Cybersecurity Challenges

Protecting DoD's Unclassified Information

Industry Information Day, June 23, 2017

Outline

- Protecting DoD's Unclassified Information – Regulations, Policy and Guidance
- Covered Defense Information
- Subcontractor Flowdown
- Adequate Security
- Cloud Environment
- Implementation Processes and Procedures
- Resources

Protecting DoD's Unclassified Information – Regulations, Policy and Guidance

Protecting DoD's Unclassified Information – Regulations, Policy and Guidance

Cybersecurity Policy and Guidance

- DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations"
- NIST "Framework for Improving Critical Infrastructure Cybersecurity"
- Federal Risk and Authorization Management Program (FedRAMP)
- "DoD Cloud Computing Security Requirements Guide" (SRG)

DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems"

DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," ***June 6, 2012***

- **Establishes policy for managing the security of unclassified DoD information on non-DoD information systems**
- **Applies to all unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems**
- **Requires that adequate security be provided for all unclassified DoD information on non-DoD information systems.**
  - **Appropriate requirements shall be incorporated into all contracts, grants, and other legal agreements with non-DoD entities**

NIST SP 800-53 and NIST SP 800-171

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations *(Revision 4, April 2013)*	NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations *(Revision 1, December 2016)*
• Catalog of security and privacy controls for federal information systems and organizations to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors	• Recommended requirements for protecting the confidentiality of CUI when: – CUI is resident in nonfederal information systems/ organizations – Information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies

NIST Cybersecurity Framework

The Cybersecurity Framework complements, and does not replace, an organization's risk management process and cybersecurity program

NIST "Framework for Improving Critical Infrastructure Cybersecurity"

(Version 1.0 published Feb 12, 2014, Draft Version 1.1, published Jan 10, 2017)

- **A risk-based approach to managing cybersecurity consisting of:**
  - **Framework Core: A set of activities, desired outcomes, and applicable references that provide a "common language" of industry standards, guidelines, and practices**
  - **Framework Functions: Identify, Protect, Detect, Respond, Recover; these functions provide a strategic view of the lifecycle of an organization's management of cybersecurity risk**
  - **Framework Profile - The alignment of standards, guidelines, and practices to the Framework Core – a roadmap for reducing cybersecurity risk**

Executive Order 13800 – "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017

- ***Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity… to manage the agency's cybersecurity risk.***

FedRAMP and the DoD Cloud Computing Security Requirements Guide

Federal Risk and Authorization Management Program (FedRAMP)

- Government-wide program that provides standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for the Federal Government
- Defines FedRAMP "Low", "Moderate", and "High" baselines – a tailored set of Controls/Control Enhancements (C/CEs) based on the Low, Moderate, and High baselines recommended in NIST SP 800-53

DoD Cloud Computing Security Requirements Guide

Version 1 Release 3 | 6 March 2017

- Outlines security model by which DoD will leverage cloud computing along with the security controls and requirements necessary for using cloud-based solutions
- Applies to DoD-provided cloud services and those provided by a contractor on behalf of the Department
- Defines security information impact levels that consider the potential impact should the confidentiality or the integrity of the information be compromised
- Addresses DoD use of FedRAMP Security Controls

Protecting DoD's Unclassified Information – Regulations, Policy and Guidance

Acquisition and Other Regulations, Policy and Guidance

- **FAR (48 CFR) Subpart 4.19 – "Basic Safeguarding of Contractor Information Systems" (see also FAR Subparts 7, 12, & 52)**
- **32 CFR Part 236, "DoD Defense Industrial Base Cybersecurity Activities"**
- **32 CFR 2002, "Controlled Unclassified Information"**
- **DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information"**
- **DoDI 5000.02, Enclosure 14, "Cybersecurity in the Defense Acquisition System"**
- **DFARS Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (see also DFARS Subparts 202, 212, & 252)**
- **DFARS Subpart 239.76, "Cloud Computing" (see also DFARS Subpart 252)**

48 CFR Parts 4, 7, 12 & 52 – Basic Safeguarding of Contractor Information Systems

FAR Clause 52.204-21, "Basic Safeguarding of Contractor Information Systems," ***Final Rule, effective June 2016***

- **Required for use in solicitations and contracts when the contractor or a subcontractor may have Federal contract information residing in or transiting through its information system**
- **Requires the contractor/subcontractor to safeguard Federal contract information on the Contractor's Internal Information System**
  - **Required Information Security Protections: Basic requirements and procedures as listed in clause (subset of 17 of the 110 requirements in NIST SP 800-171)**

Federal Contract Information – "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 Websites) or simple transactional information, such as necessary to process payments."

32 CFR Part 236, DoD Defense Industrial Base (DIB) Cybersecurity (CS) Activities

32 CFR Part 236, "[DoD] Defense Industrial Base (DIB) Cyber Security (CS) Activities," *Updated final rule published October 4, 2016*

- **The DoD DIB CS Program: A public-private cybersecurity partnership designed to:**
  - **Improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.**
  - **Enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems**
- **Final rule modifies the eligibility criteria to permit greater participation in the voluntary DoD DIB CS information sharing program**
- **Final rule mandates reporting of cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support**

32 CFR 2002, Controlled Unclassified Information

32 CFR Part 2002, "Controlled Unclassified Information," *Final rule effective November 14, 2016*

- **The National Archives and Records Administration (NARA), as the executive agent designated to oversee the Government-wide CUI program, issued regulation to establish policy on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements**
- **Affects Federal executive branch agencies that handle CUI and organizations that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency**
- **Directs use of NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality – at impact level-moderate, in accordance with FIPS 199 – on non-Federal information systems**

DoDM 5200.01, Volume 4 – DoD Information Security Program: Controlled Unclassified Information (CUI)

- DoDM 5200.01, Volume 4, provides guidance for the identification and protection of CUI
- Published on February 24, 2012, DoDM 5200.01 Vol 4 will be updated* to
  - Codify categories and subcategories of CUI
  - Specify unique markings
  - Outline process for handling unauthorized disclosures
  - Identification of particular training requirements for all DoD associated personnel
- During the interim, DoD Components will continue to follow and apply DoDM 5200.01 Vol 4 until the new version has been signed and published*

* As per USD(I) Memo, dated April 11, 2017, "Guidance on Implementation of Controlled Unclassified Information"

DoDI 5000.02, Enclosure 14 – Cybersecurity in the Defense Acquisition System

- **Establishes cybersecurity as a requirement for all DoD programs to be considered and implemented in all aspects of acquisition programs across the life cycle.**
  - **Acquisition workforce responsible for cybersecurity from the earliest research/ technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**
- **Scope of program cybersecurity includes:**
  - **Program information: Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system**
  - **Organizations and Personnel: Government program offices, prime and subcontractors, along with manufacturing, testing, depot, & training organizations**
  - **Networks: Government, Government support activities, and contractor owned and operated networks**
  - **Systems and Supporting Systems: The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and support systems**

Change 2 to DoDI 5000.02, Enclosure 14 issued Feb 2, 2017

DoDI 5000.02, Enclosure 14 – Cybersecurity in the Defense Acquisition System

Program Responsibilities:

- **What the Program Manager should pay attention to:**
  - Program information *(to include the identification and marking of),* organizations and personnel, enabling networks and systems, and supporting systems
- **Potential exploitation points that the PM will consider for the Program and the System:**
  - Government Program Organizations; Contractor Organizations and Environments, Software and Hardware; System Interfaces; Enabling and Support Equipment, Systems, and Facilities; and Fielded Systems
- **Activities to mitigate cybersecurity risks to program information:**
  - Appropriate classification, marking and understanding the exposure of the unclassified program information
  - Use of FAR/DFARS Clauses to protect information
  - Assessment of unclassified controlled technical information losses
  - Contractor and industry participation in the voluntary DIB CS Program

Protecting the DoD's Unclassified Information…

Information System Security Requirements

Contractor's Internal System

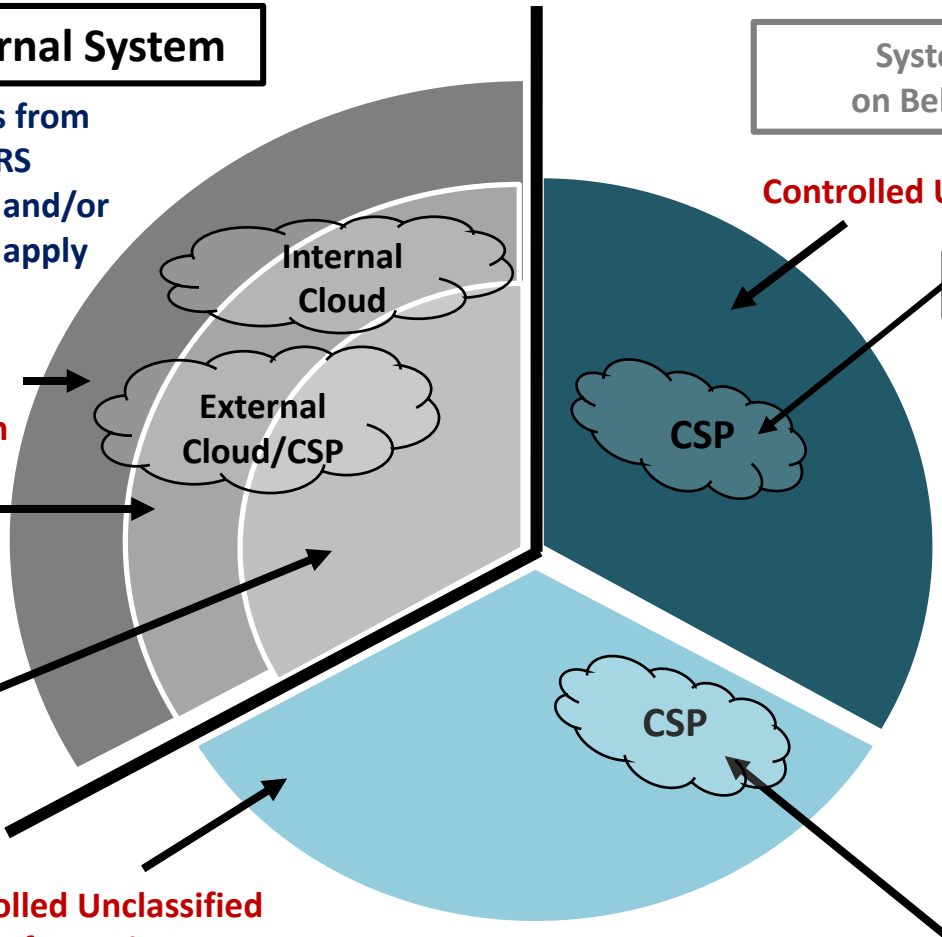
Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information



System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

DoD Owned and/or Operated Information System

Questions?

Protecting DoD's Unclassified Information – Regulations, Policy and Guidance?

Network Penetration Reporting and Contracting for Cloud Services

Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)

48 CFR Parts 202, 204, 212, 239 & 252:

		Provision/Clause Prescription
Safeguarding Covered Defense Information	– (p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information	→ All solicitations except COTs
	– (c) Section 252.204-7009, Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	→ Solicitations/contracts for services that support safeguarding/reporting
	(c) Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting	→ All solicitations/contracts except COTs
Contracting For Cloud Services	– (p) Section 252.239-7009, Representation of Use of Cloud Computing	→ Solicitations/contracts for IT services
	– (c) Section 252.239-7010, Cloud Computing Services	→

Commercially off-the-Shelf (COTS) Items versus Commercial Items

- **DFARS provision 252.204–7008 and DFARS clause 252.204–7012 are not prescribed for use in solicitations or contracts that are solely for the acquisition of commercially available off-the-shelf (COTS) items.**
- **COTS is a commercial item that has been sold in the commercial marketplace in substantial quantities, and is offered to the government in a contract or subcontract without modification**
  - **Procurements solely for the acquisition of COTS items are extremely unlikely to involve covered defense information or operationally critical support**
- **Commercial items include COTS, but also other commercial items that are or about to be available in the marketplace, but which also can be modified to meet Government requirements.**
  - **If a commercial item must be modified to meet Government requirements, such modification may require the use and safeguarding of covered defense information, or the resulting service could be operationally critical for DoD**

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

DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1. **Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractors internal information system or network**
2. **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**
3. **Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center**
4. **If requested, submit media and additional information to support damage assessment**
5. **Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information**

Implementing Guidance for "Network Penetration Reporting and Contracting for Cloud Services"

- **Procedures, Guidance, & Information (PGI) 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting,"** ***December 2015***
  - **Companion resource to the DFARS that contains internal DoD procedures, guidance and supplemental information to be used at the discretion of the contracting officer**
- **"Network Penetration Reporting and Contracting for Cloud Services … Frequently Asked Questions (FAQs)…,"** ***January 27, 2017***
  - **Answers to implementation questions raised by a variety of stakeholders to include: industry; contracting offices; requiring activities and program management offices; and cybersecurity professionals**
- **"Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012, Safeguarding Unclassified Controlled Technical Information,"** ***August 2015***
  - **Provides implementation/guidance for stakeholders involved in the conduct of damage assessment activities**

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

	Nov 18, 2013 *(Final Rule)*	Aug 26, 2015 / Dec 30, 2015 *(Interim Rules)*	October 21, 2016 *(Final Rule)*
Scope – What Information	• Unclassified Controlled Technical Information	• Covered defense information • Operationally Critical Support	• Revised/clarified definition for covered defense information
Adequate Security - Minimum Protections	• Selected controls in NIST SP 800-53	• Aug 2015 NIST SP 800-171	• NIST SP 800-171
Deadline for Adequate Security	• Contract Award	• Dec 2015 – As soon as practical, but NLT 31 Dec 17	• As soon as practical, but NLT 31 Dec 2017
Subcontractor/ Flowdown	• Include the substance of the clause in all subcontracts	• Include in subcontracts for operationally critical support, or when involving covered contractor information system	• Contractor to determine if information required for subcontractor performance retains identity as CDI

When Contractors are faced with implementing multiple versions of the clause, Contracting Officers may work with Contractors, upon mutual agreement, to implement the latest version of the clause

Covered Defense Information

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**

Covered Defense Information – Changes in Final Rule

Covered defense information means: Aug 2015
unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(2) Falls in any of the following categories:

(i) Controlled technical information.
(ii) Critical information
(iii) Export control
(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).

Covered defense information means: Oct 2016

- **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

CUI Registry – public registry of information that requires safeguarding or dissemination controls pursuant to/consistent w/ law, regulations, government-wide policies.

Identification and Marking of Covered Defense Information

Existing DoD policy/regulations require DoD to:

- **Identify covered defense information and mark information in accordance with DoD procedures for identification and protection of controlled unclassified information (CUI) found in DoDM 5200.01 Vol 4, DoD Information Security Program: CUI**
  - **Determine the appropriate marking for controlled technical information in accordance with the procedures for applying distribution statements on technical documents found in DoDM 5200.01 Vol 4 and DoDI 5230.24, Distribution Statements on Technical Documents**
- **Document in the contract (e.g., Statement of Work, CDRLs) information, including covered defense information, that is required to be developed for performance of the contract, and specify requirements for the contractor to mark, as appropriate, information to be delivered to DoD. (see, e.g., MIL-Handbook 245D, and Contract Data Requirements List (CDRL) (DD Form 1423))**

The contractor is responsible for:

- **Following the terms of the contract, which includes the requirements in the Statement of Work**

DoDI 5230.24 – Distribution Statements on Technical Documents

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***

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

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.

Identification and Marking of Covered Defense Information
Preparation of Statement of Work (SOW)

Statement of Work (Section C)

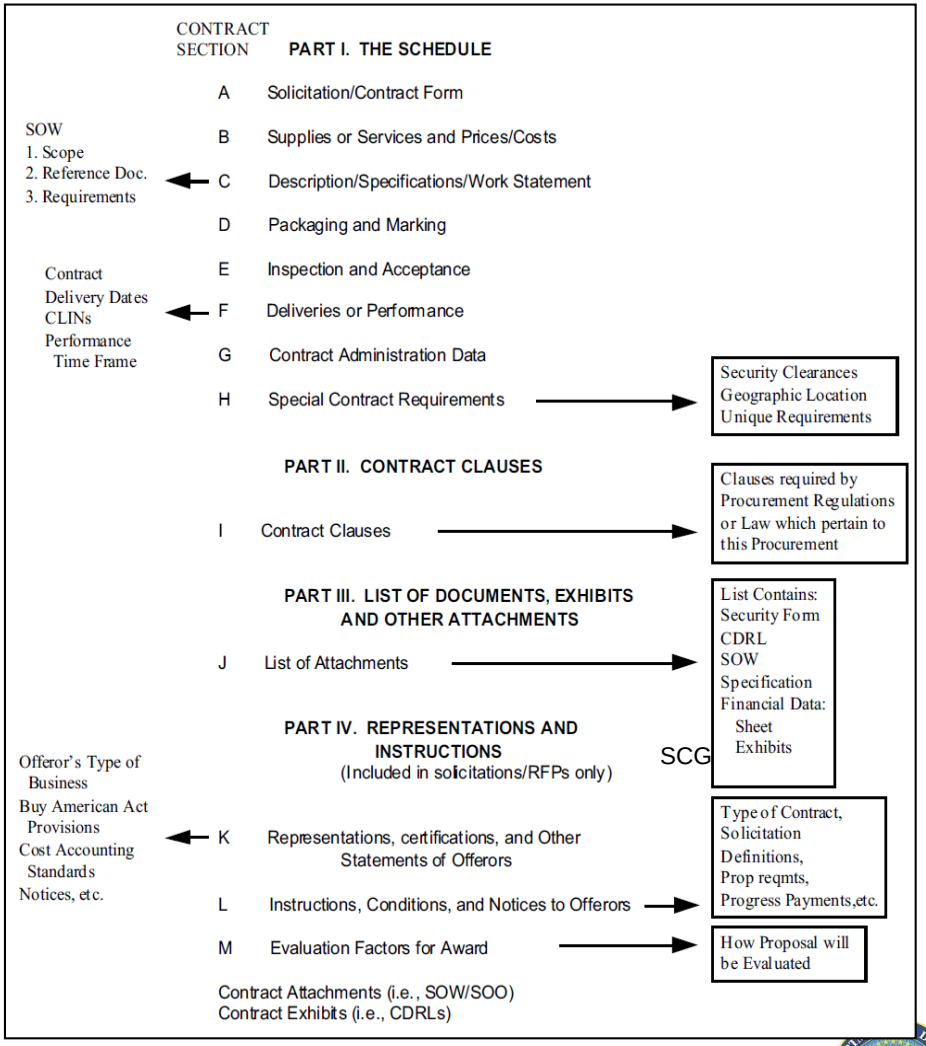
- Prepared by Requiring Activity

Contract Clauses (Section I), includes

- 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)

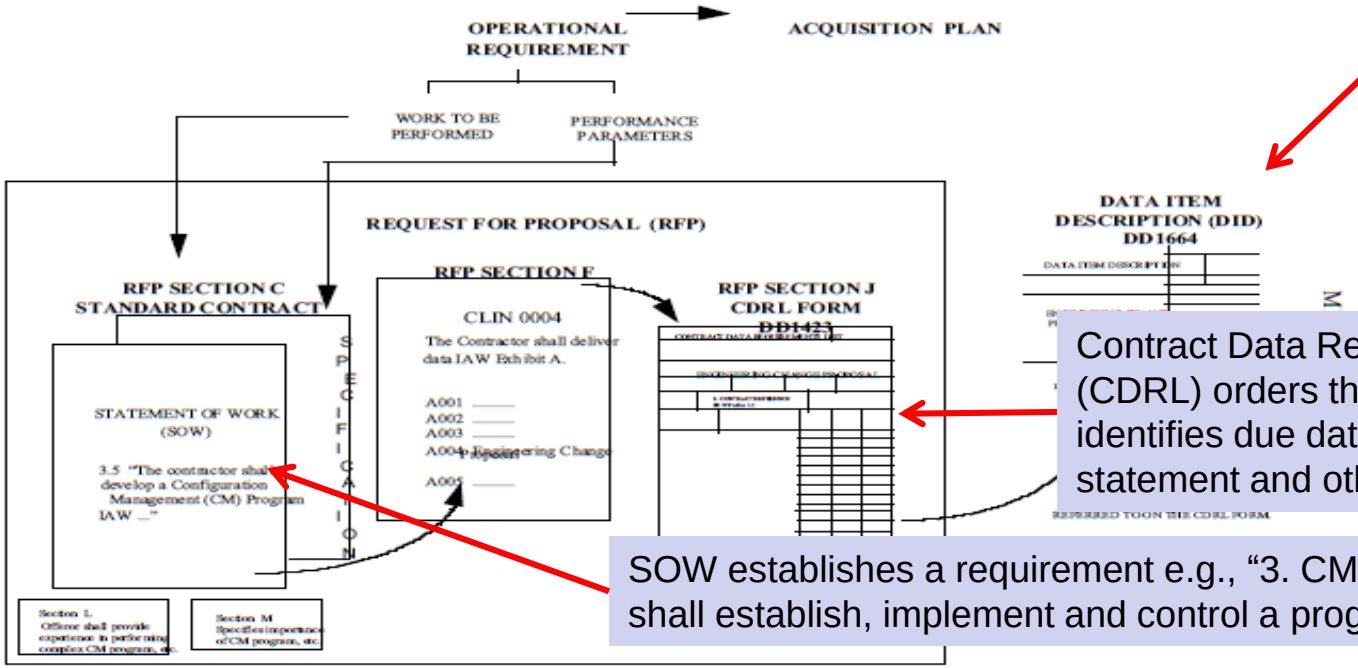
- Data deliverables as identified in Contract Data Requirements List (CDRL)
- Security Classification Guides
- Specifications
- Other Government Furnished Information



Identification and Marking of Covered Defense Information

Preparation of Statement of Work (SOW)

MIL-Handbook 245D applies to preparation of SOWs for projects and programs that have deliverables and/or services performed. It is written to implement the acquisition policies established in DoDD 5000.1



Data Item Description (DID) provides the format and content requirements for that Configuration Management (CM) item, with non-essential references tailored out of the DID.

Contract Data Requirements List (CDRL) orders the CM data item and identifies due date, distribution statement and other such parameters

SOW establishes a requirement e.g., "3. CM 5 The contractor shall establish, implement and control a program IAW…"

Example of Specification – SOW – CDRL - DID Relationship

Identification and Marking of Covered Defense Information
Contract Data Requirements List (CDRL) – Form DD1423

Department of Defense
INSTRUCTION

NUMBER 5230.24
August 23, 2012
Incorporating Change 1, Effective April 28, 2016

USD(AT&L)

SUBJECT: Distribution Statements on Technical Documents

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 5230.24 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5134.01 (Reference (b)) and pursuant to section 133 of title 10, United States Code (U.S.C.) (Reference (c)) to establish DoD policies, assign responsibilities, and prescribe procedures for marking and managing technical documents, including research, development, engineering, test, sustainment, and logistics information, to denote the extent to which they are available for secondary distribution, release, and dissemination without additional approvals or authorizations.

b. Establishes a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law.

c. Facilitates implementation of DoDD 5230.25 (Reference (d)) by enabling document originators to signify to what extent technical documents must be controlled in accordance with procedures of that Directive.

2. APPLICABILITY. This Instruction:

a. Applies to:

(1) The OSD, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

(2) Newly created, revised, or previously unmarked classified and unclassified technical documents generated or managed by all DoD-funded research, development, test, and evaluation

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Mana... Contrac...

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0701-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if does not display a currently valid OMB control number. Please DO NOT RETURN your form to the above address. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
	A	TDP ___ TM ___ OTHER IPSC

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
Distributed Common Ground System - Army	TBD	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
A002	Software Transition Plan (STRP)	

4. AUTHORITY *(Data Acquisition Document No.)*	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81429A	PWS Para 4.3.15	SFAE-IEW-DC

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
LT	D	ASREQ	SEE BLOCK 16	b. COPIES

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION	a. ADDRESSEE	Draft	Final Reg	Final Repro
		SEE BLOCK 16	SFAE-IEW-DC *ELECTRONIC SUBMITTAL		2	

16. REMARKS

BLOCK 9: The Government requires thirty (30) working days for review and comment. Final copy shall be submitted NLT thirty (30) working days after

SEE BLOCK 16

17. PRICE GROUP

18. ESTIMATED TOTAL PRICE

Item 9. For technical data, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDI 5230.24)

No change to existing marking procedures for contract deliverables – e.g., controlled technical information is marked in accordance with DoDI 5230.24

Subcontractor Flowdown

Subcontractor Flowdown

When should DFARS Clause 252.204-7012 flow down to subcontractors?

- **The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information**
- **The contractor shall determine if the information required for subcontractor performance is, or retains its identify as, covered defense information and requires safeguarding**
- **Flowdown is a requirement of the terms of the contract with the Government, which must be enforced by the prime contractor as a result of compliance with these terms**
  - **If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not be shared with the subcontractor or otherwise reside on it's information system**

The Department's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flowdown of information requiring protection.

Questions?

DFARS Clause 252.204-7012

Adequate Security

Adequate Security

DFARS 252.204-7012 (b) Adequate Security. **The Contractor shall provide adequate security on all covered contractor information systems. To provide 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, as soon as practical, but not later than December 31, 2017

****

(b)(3): [The Contractor shall] 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

NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

Why NIST SP 800-171?

- Developed for use on contractor and other nonfederal information systems to protect CUI* at confidentiality impact level "moderate", in accordance with FIPS 199 (32 CFR 2002.12)
- Requirements are performance-based, significantly reduce unnecessary specificity
  - Enables contractors to comply using systems and practices likely already in place
  - More easily applied to existing systems
- Provides standardized/uniform set of requirements for all CUI security needs
  - Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers)
  - Allows contractor to implement alternative, but equally effective, security measures to satisfy CUI security requirements

* For DoD, this applies to covered defense information as defined in DFARS 252.204-7012

NIST SP 800-171 – Performance-Based, More Flexible

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions authorized users are permitted to execute.	**AC-2 ACCOUNT MANAGEMENT** **The organization:** a. Identifies/selects the following types of information system accounts to support organizational missions/ business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **AC-3 ACCESS ENFORCEMENT** **The information system** enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **AC-17 REMOTE ACCESS** **The organization:** a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

NIST SP 800-171 – Performance-Based, More Flexible

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.8.9 Protect the confidentiality of backup CUI at storage locations.	**CP-9 INFORMATION SYSTEM BACKUP** **The organization:** a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. **Protects the confidentiality**, integrity, and availability **of backup** information **at storage locations.**
3.5.5 Prevent reuse of identifiers for a defined period. **3.5.6** Disable identifiers after a defined period of inactivity.	**IA-4 IDENTIFIER MANAGEMENT** **The organization manages information system identifiers by:** a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. **Preventing reuse of identifiers for** [*Assignment: organization-**defined** time **period***]; and e. **Disabling the identifier after** [*Assignment: organization-**defined** time **period of inactivity***].

An Approach to Implementing NIST SP 800-171

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**

   Note that the complexity of the company IT system may determine whether additional software or tools are required
2. **Determine which of 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													

Implementing NIST SP 800-171 Requirements

Cybersecurity Evaluation Tool (CSET)

- **CSET is a no cost application developed by the DHS's Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT)**
  - **The tool provides a systematic approach for evaluating an organization's security posture by guiding asset owners and operators through a step-by-step process to evaluate their industrial control system and information technology network security practices**
  - **To use the assessment tool, users select one or more government and industry recognized cybersecurity standards, including NIST SP 800-171.**
  - **CSET generates questions that are specific to those requirements and presents the assessment results in both summary and detailed form**

- **Download at https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET or to request a physical copy of the software, contact cset@dhs.gov**
- **Select "Advanced Mode" which will provide the option to select NIST 800-171**

NIST SP 800-171 Security Requirement 3.5.3 – Multifactor Authentication

- **Security Requirement 3.5.3 requires multifactor authentication for:**
  - **local and network access to privileged accounts and**
  - **network access to non-privileged accounts**
- **Multifactor authentication to an information system uses two or more methods of authentication involving:**
  - **Something you know (e.g., password)**
  - **Something you have (e.g., a One-Time Password generating device like a fob, smart-card, or a mobile app on a smart-phone); or**
  - **Something you are (e.g., a biometric like a fingerprint or iris)**
- **'Network access' means access to the information system through a network, e.g., local area network (LAN), wide area network (WAN), or Internet (e.g., remote access)**
- **'Local access' is a direct connection without use of a network**
- **Risk is NOT limited to just remote or privileged access**

NIST SP 800-171 Security Requirement 3.5.3 – Multifactor Authentication

- **Multifactor Authentication is NOT "Somewhere you are" (e.g. in a 'Controlled Access Facility') - "where" does not distinguish between individuals**
- **Multifactor Authentication is NOT required for access to a mobile device**
  - **Mobile devices are not considered a network device or information system**
  - **MFA is generally not supported by mobile devices**
  - **Covered defense information must be encrypted on mobile devices (3.1.19)**
  - **If used to access a covered contractor information system (e.g., via web access), the information system must provide for the required MFA to the system (which would be entered via the mobile device)**

NIST SP 800-171 Security Requirement 3.13.11 – FIPS Validated Encryption

- **Security Requirement 3.13.11 requires use of FIPS-validated cryptography when used to protect the confidentiality of CUI**
- **FIPS-validated cryptography means the cryptographic module has been tested and validated to meet FIPS 140-1 and -2 requirements**
- **FIPS-validated cryptography is required only to protect CUI and only when transmitted or stored outside the protected environment (including wireless/remote access) of the covered information system if not separately protected (e.g., by a protected distribution system)**
  - **FIPS validated encryption is required due to the high failure rate experienced during validation process**
  - **Encryption used for other purposes, such as within applications or devices, within the protected environment of the covered information system does not need to be FIPS-validated**

NIST SP 800-171 Security Requirement 3.13.11 – FIPS Validated Encryption

- **Application of a patch that 'invalidates' FIPS validated encryption (since the encryption module "with the patch" has not been validated by NIST) should be addressed as a temporary deficiency in a plan of action per NIST SP 800-171 requirement 3.12.2**
- **Software/hardware upgrades essential for operations, that invalidate the FIPS certification, can be addressed as a temporary deficiency per NIST SP 800-171 requirement 3.12.2**
- **Enduring 'specific' exceptions to FIPS validation can be addressed in the SSP per NIST SP 800-171 requirement 3.12.4**

Questions?

Adequate Security

Cloud Environment

Cloud Computing

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

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

DFARS Clause 252.204-7012 – "Security requirements equivalent to FedRAMP Moderate baseline"

- **NIST SP 800-171 was not developed to accommodate the additional security requirements necessary to protect information when using an external Cloud Service Provider.**
  - **The FedRAMP "moderate" baseline was developed to include these requirements.**
- **The contractor is required to ensure that the cloud services contracted to process and store covered defense information meet the same requirements as the FedRAMP "moderate" baseline.**
  - **The contractor is not required to, or precluded from, use of a CSP service authorized/approved by the FedRAMP program**
- **The contractor can ensure that the cloud provider meets security requirements equivalent to FedRAMP "moderate" in the same way the contractor would normally ensure any services or product being contracted for will meet his requirements. The contractor may:**
  - **Use a CSP service approved by FedRAMP at the moderate level**
  - **Use a similar service that has not formally been approved by FedRAMP, if the CSP can demonstrate to the contractor that it is equivalent**

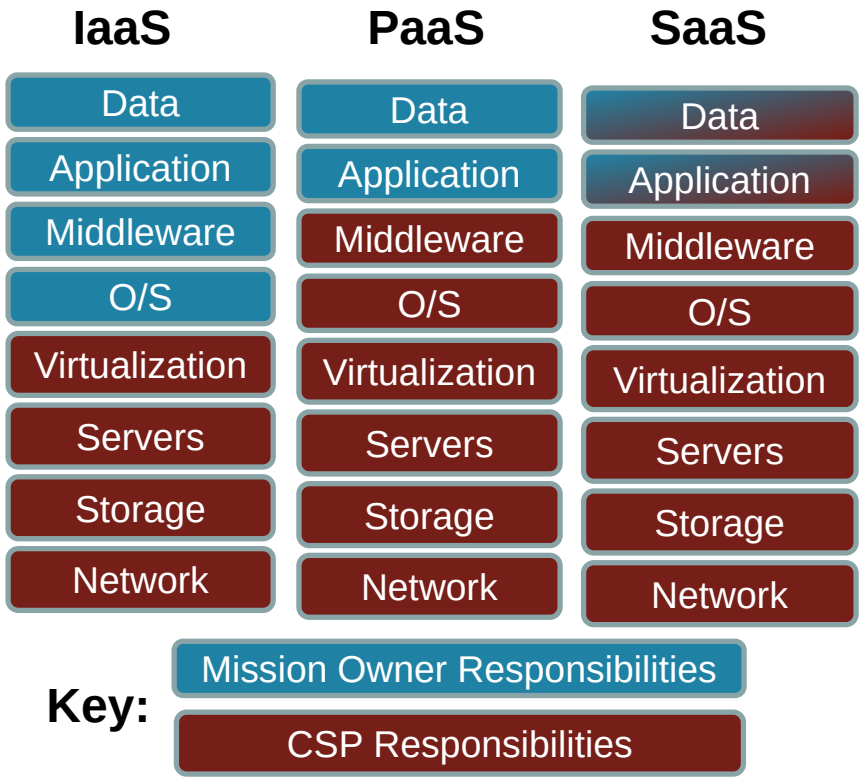
DFARS 252.204-7012 Requirements for Cloud Computing

- **Per DFARS 252.204-7012 (b)(2)(ii)(D), the contractor shall require and ensure that the cloud service provider (CSP) meets:**
  - **Security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) "moderate" baseline and**
  - **Complies with requirements in paragraphs (c) through (g) for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment**

- **In most cases, the contractor will not actually 'flow down' the DFARS clause to the CSP, but must ensure, when using a CSP as part of its covered contractor information system, that the contractor can continue to meet the DFARS clause requirements, including the requirements in DFARS 252.204-7012 (c)-(g)**
- **If the CSP is considered a subcontractor for the contract effort and will be handling covered defense information, then DFARS clause 252.204-7012 would flow down, but this would not be typical**

Typical Cloud Service Provider (CSP) Responsibility Model

CSP responsibilities will vary depending on the cloud service model being acquired



- **The CSP shall implement requirements for cyber incident reporting, malicious software submission, media preservation/ protection, access to additional information/equipment necessary for forensic analysis, and cyber incident damage assessment activities, for which they are capable of delivering/observing**

Example 1: If the CSP observes a cyber incident, it should report the incident

Example 2 : If the CSP is providing IaaS and cannot observe a cyber incident on the customers application or data, it will not be able to report the incident

I – Infrastructure P – Platform S – Software aaS – as a Service

Questions?

Cloud Environment

Implementation Processes and Procedures

Implementation Processes and Procedures

- **Alternative but Equally Effective Security Measures**
- **Contractor Compliance and Demonstrating Implementation of NIST SP 800-171**
- **Cyber Incident Reporting**
- **Malware Submission**
- **Cyber Incident Damage Assessment Activities**
- **Tracking DFARS Clause 252.204-7012 Implementation**

Alternative but Equally Effective Security Measures

Alternative but Equally Effective Security Measures

- **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**

Contractor Compliance and

Demonstrating Implementation of NIST SP 800-171

Compliance with DFARS Clause 252.204-7012 and Implementation of NIST SP 800-171

- **DFARS Clause 252.204-7012 requires contractors/subcontractors to:**
  - **Safeguard covered defense information,**
  - **Report cyber incidents,**
  - **Submit malicious software, and**
  - **Support damage assessment**
  - **Flow down the clause**
- **By signing the contract, the contractor agrees to comply with contract terms**
  - **If oversight related to these requirements is deemed necessary, then it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract**
- **To safeguard covered defense information, the Contractor shall implement NIST SP 800-171, as soon as practical, but not later than Dec 31, 2017**
  - **The system security plan and any associated plans of action are the mechanism to demonstrate implementation of NIST SP 800-171**

Contractor Compliance and Demonstrating Implementation of NIST SP 800-171

Q: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A: The DFARS rule did not add any unique/additional requirement for the Government to monitor contractor implementation of required security requirements.

Q: Will the DoD certify that a contractor is compliant with required security requirements?

A: No.

Q: Is a 3rd Party assessment or certification of compliance required?

A: 3rd party assessments or certifications of compliance are not required, authorized, or recognized by DoD. By signing the contract, the contractor agrees to comply with the terms of the contract. Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Using the System Security Plan (SSP) to Demonstrate Implementation of Security Requirements

NIST SP 800-171, Security Requirement 3.12.4 — 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.

- **The System Security Plan is used to document, for example:**
  - **Situations where requirements cannot practically be applied (non-applicable)**
  - **An alternative but equally effective security measure approved by DoD CIO**
  - **Exceptions to accommodate special circumstances (e.g., CNC machines and/or shop floor machines)**
  - **Individual, isolated or temporary deficiencies addressed by assessing risk and applying mitigations**
- **Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented** ***(see NIST SP 800-171, Security Requirement 3.12.2)***

Using the System Security Plan (SSP) to Demonstrate Implementation of NIST SP 800-171

- **When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements**
- **Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization**

Reference: NIST SP 800-171, Revision 1, Chapter 3

Q: How can the DoD/Requiring Activity consider an offeror's implementation of NIST SP 800-171 in the source selection process?

A: Approaches could include establishing the implementation of NIST SP 800-171 as a separate technical evaluation factor, or evaluating the implementation of NIST SP 800-171 on an acceptable or unacceptable basis

DCMA Role

DCMA – Where applicable, will verify that applicable cybersecurity clauses are in the contract. In addition, as part of normal software surveillance activities, personnel will engage with contractors to implement the following actions in regards to cyber-security:

- **Verify contractor has a system security plan**
- **Verify contractor submitted to the DoD CIO within 30 days of any contract award made through October 2017, a list/notification of the security requirements not yet implemented**
- **Verify contractor possesses DoD approved External Certificate Authority (ECA) issued medium assurance public key infrastructure (PKI) certificate**
- **If DCMA detects or is made aware of potential cybersecurity issue, DCMA will notify the contractor, DoD program office, and the DoD CIO**
- **As required, facilitate the entry of government external assessment team into applicable contractor facilities via coordination with cognizant government and contractor stakeholders**

Cyber Incident Reporting

Cyber Incident Reporting

What is a cyber incident?

A "Cyber incident" is an action(s) taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

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 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 in the cyber incident**
- **If contract contains requirement for operationally critical support, determine if the incident affects the contractor's ability to provide operationally critical support**
- **Rapidly report (within 72 hours of the discovery of an incident) directly to DoD**
  - **Subcontractors provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable**

DFARS Clause 252.204-7012(c)(1)

Cyber Incident Reporting

When reporting a cyber incident, contractors/subcontractors submit to DoD—

- **A cyber incident report via https://dibnet.dod.mil/**
- **Malicious software if detected and isolated**
- **Media or access to covered contractor information systems and equipment when requested by the requiring activity/contracting officer**

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 requiring activity(ies)**
- **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)**

Cyber Incident Reporting

The cyber incident report – contractors shall report as much of the following information as can be obtained within 72 hours of discovery of a cyber incident:

Company name and point of contact information	Date incident discovered
Data Universal Numbering System (DUNS) Number	Incident/Compromise narrative
Contract number(s) or other type of agreement affected or potentially affected	Type of compromise (unauthorized access, unauthorized release, unknown, not applicable)
Contact or other type of agreement clearance level	Description of technique or method used in cyber incident
Contracting Officer or other agreement contact	
USG Program Manager point of contact (address, position, telephone, email)	Incident outcome (successful compromise, failed attempt, unknown)
Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)	Impact to Covered Defense Information
Facility CAGE code	Impact on ability to provide operationally critical support
Incident location CAGE code	DoD programs, platforms or systems involved
Location(s) of compromise	Any additional information relevant to incident

OMB Information Collection # 0704_0489, expiration 10/31/2019

Malware Submission

Malicious Software (Malware) Submission

When a contractor discovers and isolates malicious software, the contractor will submit malware to DoD as follows —

- **Access the Malware Submission Form at https://dcise.cert.org/icf/**
  - **This site requires a DoD approved External Certificate Authority (ECA) issued medium assurance public key infrastructure (PKI) certificate**
- **Indicate the cyber incident report number associated with this malware**
- **Select the malware to upload and click submit**
- **Do NOT send malware to the contracting officer!**
- **If a contractor needs assistance, contact DCISE@dc3.mil**

Cyber Incident Damage Assessment Activities

Cyber Incident Damage Assessment Activities

DoD decision to conduct a cyber incident damage assessment —

- **Contracting officer verifies clause is included in the contract**
- **The DoD Component damage assessment office (DAMO) and Requiring Activity will determine if a cyber incident damage assessment is warranted**
- **Once the decision to conduct an assessment is made - the Requiring Activity will notify the contractor via the Contracting Officer, and the Contracting Officer will request media from the contractor**

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**

Tracking DFARS Clause 252.204-7012 Implementation

Tracking DFARS Clause 252.204-7012 Implementation

- **OUSD(AT&L) DPAP –** Tracks inclusion of DFARS Clause 252.204-7012 in new awards via Clause Compliance Scorecard. Detailed breakdown posted quarterly at: http://www.acq.osd.mil/dpap/pdi/eb/clause_compliance_scorecard.html
- **DoD CIO –** Receives contractor notifications of security requirements not implemented at the time of contract award
- **DoD Cyber Crime Center (DC3) –** Receives and tracks contractor cyber incident reports
- **OUSD(AT&L)DASD SE/DAMOs/JAPEC and MILDEPS/Agencies –** Track cyber incident damage assessment activities

Questions?

Implementation Processes and Procedures

Moving Forward

In the Works

- **Frequently Asked Questions (FAQs), Network Penetration Reporting and Contracting for Cloud Services,** ***Update Pending***
- **Procedures, Guidance, & Information (PGI) 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting,"** ***Revision currently ready for publication***
- **"Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012, Safeguarding Unclassified Controlled Technical Information,"** ***Under revision to align with Final Rule***
- **FAR Case 2017-016, "Controlled Unclassified Information,"** ***Open case to implement the National Archives and Records Administration (NARA) Controlled Unclassified information (CUI) program of E.O. 13556***
- **DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems,"** ***Under revision to align with FAR, DFARS, etc.***

In the Works – Updated FAQs

Quick Look for FAQ Topics	
Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7008 and 252.204-7012) • **General** Q1 – Q16 • **Covered Defense Information** Q17 – Q28 • **Operationally Critical Support** Q29 • **Safeguarding Covered Defense Information** Q30 – Q32 • **Cyber Incidents and Reporting** Q33 – Q42 • **Submission of Malicious Software** Q43 • **Cyber Incident Damage Assessment** Q44	**NIST SP 800-171** • **General Implementation Issues** Q46 – Q63 • **Specific Security Requirements** Q46 – Q63 **Cloud Computing** • **General** Q93 – 95 • **Cloud solution being used to store data on DoD's behalf** (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services, apply) Q96 • **Contractor using cloud solution to store covered defense information** (DFARS 252.204-7008 and 252.204-7012 apply) Q97 – Q102
Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21) Q41	**Limitations on the use or disclosure of third-party contractor reported cyber incident information** (DFARS Clause 252.204-7009) Q44

Resources

- Cybersecurity in DoD Acquisition Regulations page at *(http://dodprocurementtoolbox.com/)* for Related Regulations, Policy, Frequently Asked Questions, and Resources, *June 26, 2017*
- DPAP Website (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) for DFARS, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- NIST SP 800-171, Revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.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?