

Cybersecurity Challenges

Protecting DoD's Unclassified Information

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

January 2018





Outline

- **Protecting DoD's Unclassified Information**
- **DFARS Clause 252.204-7012 — Safeguarding covered Defense Information and Cyber Incident Reporting**
- **Adequate Security — NIST SP 800-171**
- **Cyber Incident Reporting and Damage Assessment**
- **Contractor Compliance**
- **Resources**





What DoD Is Doing

DoD has a range of activities that include both regulatory and voluntary programs to improve the collective cybersecurity of the nation and protect U.S. interests

- **Securing DoD's information systems and networks**
- **Codifying cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy**
- **Contractual requirements implemented through the Defense Federal Acquisition Regulation Supplement (DFARS)**
- **DoD's DIB Cybersecurity Program for voluntary cyber threat information sharing**
- **Leveraging security standards such as those identified in National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (*Revision 1 published Dec 2016*)**





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 contractor's 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**





Covered Defense Information – Definition

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

Existing DoD policy/regulations require DoD to:

- **Identify covered defense information and mark information in accordance with DoD procedures for controlled unclassified information (CUI) found in DoDM 5200.01 Vol 4, DoD Information Security Program: CUI**
- **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,**
 - **Specify requirements for the contractor to mark, as appropriate, information to be delivered to DoD**

The contractor is responsible for:

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





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.





Adequate Security for 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 Information 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





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, hardware, or other 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





Implementing NIST SP 800-171 Security 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 Security Requirements

- If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, 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(see 252.204-7008(c)(2)(i) and 252.204-7012(b)(2)(ii)(B))

-
- For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award
- (see 252.204-7012(b)(2)(ii)(A))





Cyber Incident Reporting

What is a cyber incident?

- 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 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 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 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**





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 has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)**
 - **DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements**
 - **Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD**
- **If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract**





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

- **NIST SP 800-171 was revised (Revision 1) in December 2016 to enable nonfederal organizations to demonstrate implementation or planned implementation of the security requirements with a “system security plan” and 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**





Implementation of NIST SP 800-171

- **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 to describe:**
 - **How and when any unimplemented security requirements will be met**
 - **How any planned mitigations will be implemented**
 - **How and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems**
- **The solicitation may require or allow elements of the system security plan, which demonstrates/documents implementation of NIST SP 800-171, to be included with the contractor's technical proposal, and may subsequently be incorporated (usually by reference) as part of the contract (e.g., via a Section H special contract requirement)**





Role of the System Security Plan and Plans of Action in Source Selection and Contract Formation / Administration

NIST SP 800-171, Revision 1, Chapter 3: 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 system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization

Examples of how a requiring activity may utilize the system security plan and associated plans of action include:

- Requiring that proposals i) identify any NIST SP 800-171 security requirements not implemented at the time award and ii) include associated plans of action for implementation
- Identifying in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award
- Identifying in the solicitation that the contractor's approach to providing adequate security will be evaluated in the source selection process





DIB CS Web Portal



Report a Cyber Incident

Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#)

[Report a Cyber Incident](#)



Apply to DIB CS Program

Cleared defense contractors apply to join the DIB CS Program for voluntary cyber threat information sharing. Access requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#)

[Apply to Program](#)

DIBNet.dod.mil



Login to DIB CS Information Sharing Portal

Current DIB CS Program participants login to the DIBNet portal. Access requires a DoD-approved medium assurance certificate. For more information please visit the [ECA website](#)

[DIB CS Program Participant Login](#)





Implementing NIST SP 800-171 – Where to Get Assistance

- **NIST MEP Handbook Cybersecurity Handbook (HB-162) (20 Nov 2017)**
 - The Handbook provides a step-by-step guide to assessing a small manufacturer's information systems against the security requirements in NIST SP 800-171 rev 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."
- **Draft NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information, (Public comments due 15 Jan 2018)**
 - This document is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- **Cybersecurity Evaluation Tool (CSET)**
 - No-cost application, developed by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control system and information technology network security practices





Resources

- **Cybersecurity in DoD Acquisition Regulations** page at <http://dodprocurementtoolbox.com/> for Related Regulations, Policy, Frequently Asked Questions, and Resources
- **DPAP Website**
<http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html> for DFARs, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- **Cybersecurity Evaluation Tool (CSET) - Download** at <https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET> or request physical copy of software at cset@dhs.gov — Select “Advanced Mode” to display option to select NIST 800-171
- **NIST Manufacturing Extension Partnership** at <https://www.nist.gov/mep>
- **The Procurement Technical Assistance Program (PTAP)** at <http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx>

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





Questions?





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**

