Cybersecurity Challenges
Protecting DoD’s Unclassified Information

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

SOFIC 2019
Outline

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

Cyber threats targeting government unclassified information have dramatically increased

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

Internet Security Threat Report, Symantec 2018

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

CISCO Annual Cybersecurity Report 2018

Cybercrime will cost businesses over $2 trillion by 2019

Juniper Research

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

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

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

• Secure DoD’s information systems and networks

• Implement contractual requirements to secure contractor systems and networks through the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS)

• Leverage National Institute of Standards and Technology (NIST) information security standards and guidelines for federal and nonfederal information systems

• Codify cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy

• Promote cyber threat awareness through information sharing opportunities

The Department continues to focus on elevating cybersecurity in the DoD Supply Chain
Protecting the DoD’s Unclassified Information

**Contractor’s Internal System**
- DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21, and security requirements from NIST SP 800-171 apply

**DoD Information System**
- System Operated on Behalf of the DoD

**Cloud Service Provider (CSP)**
- Federal Contract Information
- Controlled Unclassified Information (USG-wide)
- Covered Defense Information (DoD CUI)
- Internal Cloud: NIST SP 800-171
- External CSP: Equivalent to FedRAMP Moderate

**DoD Owned and/or Operated Information System**
- CSP
- DoD Cloud Computing SRG
- Risk Management Framework and ‘Authority to Operate’ shall apply

**DFARS Clause 252.239-7018, may apply**

When cloud services are used to process data on the DoD’s behalf, DFARS Clause 252.239-7010 and the DoD Cloud Computing SRG apply
DFARS Clause 252.204-7012 - Requirements

Requires the program office/requiring activity to:

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

Requires the contractor/subcontractor to:

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

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

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

<table>
<thead>
<tr>
<th>Information Types</th>
<th>Classification</th>
<th>Classifications Level</th>
<th>Markings (Not all inclusive)</th>
<th>Distribution Statements</th>
<th>Distribution Statement “category”</th>
<th>Addresses list</th>
<th>Methods Contractor is Directed to Provide Deliverables to the Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples include:</td>
<td>Includes:</td>
<td>Includes:</td>
<td>Examples Include: Export Controlled</td>
<td>Examples Include:</td>
<td>Examples include:</td>
<td>Contains the list of addresses in Blk 14:</td>
<td>Examples include:</td>
</tr>
<tr>
<td>Technical</td>
<td>Unclassified</td>
<td></td>
<td>Atomic Energy</td>
<td>B</td>
<td>Administrative/Operational Use</td>
<td>Examples include:</td>
<td>Mail</td>
</tr>
<tr>
<td>Export Controlled</td>
<td>Classified</td>
<td>CONFIDENTIAL</td>
<td>NOFORN</td>
<td>C</td>
<td>Specific Authority</td>
<td>Examples include:</td>
<td>Email</td>
</tr>
<tr>
<td>Financial</td>
<td></td>
<td>SECRET</td>
<td>FOOU</td>
<td>D</td>
<td>Critical Technology</td>
<td>Examples include:</td>
<td>Upload to Requiring Activity Integrated Development Environment</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td>TOP SECRET</td>
<td>FORMERLY RESTRICTED</td>
<td>E</td>
<td>Export Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A Foreign Government</td>
<td>F</td>
<td>Foreign Government Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Agreement Statements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NATO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“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
## Government Furnished Information in a solicitation/contract

### GOVERNMENT FURNISHED INFORMATION

**ATTACHMENT J-2**

**PROGRAM 1**

<table>
<thead>
<tr>
<th>LINE ITEM NUMBERS</th>
<th>EQUIPMENT NOMENCLATURE</th>
<th>EQUIPMENT DESIGNATOR</th>
<th>DOCUMENT TITLE</th>
<th>DOCUMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCHEDULE (1)</td>
<td>VOLUME (5)</td>
<td>REV (6)</td>
<td>MOD (3)</td>
<td>MOD (3)</td>
</tr>
<tr>
<td>AVG (2)</td>
<td>PRRT (4)</td>
<td>CHG (7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUP (8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DOG DATE (9)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GIF DUE DATE (10)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Interface Control Drawing, 8217165 NSSN Class Submarine Structurally Integrated Endlosure
- Interface Control Drawing, NAVSEA 72257771 Universal Modular Mast (UMM)
- SSN 780-783 C3I System Interface Control Document (ICD/IDD)
- Interface Design Document, Between ESM Subsystem and Imaging System, ESM 77C735359
- Interface Control Document (ICD) MMM Antenna Control Unit (ACU)
- Interface Design Document (IDD) MMM Antenna Control Unit (ACU) - Interface Requirements Specification (IRS)

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

* List is Contained in publically released solicitation
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
Information can be shared with:
- DoD and DoD contractors
- Australia, in accordance with the PMO agreement

Information has export control requirements

International markings are currently not consistent with US Markings

* CDRL located in publically released solicitation

**Example of Marking Directions for Controlled Technical Information**

<table>
<thead>
<tr>
<th>BLOCK 2: 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>AS</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MA</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic (FIPS 200)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Derived (800-53)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.4</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
<td></td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.5</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
<td></td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.6</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
<td></td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.7</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
<td></td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.8</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.9</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.10</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.11</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.12</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Policy/Process</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Policy or Software Requirement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Configuration or Software</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Configuration or Software or Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software or Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Unclassified*
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

- 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

See FAQ 59 - 62
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
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.
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
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 252.205-7012 does not require DoD to ‘certify’ that a contractor is compliant with the NIST SP 800-171 security requirements.
- The scope of DFARS Clause 252.205-7012 does not require the contractor to obtain third party assessments or certifications of compliance.
- DoD does not recognize third party assessments/certifications of compliance.

Per NIST SP 800-171, federal agencies may consider the submitted system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a nonfederal organization information systems/networks.
Existing Oversight of DFARS Clause 252.204-7012
Defense Contract Management Agency (DCMA)

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

• Encourage industry to adopt corporate, segment, or facility-level system security plans as may be appropriate in order to ensure more consistent implementations and to reduce costs

• Verify that system security plans and any associated plans of action are in place (DCMA will not assess plans against the NIST 800-171 requirements)

• If potential cybersecurity issue is detected – notify contractor, DoD program office, and DoD CIO

• During the normal Contract Receipt and Review process - verify that DFARS Clause 252.204-7012 is flowed down to sub-contractors/suppliers as appropriate

• For contracts awarded before October 2017 - verify that contractor submitted to DoD CIO notification of security requirements not yet implemented

• Verify contractor possesses DoD-approved medium assurance certificate to report cyber incidents

• When required, facilitate entry of government assessment team into contractor facilities via coordination with cognizant government and contractor stakeholders

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

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

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

- Provides program offices and requiring activities with sample Statement of Work (SOW) language to be used in conjunction with DPC guidance
- Addresses access to/delivery of the contractor’s system security plan, access to/delivery of the contractor’s plan to track flow down of DoD CUI and plan to assess of compliance of Tier 1 Level suppliers
USD(A&S) Memo (Jan 21, 2019), Subject: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review

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

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

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

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

Trusted public-private cybersecurity partnership
## Quick Look for FAQ Topics

<table>
<thead>
<tr>
<th>Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7008 and 252.204-7012)</th>
<th>NIST SP 800-171</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General Q1 – Q18</td>
<td>• General Implementation Issues Q49 – Q67</td>
</tr>
<tr>
<td>• Covered Defense Information Q19 – Q30</td>
<td>• Specific Security Requirements Q68 – Q98</td>
</tr>
<tr>
<td>• Operationally Critical Support Q31</td>
<td></td>
</tr>
<tr>
<td>• Safeguarding Covered Defense Information Q32 – Q34</td>
<td>Cloud Computing</td>
</tr>
<tr>
<td>• Cyber Incidents and Reporting Q35 – Q45</td>
<td>• General Q99 – 101</td>
</tr>
<tr>
<td>• Submission of Malicious Software Q46</td>
<td>• Cloud solution being used to store data on DoD’s behalf (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services) Q102</td>
</tr>
<tr>
<td>• Cyber Incident Damage Assessment Q47</td>
<td>• Contractor using cloud solution to store covered defense information (DFARS 252.204-7008 and 252.204-7012 apply) Q103 – Q109</td>
</tr>
</tbody>
</table>

| 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

• 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

• 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


- NIST SP 800-171, Revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf)


- DoD’s Defense Industrial Base Cybersecurity program (DIB CS Program) (https://dibnet.dod.mil)

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