

Cybersecurity Challenges

Protecting DoD's Unclassified Information

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

July 31, 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





Cybersecurity Landscape

Verizon's 2019 Data Breach Investigations Report cites of 41,686 security incidents. 2,013 resulted in confirmed data breaches.

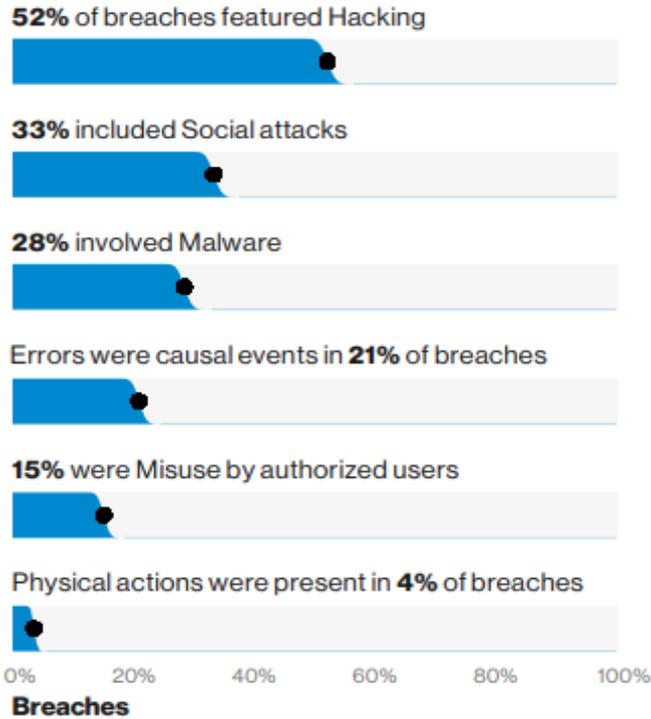


Figure 3. What tactics are utilized?

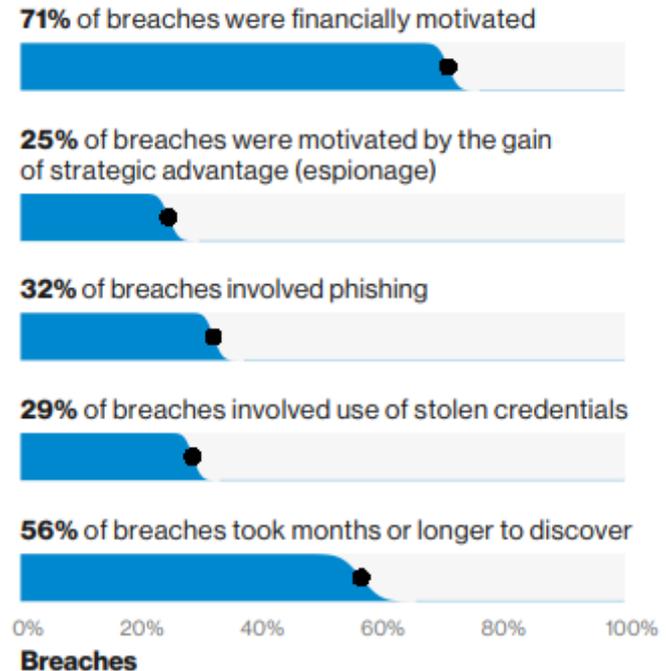


Figure 5. What are other commonalities?





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





Contractual Requirements in the FAR/DFARS

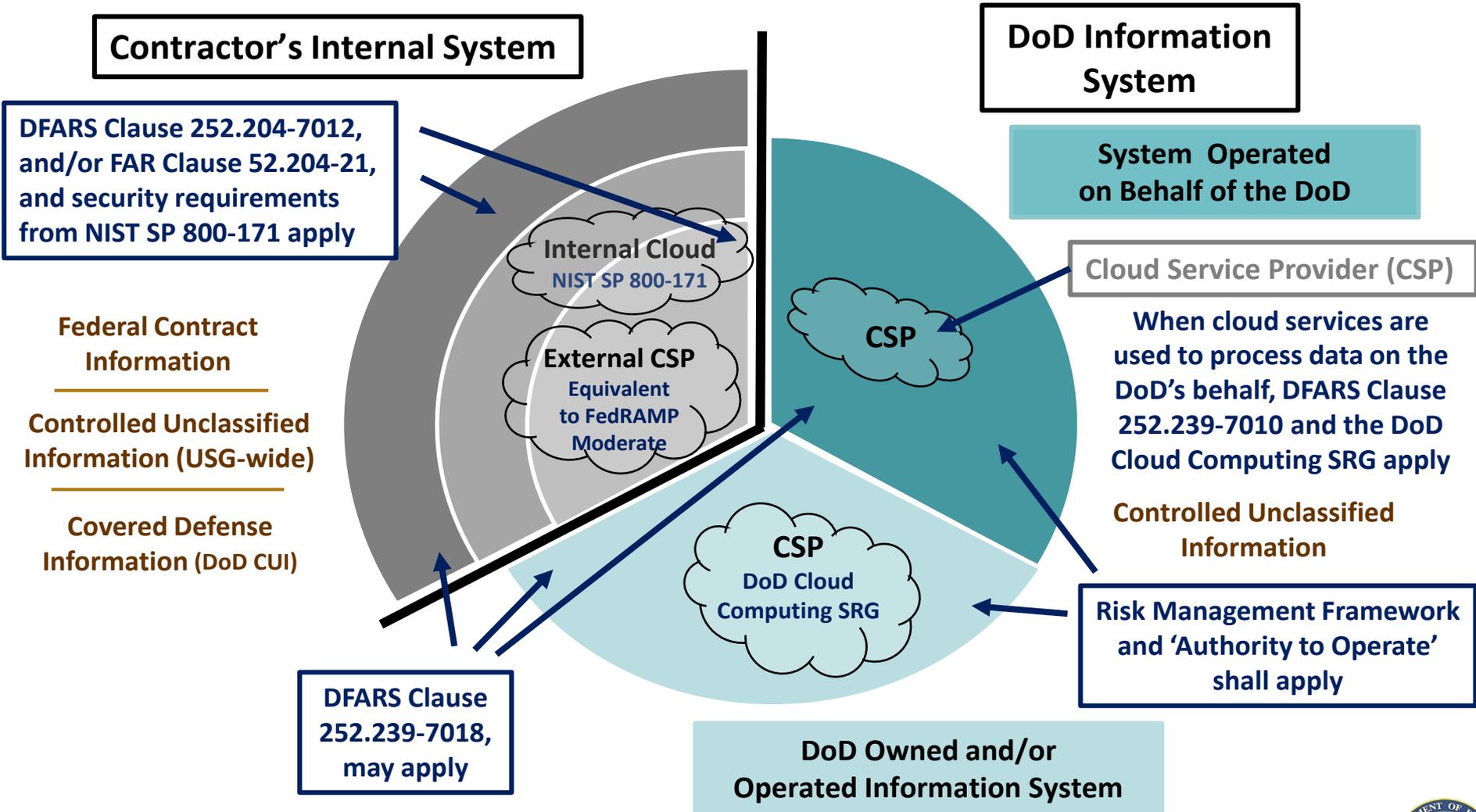
Implementing contractual requirements through the Federal Acquisition Regulation (FAR)/Defense Federal Acquisition Regulation Supplement (DFARS):

- **FAR Clause 52.204-2, Security Requirements (*for classified information*)**
 - Required when contract involves access to Confidential, Secret, or Top Secret information
 - Requires that a DD 254 be issued by the government with each Invitation for Bid, Request for Proposal, or Request for Quote
- **FAR Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems**
 - Requires 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)
- **DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (and DFARS Provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls)**





Protecting the DoD's Unclassified Information





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

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

DoD Policy was established in 1987

** 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 (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





DoDI 5230.24 Marking “Reasons”

DoDI 5230.24, August 23, 2012

12 Reasons contained in the Department’s policy for applying marking and dissemination statements to technical information

U.S. Government agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).”

- (1) This statement may be used on unclassified and classified technical documents.
- (2) Reasons for assigning Distribution Statement B are listed in Table 1.

Table 1. Reasons to Assign Distribution Statement B

Administrative or Operational Use	To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes including data or information intended for the sole purpose of operating and sustaining DoD weapon systems. This statement may apply to manuals, pamphlets, weapon system specifications, technical orders, technical reports, and other publications or technical data containing valuable technical or operational information.
Contractor Performance Evaluation	To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors. Assigned pursuant to subparts 203.104-4 of Reference (p).

Change 3, 10/15/2018

15

ENCLOSURE 4

DoDI 5230.24, August 23, 2012

Table 1. Reasons to Assign Distribution Statement B, Continued

Critical Technology	To protect information on technologies essential to the design, development, production, operation, application, or maintenance of an article or service that makes or could make a significant contribution to the military potential of any country, including the United States. This includes, but is not limited to, design and manufacturing knowledge, technical data, keystone equipment, and inspection and test equipment or data that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified. Assigned pursuant to subpart 800.209 of title 31, CFR (Reference (r)); ITAR; and EAR.
Export Controlled	To protect information subject to the provisions of Reference (d). Distribution “X” is superseded by issuance of this Instruction. Subsequent dissemination of formerly Distribution X documents shall display Distribution Statement C, with export control as the reason and shall be marked as directed in paragraph 8 a of Enclosure 3, unless changed by the controlling DoD office.
Foreign Government Information	To protect and limit distribution in accordance with the desires of and agreements with the foreign government that furnished the technical information. Assigned pursuant to chapter 15 of title 50, U.S.C. (Reference (s)) and Executive Order 13526 (Reference (t)).
Operations Security	To protect information and technical data that may be observed by adversary intelligence systems and to determine what indicators hostile intelligence systems may obtain that could be interpreted or assembled to derive critical information in time to be useful to adversaries. Assigned in accordance with DoDD 5205.02E (Reference (u)).
Premature Dissemination	To protect patentable information on systems or processes in the development or concept stage from premature dissemination. Assigned pursuant to section 205 of title 35, U.S.C. (Reference (v)).

Change 3, 10/15/2018

16

ENCLOSURE 4

DoDI 5230.24, August 23, 2012

Table 1. Reasons to Assign Distribution Statement B, Continued

Proprietary Information	To protect information not owned by the U.S. Government and marked with a statement of a legal property right. This information is received with the understanding that it not be routinely transmitted outside the U.S. Government. See Enclosure 5 of this Instruction for information on third party-imposed restrictive markings. Assigned pursuant to Public Law 104-294 (Reference (w)); section 1498(a) of title 28, U.S.C. (Reference (x)); title 17, U.S.C. (Reference (y)); section 1905 of title 18, U.S.C. (Reference (z)); and section 638 of title 15, U.S.C. (Reference (aa)).
Test and Evaluation	To protect the results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product. Assigned pursuant to part 311.8 of title 32, CFR (Reference (ab)).
Software Documentation	To protect technical data relating to computer software that is releasable only in accordance with the software license in subpart 227.72 of Reference (p). It includes documentation such as user’s or owner’s manuals, installation instructions, operating instructions, and other information that explains the capabilities of or provides instructions for using or maintaining computer software.
Specific Authority	To protect information not specifically included in the reasons listed in this table, but which requires protection in accordance with valid documented authority, such as Executive Orders, statutes, and regulations, such as the Atomic Energy Federal regulation. When filling in the reason, cite “Specific Authority (identification of valid documented authority).”
Vulnerability Information	To protect information and technical data that provides insight into vulnerabilities of U.S. critical infrastructure, including DoD warfighting capabilities vital to National Security that are otherwise not publicly available. Assigned pursuant to Public Law 107-296 (Reference (ac)).

c. “DISTRIBUTION STATEMENT C. (Secondary [optional]) Distribution authorized to U.S. Government agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).”

Change 3, 10/15/2018

17

ENCLOSURE 4

DoDI 5230.24 Marking and Dissemination Reason are consistent with Government Wide Policy Regulation and Law and the CUI Registry for DoD CUI Technical Information





Example of Marking and Dissemination Statements on Covered Defense Information

DISTRIBUTION STATEMENT D: Distribution

authorized to the Department of Defense and U.S. DoD contractors only (Administrative) (22 August 2018). Other requests for this document shall be referred to [insert name and code of Program Office/Requiring Activity].

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.

DESTRUCTION NOTICE: For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document. For classified documents, destroy in accordance with [insert organization instruction] or DoD 5220.22-M.

INTERFACE REQUIREMENTS SPECIFICATION

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors only (Administrative or Operational Use) (22 August 2018). Other requests for this document shall be referred to [insert name and code of Program Office/Requiring Activity].

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.

DESTRUCTION NOTICE: For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document. For classified documents, destroy in accordance with [insert organization instruction] or DoD 5220.22-M.





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 (GFI) in a solicitation/contract

GOVERNMENT FURNISHED INFORMATION

ATTACHMENT J-2

PR # N00024-18-R-6200

PROGRAM			CONTRACT NO.: TBD					DATE: 9 May 2018		
Q-10 TI-20								CODE: PMS 435		
LINE ITEM NUMBERS		MOD (3)	EQUIPMENT NOMENCLATURE EQUIPMENT DESIGNATOR DOCUMENT TITLE DOCUMENT NUMBER (4)	(5)					DOC DATE (6)	GFI DUE DATE (7)
SCHEDULE (1)	A/C (2)			VOL	PRT	REV	CHG	SUP		
			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							
			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)

Program Office/Requiring Activity Responsibilities:

- Must ensure GFI is properly marked prior to providing to Contractor in Request for Proposal and after contract award
- Technical information marked “Publically Released” “Distribution A” is not Controlled Technical Information nor is it covered defense information

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

Program Office should consider adding columns for “Distribution Statement” and “Reason” to know the marking for each GFI

* List is Contained in publically released solicitation





Covered Defense Information in Solicitations and Contracts

CDRLs Summary

CDRL#s	DID #	Title
A001	DI-MISC-80652	Technical Information Report
A002	DI-QCIC-80553A	Acceptance Test Plan
A003	DI-NDTI-80809B	Test/Inspection Report
A004	DI-SESS-80639D	Engineering Change Proposal (ECP)
A005	DI-IPSC-81431A	System/Subsystem Specification (SSS)
A006	DI-SESS-80858C	Supplier's Configuration Management Plan (SCMP)
A007	DI-SESS-81000E	Product Drawings/Models and Associated Lists
A008	DI-MISC-80508B	Technical Report/Study Services Report
A009	DI-DRPR-80651	Engineering Drawings
A010	DI-SESS-80776A	Technical Data Package
A011	DI-IPSC-80590B	Computer Program End Item Document
A012	DI-IPSC-81433A	Software Requirements Specification (SRS)
A013	DI-IPSC-81435A	Software Design Description (SDD)
A014	DI-IPSC-81441A	Software Product Specification (SPS)
A015	DI-IPSC-81442A	Software Version Description (SVD)
A016	DI-SESS-80640D	Request for Variation
A017	DI-SESS-81003E	Commercial Drawings/Models and Associated Lists
A018	DI-MGMT-81255	Production Status Report
A019	DI-CMAN-81253A	Configuration Status Accounting Information
A020	DI-MGMT-81889	Manufacturing Plan
A021	DI-ADMN-81249A	Conference Agenda
A022	DI-ADMN-81505	Report, Record of Meeting/Minutes
A023	DI-SESS-81757A	Design Review Information Package (DRIP)
A024	DI-CMAN-81516	As-Built Configuration List
A025	DI-NDTI-80603A	Test Procedure
A026	DI-SAFT-80106C	Health Hazard Assessment Report (HHAR)
A027	DI-HLSS-81070	Training Development Management Plan
A028	DI-IPSC-81432A	System/Subsystem Design Description (SSDD)
A029	DI-PSSS-81656A	Bill of Materials (BOM) for Diminishing Manufacturing Sources and Material Shortages Management
A030	DI-FNCL-81566C	Functional Cost-Hour Report
A031	DI-IPSC-81434A	System/Model Description/Requirements (SMDS)

Program Office / Requiring Activity typically uses the Contract Data Requirements List (CDRL) to order the data / information item and identifies due date, marking and distribution statement and other such parameters

Example of the type of Covered Defense Information that is ordered in a solicitation

- Example directs 73 types of data deliverables; largely technical
- Marking and dissemination statements may vary

CDRLs Summary

CDRL#s	DID #	Title
A066	DI-MGMT-82001	DoD Risk Management Framework (RMF) Package Deliverables
A067	DI-MGMT-81844	Information Assurance (IA) Test Plan
A068	DI-PSSS-80980B	Reliability-Centered Maintenance (RCM) Failure Modes and Effects Analysis (FMEA) Report
A069	DI-MGMT-82099	Open Systems Management Plan
A070	DI-DRPR-81242	Installation Control Drawings
A071	DI-MISC-81943	Trip/Travel Report
A072	DI-MGMT-82037	Enterprise Resource Planning (ERP) Content Plan
A073	DI-TMSS-81814A	IETM Content Plan

Program Office should consider adding columns for “Distribution Statement” and “Reason” directed on the deliverables

* Contained in publically released solicitation





Identification and Marking of Covered Defense Information

Statement of Work (Section C)

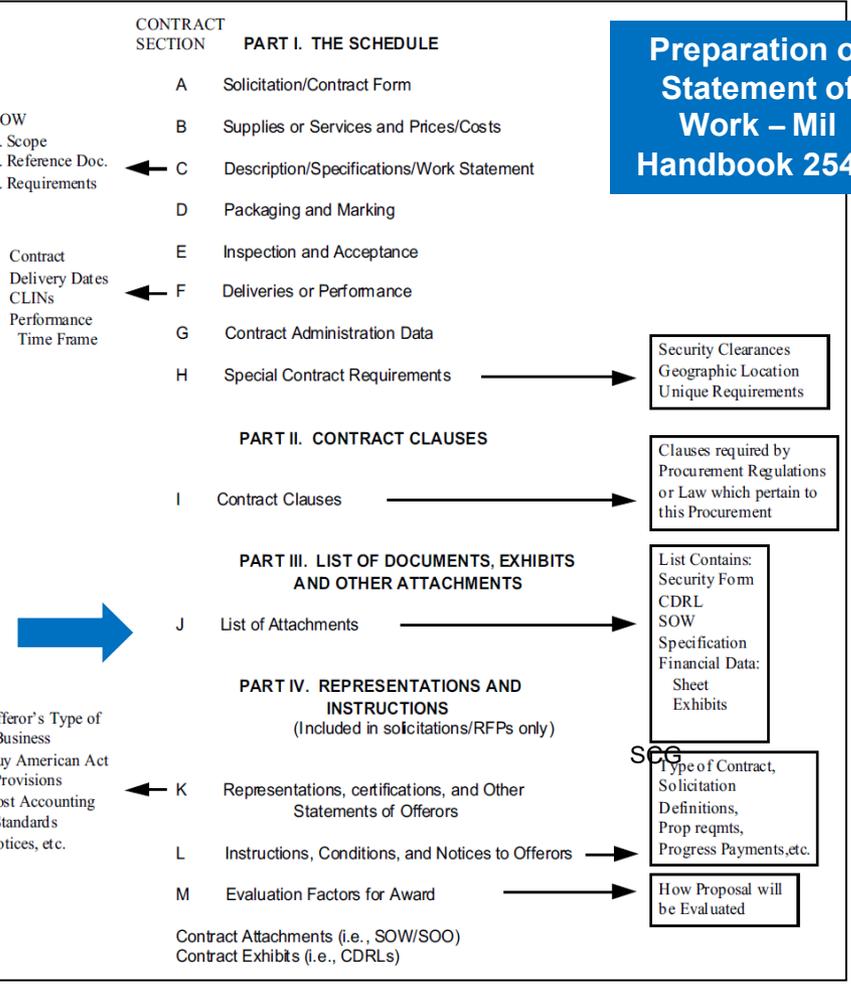
- Prepared by Program Office (PM)/ Requiring Activity (RA)

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

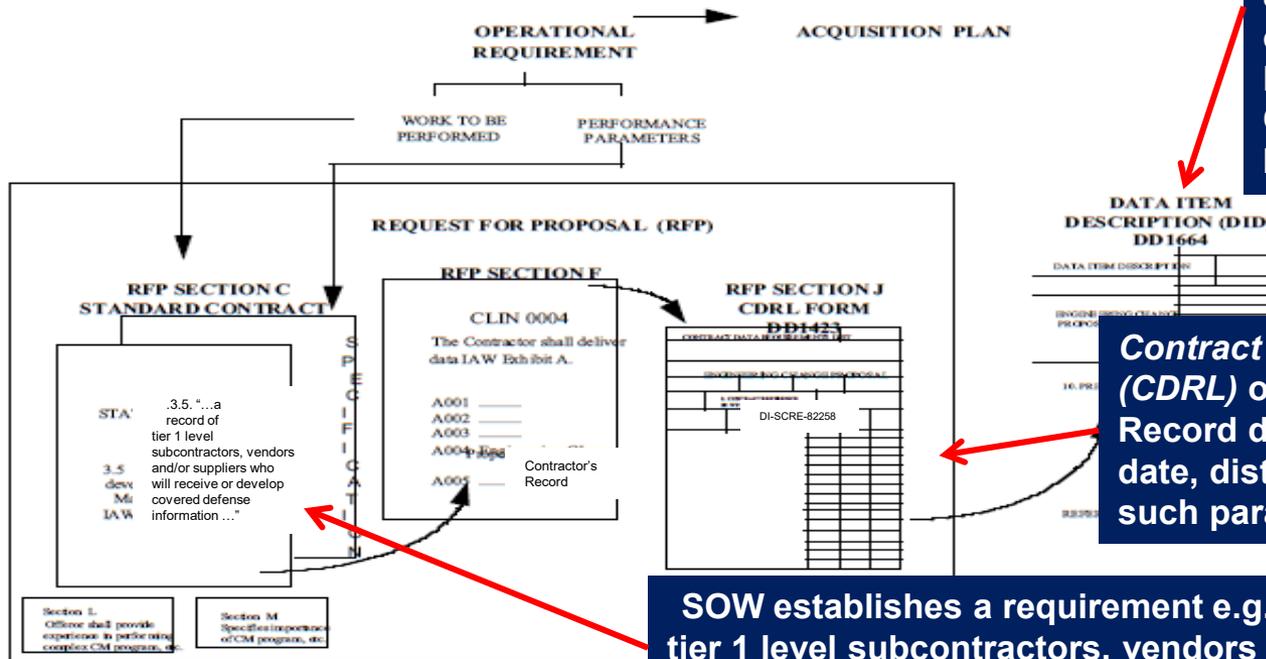




Identification and Marking of Covered Defense Information

Example of requesting delivery of the Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information

Data Item Description (DID) provides the format and content requirements for data item, with non-essential references tailored out of the DID. (e.g. DI-SCRE-82258, "Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information")



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

SOW establishes a requirement e.g., "3.5. "...a record of tier 1 level subcontractors, vendors and/or suppliers who will receive or develop covered defense information ..."

FIGURE 5. SPEC-SOW-CDRL-DID Relationship.





Identification and Marking of Covered Defense Information

Contract Data Requirements List (CDRL) – Form DD1423

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 Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed forms to the Government Printing Contracting Office for the Contract/PR No. listed in Block E.			
A. CONTRACT LINE ITEM NO. 0009	B. EXHIBIT A	C. CATEGORY TM	OTHER IPSC
D. SYSTEM/ITEM TACTICAL CONTROL SYSTEM	E. CONTRACT/PR NO. N00024-18-R-6407	F. CONTRACTOR TBD	
1. DATA ITEM NO. A019	2. TITLE OF DATA ITEM SOFTWARE PRODUCT SPECIFICATION (SPS)	3. SUBTITLE SPS and Software Build Deliveries	17. PRICE GROUP
4. AUTHORITY DI-IPSC-81429A	5. CONTRACT REFERENCE SEE BLK 16	6. REQUIRING OFFICE PMS425	18. ESTIMATED TOTAL PRICE
7. DD 250 REQ DD 250	8. DISTRIBUTION STATEMENT D	9. DATE OF DATE 11/13/18	
10. APP CODE N/A	11. DATE OF DATE 11/13/18	12. DATE OF FIRST SUBMISSION SEE BLK 16	
13. REMARKS BLOCK 4: All Build Delivery program pages shall be on CD ROM or DVD BLOCK 5: SOW Para 4.1.1, A.11.3, A.12.1.3, B.5.1, C.2.3.1, C.2.3.2, C.2.3.3, D.4, E.3.1, F.12.1. BLOCK 8: NUWC/NPT will sign DD250 for each build. 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 2007. 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 2320.25. 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: Interim Build Deliveries shall be as scheduled in the approved Project Planning Chart. For the Final Build Delivery, all supporting documentation, source code and all supporting files required to fully recompile and reconstitute the tactical software build for system deployment, executable object code and data files (including listings of all open hardware/software/firmware/documentation/PTRs), shall be submitted NLT thirty (30) days after the completion of the first Delivery Readiness Review (DRR). Thirty builds, including all data listed above, shall be as scheduled in the approved Project Planning Chart. BLOCK 14: Submittal shall be via Registered Mail. The Contractor shall only send electronic delivery notifications, not the data product to distribution addresses. Distribution and email addresses are provided in the attached "CDRL Distribution List".			
14. DISTRIBUTION Draft Reg Repr	15. TOTAL 0 5 0	16. APPROVED BY Angel Jacson, PMS425A3	16. APPROVED BY 3/10/18

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 Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed forms to the Government Printing Contracting Office for the Contract/PR No. listed in Block E.			
A. CONTRACT LINE ITEM NO. 0011	B. EXHIBIT A	C. CATEGORY TDP	OTHER IPSC
D. SYSTEM/ITEM Distributed Common Ground System - Army	E. CONTRACT/PR NO. TBD	F. CONTRACTOR TBD	
1. DATA ITEM NO. A007	2. TITLE OF DATA ITEM Software Transition Plan (STRP)	3. SUBTITLE	17. PRICE GROUP
4. AUTHORITY DI-IPSC-81429A	5. CONTRACT REFERENCE PWS Para 4.3.15	6. REQUIRING OFFICE SFAE-IEW-DC	18. ESTIMATED TOTAL PRICE
7. DD 250 REQ LT	8. DISTRIBUTION STATEMENT D	9. DATE OF DATE 11/13/18	
10. APP CODE BLOC	11. DATE OF DATE 11/13/18	12. DATE OF FIRST SUBMISSION SEE BLOCK 16	
13. REMARKS BLOCK 9: The Government requires thirty (30) working days for review and completion. Final copy shall be submitted NLT thirty (30) working days after	14. DISTRIBUTION Draft Reg Repr	15. TOTAL 0 5 0	16. APPROVED BY 3/10/18

Item 9. For technical information, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDI 5230.24); information is controlled when distribution statement is B-F

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

* Contained in publically released solicitation





Example* of Marking Directions for Controlled Technical Information

A Cooperative Program Example

1. DATA ITEM NO. A012		2. TITLE OF DATA ITEM SOFTWARE REQUIREMENTS SPECIFICATION (SRS)/ INTERFACE REQUIREMENTS SPECIFICATION (IRS)		3. SUBTITLE	
4. AUTHORITY (Data Acquisition Doc. No.) DI-IPSC-81433A		5. CONTRACT REFERENCE SOW Paragraphs A.2.1, A.6.3, B.2.1, D.3.2,F.8		6. REQUIRING OFFICE PMS425	
7. DD 250 REQ LT	9. DIST STATEMENT REQUIRED D (SEE BLK 16)	10. FREQUENCY ASREQ	12. DATE OF FIRST SUBMSSN SEE BLOCK 16		14. DISTRIBUTION
8. APP CODE A		11. AS OF DATE N/A	13. DATE OF SUBSEQ SUBMSSN 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-I 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.					
a. ADDRESSEE		b. COPIES			
	Draft	Reg	Repr		
			d		
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

* Contained 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 how the contractor shall protect covered defense information; The requirement to 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							Unclassified							24



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 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 252.204-7012 does not require DoD to 'certify' that a contractor is compliant with the NIST SP 800-171 security requirements**
 - **The scope of DFARS Clause 252.204-7012 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.**





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

Actions DCMA will take based on existing scope of 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
- 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, Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012 (Nov 6, 2018)**
 - Provides acquisition personnel with framework of tailorable actions to assess the contractor's approach to protecting DoD CUI
- **ASD(A&S) Memo, Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base (Dec 17, 2018)**
 - Provides program offices and requiring activities with sample Statement of Work language to be used in conjunction with DPC guidance
- **USD(A&S) Memo, Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review (Jan 21, 2019)**
 - Adds safeguarding of DoD CUI to DCMA review of contractor purchasing systems IAW DFARS Clause 252.244-7001, Contractor Purchasing System Administration
- **USD(A&S) Memo, Strategically Implementing Cybersecurity Contract Clauses (Feb 5, 2019)**
 - DCMA to apply a standard DoD CIO methodology to assess implementation of NIST SP 800-171 security requirements at a strategic level

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





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

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





Standard DoD Methodology to Strategically Assess Contractor Implementation of NIST SP 800-171

- DCMA will apply a standard DoD CIO methodology to assess contractor implementation of NIST SP 800-171 as required by DFARS clause 252.204-7012
- The *NIST SP 800-171 DoD Assessment* provides for a 'strategic assessment' at the information system(s)/company level
 - Enables DoD to share assessment results with DoD Components as alternative to contract-by-contract approach
- Objective assessment of NIST SP 800-171 security requirements, resulting in a score that reflects net effect of security requirements not yet implemented
- DCMA will conduct sixteen pilot *NIST SP 800-171 DoD Assessments* between June and August 2019 for 'pathfinder' companies with contracts for which DCMA provides contract oversight
- Upon completion of these sixteen pilot assessments, DoD will update its procedures and codify them in policy/regulation as required





Resources - Defense Industrial Base (DIB) Cybersecurity Program

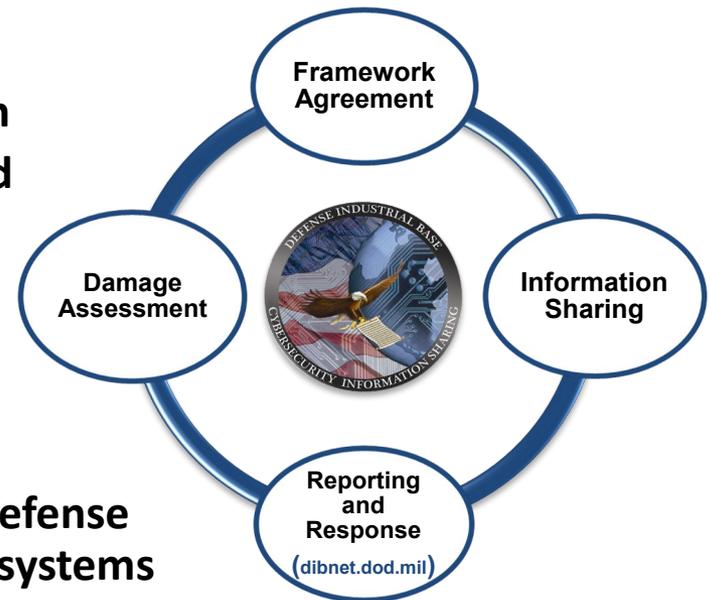
Mission - Enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

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**

See 32 CFR Part 236, DoD Defense Industrial Base Cybersecurity Activities

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

