract, task order, or delivery order and provided to 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***

* **"In support of the performance of the contract" is not meant to include the contractor's internal information (e.g., human resource or financial) that is incidental to contract performance**

Identification and Marking of Covered Defense Information

The Program Office/Requiring Activity must:

- Identify/mark covered defense information provided as Government Furnished Information (GFI)
  - DoDM 5200.01 Vol 4, DoD Information Security Program: CUI
  - DoDI 5230.24, Distribution Statements on Technical Documents
- Direct appropriate marking and dissemination requirements for covered defense information in the contract when covered defense information is to be acquired
  - Contract Data Requirements Lists (CDRL), DD Form 1423); Blocks 9 and 16
- Verify covered defense information is appropriately marked when provided to the contractor as GFI

The Contractor must:

- Follow the terms of the contract, to include:
  - Follow marking and dissemination requirements contained on GFI
  - Apply the marking and dissemination statements directed in the contract
  - Appropriately disseminate controlled unclassified information and marking and dissemination requirements to subcontractors

Marking and Dissemination Statements on Covered Defense Information

Dissemination Limitation	Reason	Date	Controlling Org
Distribution A: Public Release* **Distribution B: U.S. Govt Only** **Distribution C: U.S. Govt & Contractors** **Distribution D: DoD & US DoD Contractors** **Distribution E: DoD only** **Distribution F: Further dissemination only as directed by controlling office**	Administrative or Operational Use Contractor Performance Evaluation Critical Technology Direct Military Support Export Controlled Foreign Government Information Operations Security Premature Dissemination Proprietary Information Software Documentation Specific Authority Test and Evaluation Vulnerability Information	Note: Reason Determination Date	Note: Controlling Org can be different than the Authoring Org

**** Distro A: Public Release – NO Dissemination limitation***

DoD Policy was established in 1987

Example of Marking for Distribution Statement E

Distribution authorized to DoD only; Proprietary Information; 15 Apr 2017. Other requests for this document shall be referred to AFRL/VSSE, 3550 Aberdeen Ave. SE, Kirtland AFB, NM 87117-5776. REL TO UK

Example of Marking for Export Control Warning (Also requires separate distribution statement)

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

DoD Policy: DoDI 5230.24 – Distribution Statements on Technical Documents

Typical Marking and Dissemination Requirements Directed by Program Offices/Requiring Activities in a Contract

Information Types	Classification	Classification Level	Markings (Not all inclusive)	Distribution Statements	Distribution Statement "category"	Addressees list	Methods Contractor is Directed to Provide Deliverables to the Government
Examples include: Technical Export Controlled Financial Privacy	Includes: Unclassified Classified	Includes: CONFIDENTIAL SECRET TOP SECRET	Examples Include: Export Controlled Atomic Energy NOFORN FOUO RESTRICTED FORMERLY RESTRICTED A Foreign Government Agreement Statements NATO	Examples Include: B C D E F	Examples include: Administrative/ Operational Use Specific Authority Critical Technology Export Control Foreign Government Information	Contains the list of addresses in Blk 14: Examples include: ACO PCO PMO DMO PMO IDE	Examples include: Mail Email Upload to Requiring Activity Integrated Development Environment
N/A	Block 16	Block 16	Block 16	Block 9	Block 16	Block 14	Block 14 and 16

"Blocks" are in DD Form 1423- 1, Contract Data Requirements List; Examples are not inclusive

The Program Office/Requiring Activity includes DD Form 1423-1, Contract Data Requirements List to request contract data item deliverables; CDRL Form includes "blocks" to specify marking and dissemination instructions along with methods to deliver the information

- Examples are not inclusive

Covered Defense Information in Solicitations and Contracts

Government Furnished Information in a solicitation/contract

GOVERNMENT FURNISHED INFORMATION

ATTACHMENT J-2 **PR #** N00024-18-R-6200

PROGRAM T -10 TI-20	**CONTRACT NO.: TBD**	**DATE: 9 May 2018** **CODE: PMS 435**

LINE ITEM NUMBERS		**MOD**	**EQUIPMENT NOMENCLATURE EQUIPMENT DESIGNATOR DOCUMENT TITLE DOCUMENT NUMBER**	**(5)**					**DOC DATE**	**GFI DUE DATE**
SCHEDULE	**A/C**			**VOL**	**PRT**	**REV**	**CHG**	**SUP**		
(1)	**(2)**	**(3)**	**(4)**						**(6)**	**(7)**
			Interface Control Drawing, 8217165 NSSN Class Submarine Structurally Integrated Enclosure			B			5/1/2009	Upon issue of RFP
			Interface Control Drawing, NAVSEA 7225771 Universal Modular Mast (UMM)			E			4/14/2001	
			SSN 780-783 C3I System Interface Control Document (ICD/IDD) Interface Design Document, Between ESM Subsystem and Imaging System, ESM 77C733539			B			3/16/2009	
			VIRGINIA Class TI16 External Interface Control Document (E-ICD) Between Imaging and Electronic Warfare Support (ES), PMS435-ICD-IM/ESM-002-TI-16						3/1/2015	
			Interface Control Document (ICD) MMM Antenna Control Unit (ACU)							
			Interface Design Document (IDD) MMM Antenna Control Unit (ACU) - Interface Requirements Specification (IRS)							

NAVSEA 4340/2 (REV. 6-90) PAGE 1 OF 23

Example of the type of Covered Defense Information when it is provided in a solicitation; List of controlled technical information spans 23 Pages

* List is Contained in publically released solicitation

Identification and Marking of Covered Defense Information

Statement of Work (Section C)

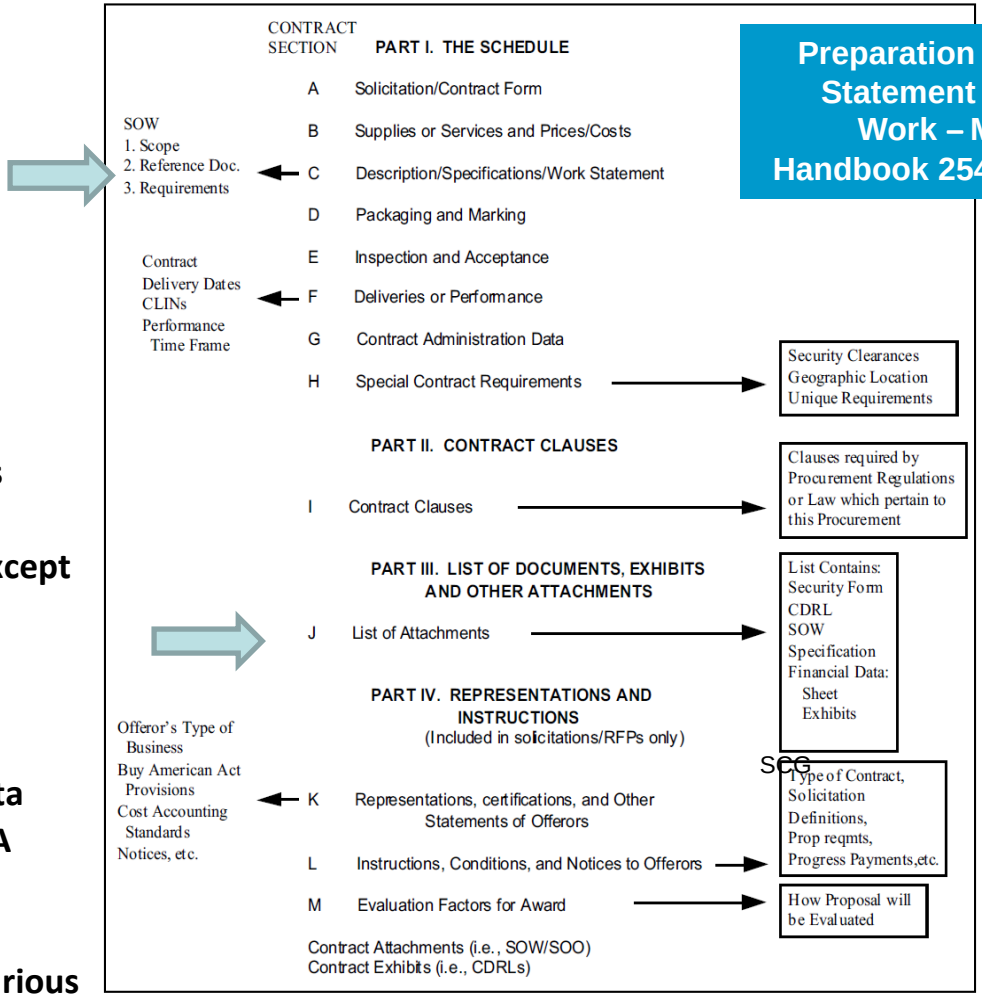
- Prepared by Program Office (PM)/ Requiring Activity (RA)

Contract Clauses (Section I),

- Prepared by Contracting Officer
- FAR Clause 52.204-2, when contract involves access to Confidential, Secret, or Top Secret information
- FAR Clause 52.204-21, when contract involves Federal Contract Information
- DFARS Clause 252.204-7012 in all contracts except COTS

List of Attachments (Section J)

- Attachments collected by Program Office
- Data deliverables as identified in Contract Data Requirements List (CDRL): Prepared by PM/RA
- Security Classification Guides
- Specifications: Prepared by PMO/RA
- Other Government Furnished Information: Various



Typical locations where you can find covered defense information is in a solicitation / contract

Example of Marking Directions for Controlled Technical Information

A Cooperative Program Example

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
A012	SOFTWARE REQUIREMENTS SPECIFICATION (SRS)/ INTERFACE REQUIREMENTS SPECIFICATION (IRS)	

4. AUTHORITY (Data Acquisition Doc. No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81433A	SOW Paragraphs A.2.1, A.6.3, B.2.1, D.3.2,F.8	PMS425

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMSSN
LT	D	ASREQ	SEE BLOCK 16

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQ SUBMSSN
A	N/A	SEE BLOCK 16

16. REMARKS

BLOCK 4: DI-IPSC-81434A contains the IRS requirements to be included in the SRS.

BLOCK 9: DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD Contractors only for Administrative or Operational use, 5 July 2017. Other requests shall be referred to Program Executive Office, Submarines, PMS 425.

Release to Australia authorized under the BYG-1 Armament Cooperative Program.

WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec. 2751 et seq.) or the Export Administration Act of 1979, as amended, Title 50 U.S.C., App 2401, et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate per the provisions of OPNAVINST 5230.25.

The information is furnished upon the condition that it or knowledge of its possession will not be released to another nation without specific authority from the Department of the Navy of the U.S.; that it will not be used for other than military purposes; that individual or corporate rights originating in the information, whether patented or not, will be respected and; that the information will be provided the same degree of security afforded it by the Department of Defense of the U.S. Regardless of any other markings on this document, it may not be declassified or downgraded without the written approval of the originating U.S. agency.

BLOCKS 10, 12 and 13: Draft submittal fifteen (15) days prior to PDR. Final submittal at CDR closure.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
PMS425	1	1	0
NUWC DMO	1	1	0
PMS425DMO	1	1	0
PCO026	1	1	0
ACO	1	1	0

- **Information can be shared with:**
  - **DoD and DoD contractors**
  - **Australia, in accordance with the PMO agreement**
- **Information has export control requirements**
- **International markings are currently not consistent with US Markings**

* CDRL located in publically released solicitation

Adequate Security to Safeguard Covered Defense Information

To provide adequate security to safeguard covered defense information:

DFARS 252.204-7012 (b) Adequate Security. … the contractor shall implement, at a minimum, the following information security protections:

****

(b)(2)(ii)(A): The contractor shall implement NIST SP 800-171, Protecting CUI in Nonfederal Systems and Organizations, as soon as practical, but not later than December 31, 2017

****

(b)(3): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required

DFARS 252.204-7012 directs <u>how</u> the contractor shall protect covered defense information; The requirement <u>to</u> protect it is based in law, regulation, or Government wide policy.

Implementing NIST SP 800-171 Security Requirements

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, but some may require security-related software or hardware. For companies new to the requirements, a reasonable approach would be to:

1. **Examine each of the requirements to determine**
   - **Policy or process requirements**
   - **Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)**
   - **IT configuration requirements**
   - **Any additional software or hardware required**

   The complexity of the company IT system may determine whether additional software or tools are required
2. **Determine which requirements can readily be accomplished by in-house IT personnel and which require additional research or assistance**
3. **Develop a plan of action and milestones to implement the requirements**

Approach to Implementing NIST SP 800-171 Requirements

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI
Basic (FIPS 200)	3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
	3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
								3.8.3			3.11.3	3.12.3		3.14.3
												(3.12.4)		
Derived (800-53)	3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.4		3.10.3			3.13.3	3.14.4
	3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.5		3.10.4			3.13.4	3.14.5
	3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.6		3.10.5			3.13.5	3.14.6
	3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.7		3.10.6			3.13.6	3.14.7
	3.1.7		3.3.7	3.4.7	3.5.7			3.8.8					3.13.7	
	3.1.8		3.3.8	3.4.8	3.5.8			3.8.9					3.13.8	
	3.1.9		3.3.9	3.4.9	3.5.9								3.13.9	
	3.1.10				3.5.10								3.13.10	
	3.1.11				3.5.11								3.13.11	
	3.1.12												3.13.12	
	3.1.13												3.13.13	
	3.1.14												3.13.14	
	3.1.15				Policy/Process			Policy or Software Requirement					3.13.15	
	3.1.16												3.13.16	
	3.1.17				Configuration			Configuration or Software						
	3.1.18													
	3.1.19				Software			Configuration or Software or Hardware						
	3.1.20													
	3.1.21				Hardware			Software or Hardware						
	3.1.22													

Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

- **To document implementation of NIST SP 800-171, companies should have a system security plan in place, in addition to any associated plans of action:**
  - **Security Requirement 3.12.4 (System Security Plan): Requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems**
  - **Security Requirement 3.12.2 (Plans of Action): Requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems, and to describe how and when any unimplemented security requirements will be met**

Alternative but Equally Effective Security Measures

See FAQ 59 - 62

- Per DFARS Clause 252.205-7012(b)(2)(ii)(B), if the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of -
  - Why security requirement is not applicable; OR
  - How an alternative but equally effective security measure is used to achieve equivalent protection
- When DoD CIO receives a request from a contracting officer, representatives in DoD CIO review the request to determine if the proposed alternative satisfies the security requirement, or if the requirement for non-applicability is acceptable
  - The assessment is documented and provided to the contracting officer, generally within 5 working days
  - If request is favorably adjudicated, the assessment should be included in the contractor's system security plan

Cloud Computing

Safeguarding Covered Defense Information and Cyber Incident Reporting
48 CFR Parts 202, 204, 212, and 252, DFARS Clause 252.204-7012

- Applies when a contractor uses an external cloud service provider to store, process, or transmit Covered Defense Information on the contractor's behalf
- Ensures that the cloud service provider:
  - Meets requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline
  - Complies with requirements for cyber incident reporting and damage assessment

Cloud Computing Services
48 CFR Parts 239 and 252, DFARS Clause 252.239-7010

- Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud
- Requires the cloud service provider to:
  - Comply with the DoD Cloud Computing Security Requirements Guide
  - Comply with requirements for cyber incident reporting and damage assessment

Cyber Incident Reporting

When a cyber incident occurs, the contractor/subcontractor shall:

- **Review contractor network(s) for evidence of compromise of covered defense information using contractor's available tools, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts**
- **Identify covered defense information that may have been affected**
- **If contract includes operationally critical support, determine if the incident affects the contractor's ability to provide operationally critical support**
- **Rapidly report directly to DoD via https://dibnet.dod.mil (within 72 hours)**
  - **Subcontractors provide incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor)**

A DoD-approved medium assurance certificate is required to access the reporting module.

Cyber Incident Reporting

Upon receipt of a cyber incident report —

- **The DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s) identified on the Incident Collection Format (ICF) via encrypted email;**
  the contracting officer(s) provide the ICF to the PM/requiring activity
- **DC3 analyzes the report to identify cyber threat vectors and adversary trends**
- **DC3 contacts the reporting company if the report is incomplete (e.g., no contract numbers, no contracting officer listed)**
- **DC3 may recommend that contracting officer request media from the contractor**

DFARS 204.7302 (d)

A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Cyber Incident Damage Assessment Activities

Purpose of the cyber incident damage assessment —

- **Determine impact of compromised information on U.S. military capability underpinned by the technology**
- **Consider how the compromised information may enable an adversary to counter, defeat, or reverse engineer U.S. capabilities**
- **Focus on the compromised intellectual property impacted by the cyber incident – not on the compromise mechanism**

DoD decision to conduct a cyber incident damage assessment —

- **Contracting officer verifies clause is included in the contract**
- **The Requiring Activity and the DoD Component damage assessment office (DAMO) will determine if a cyber incident damage assessment is warranted**

Contractor Compliance — Implementation of DFARS Clause 252.204-7012

- By signing the contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012
- It is the contractor's responsibility to determine whether it is has implemented NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)
  - The scope of DFARS Clause 252.205-7012 does not require DoD to 'certify' that a contractor is compliant with the NIST SP 800-171 security requirements
  - The scope of DFARS Clause 252.205-7012 does not require the contractor to obtain third party assessments or certifications of compliance
  - DoD does not recognize third party assessments/certifications of compliance
- Per NIST SP 800-171, federal agencies may consider the submitted system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a nonfederal organization information systems/networks.

Existing Oversight of DFARS Clause 252.204-7012
Defense Contract Management Agency (DCMA)

Actions DCMA will take in response to DFARS Clause 252.204-7012:

- **Encourage industry to adopt corporate, segment, or facility-level system security plans as may be appropriate in order to ensure more consistent implementations and to reduce costs**
- **Verify that system security plans and any associated plans of action are in place (DCMA will not assess plans against the NIST 800-171 requirements)**
- **If potential cybersecurity issue is detected –notify contractor, DoD program office, and DoD CIO**
- **During the normal Contract Receipt and Review process -verify that DFARS Clause 252.204-7012 is flowed down to sub-contractors/suppliers as appropriate**
- **For contracts awarded before October 2017 -verify that contractor submitted to DoD CIO notification of security requirements not yet implemented**
- **Verify contractor possesses DoD-approved medium assurance certificate to report cyber incidents**
- **When required, facilitate entry of government assessment team into contractor facilities via coordination with cognizant government and contractor stakeholders**

Strategies to Enhance Cybersecurity Measures Provided by DFARS Clause 252.204-7012 and NIST SP 800-171

DPC Memo (Nov 6, 2018), Subject: Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012

- **Provides acquisition personnel with framework of tailorable actions to assess the contractor's approach to protecting DoD CUI**
- **Provides guidance for reviewing system security plans and any NIST SP 800-171 security requirements not yet implemented**
- **Includes sample Contract Data Requirements Lists (CDRLs) and associated Data Item Descriptions (DIDs)**

ASD(A&S) Memo (Dec 17, 2018), Subject: Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base

- **Provides program offices and requiring activities with sample Statement of Work (SOW) language to be used in conjunction with DPC guidance**
- **Addresses access to/delivery of the contractor's system security plan, access to/delivery of the contractor's plan to track flow down of DoD CUI and plan to assess of compliance of Tier 1 Level suppliers**

Strategies to Enhance Cybersecurity Measures Provided by DFARS Clause 252.204-7012 and NIST SP 800-171

USD(A&S) Memo (Jan 21, 2019), Subject: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review

- DCMA will leverage review of contractor purchasing systems in accordance with DFARS Clause 252.244-7001, Contractor Purchasing System Administration, to:
  - Review contractor procedures to ensure contractual requirements for identifying/ marking DoD CUI flow down appropriately to their Tier 1 Level Suppliers
  - Review contractor procedures to assess compliance of Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171

USD(A&S) Memo (Feb 5, 2019), Subject: Strategically Implementing Cybersecurity Contract Clauses

- DCMA will apply a standard DoD CIO methodology to recognize industry cybersecurity readiness at a strategic level.
- DCMA will pursue, at a corporate level, the bilateral modification of contracts administered by DCMA to strategically (i.e., not contract-by-contract) obtain/assess contractor system security plans

See DPC Website at *https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance _and_enhancing_protections.html*

Resources - Defense Industrial Base (DIB) Cybersecurity Program

Mission - Enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

DIB CS Program is a public private cybersecurity partnership that:

- **Provides a collaborative environment for sharing unclassified and classified cyber threat information**
- **Offers analyst-to-analyst exchanges, mitigation and remediation strategies**
- **Provides companies analytic support and forensic malware analysis**
- **Increases U.S. Government and industry understanding of cyber threat**
- **Enables companies to better protect unclassified defense information on company networks or information systems**
- **Promotes cyber threat sharing between the U.S. Government and Industry**

DIB CS Construct

Trusted public-private cybersecurity partnership

Resources — Frequently Asked Questions (FAQs)

Quick Look for FAQ Topics	
Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7008 and 252.204-7012) • **General** Q1 – Q18 • **Covered Defense Information** Q19 – Q30 • **Operationally Critical Support** Q31 • **Safeguarding Covered Defense Information** Q32 – Q34 • **Cyber Incidents and Reporting** Q35 – Q45 • **Submission of Malicious Software** Q46 • **Cyber Incident Damage Assessment** Q47	**NIST SP 800-171** • **General Implementation Issues** Q49 – Q67 • **Specific Security Requirements** Q68 – Q98 **Cloud Computing** • **General** Q99 – 101 • **Cloud solution being used to store data on DoD's behalf (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services)** Q102 • **Contractor using cloud solution to store covered defense information (DFARS 252.204-7008 and 252.204-7012 apply)** Q103 – Q109
Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21) Q48	**Limitations on the use or disclosure of third-party contractor reported cyber incident information (DFARS Clause 252.204-7009)** Q47

Resources

- NIST Manufacturing Extension Partnership (MEP)
  - Public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers
  - Published "Cybersecurity Self-Assessment Workbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements", November 2017

  https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- Procurement Technical Assistance Program (PTAP) and Procurement Technical Assistance Centers (PTACs)
  - Nationwide network of centers/counselors experienced in government contracting, many of which are affiliated with Small Business Development Centers and other small business programs

  http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx
- Cybersecurity Evaluation Tool (CSET)
  - No-cost application, developed by DHS, provides step-by-step process to evaluate information technology network security practices

  https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Resources

- Cybersecurity in DoD Acquisition Regulations page at *(http://dodprocurementtoolbox.com/)* for Related Regulations, Policy, Frequently Asked Questions, and Resources, *June 26, 2017*
- DPC Website (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) and (https://www.acq.osd.mil/dpap/pdi/cyber/guidance_ for_assessing_compliance _and_ enhancing_protections.html)
- NIST SP 800-171, Revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf)
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf)
- DoDI 5230.24, Distribution Statements on Technical Documents (www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf)
- Cloud Computing Security Requirements Guide (SRG) (http://iasecontent.disa.mil/cloud/SRG/)
- DoD's Defense Industrial Base Cybersecurity program (DIB CS Program) (https://dibnet.dod.mil)

Questions? Submit via email at osd.dibcsia@mail.mil

Questions