

# Cybersecurity Challenges

## Protecting DoD's Unclassified Information

**Train-the-Trainer Initiative**

**Unabridged**

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

**May 2018**



**Unclassified**



# Training Objectives

**Provide the information required to implement DFARS Clause 252.204-7012:**

- **What does the contractor need to know?  
Who should tell them?**
- **What does the contracting office need to know?**
- **What does the program office need to know?**
- **What does the security office need to know?**
- **Where can YOU go with questions?**





# Outline

- **Protecting DoD's Unclassified Information on the Contractor's Internal Information System**
- **FAR Clause 52.204-21, "Basic Safeguarding of Contractor Information Systems"**
- **DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**
  - **Implementation and Compliance**
- **Additional Regulations, Policy and Guidance**
- **Resources**





# Cybersecurity Landscape

**Cyber threats targeting government unclassified information have dramatically increased**

**Cybersecurity incidents have surged 38% since 2014**

*The Global State of Information Security ©  
Survey 2016*

**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*

**Cyber attacks cost companies \$400 billion every year**

*Inga Beale, CEO, Lloyds*

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

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

*2017 Data Breach Investigations Report, Verizon*

**Cybercrime will cost businesses over \$2 trillion by 2019**

*Juniper Research*

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

*NYSE Governance Services and security vendor Veracode*





# What DoD Is Doing

**DoD 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 Federal Acquisition Regulation (FAR) and Defense FAR 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 Systems and Organizations" (*Revision 1 published Dec 2016*)**





# Acquisition Regulations – Why FAR and DFARS?

- **Title 41, U.S. Code, “Public Contracts”, requires GSA, DoD, and NASA to issue and maintain a single Government-wide procurement regulation.**
- **The Federal Acquisition Regulation (FAR) System:**
  - **Codifies uniform policies/procedures for acquisition by all executive agencies**
  - **Consists of the FAR, and agency acquisition regulations that implement or supplement the FAR (e.g., Defense FAR Supplement (DFARS))**
  - **Establishes limits on other regulations relating to procurement, so that such regulations have to be part of the FAR system**
  - **Implements statutory requirement for higher level review for repetitive use of nonstandard contract clauses.**
- **A FAR, DFARS, or DoD Component Supplement is required (and published in the Federal Register for public comment) when procurement policies/procedures:**
  - **Relate to the expenditure of appropriated funds;**
  - **Have a significant effect beyond the internal operating procedures of DoD; or**
  - **Have a significant cost or administrative impact on contractors or offerors**





# Basic Safeguarding of Contractor Information Systems

## 48 CFR Parts 4, 7, 12 & 52

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

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

Federal Contract Information – “Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Websites) or simple transactional information, such as necessary to process payments.”





# DFARS — Network Penetration Reporting and Contracting for Cloud Services

**Safeguarding  
Covered  
Defense  
Information**

– (p) **Section 252.204-7008, Compliance with Safeguarding Covered Defense Information**



## Provision/Clause Prescription

All solicitations  
except COTs

– (c) **Section 252.204-7009, Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information**



Solicitations/contracts  
for services that support  
safeguarding/reporting

(c) **Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**



All solicitations/contracts  
except COTs

**Contracting  
For Cloud  
Services**

– (p) **Section 252.239-7009, Representation of Use of Cloud Computing**



Solicitations/contracts  
for IT services

– (c) **Section 252.239-7010, Cloud Computing Services**







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

- **Overview**
- **Covered Defense Information**
- **Subcontractor Flowdown**
- **Adequate Security**
- **Cloud Environment**
- **Implementation and Compliance**





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

|  | Nov 18, 2013<br><i>(Final Rule)</i>  | Aug 26, 2015 / Dec 30, 2015<br><i>(Interim Rules)</i>   | October 21, 2016<br><i>(Final Rule)</i>   |
|--|--|---|---|
| <b>Scope – What Information</b>                | <ul style="list-style-type: none"> <li>Unclassified Controlled Technical Information</li> </ul>                  | <ul style="list-style-type: none"> <li>Covered Defense Information</li> <li>Operationally Critical Support</li> </ul>   | <ul style="list-style-type: none"> <li>Revised/clarified definition for covered defense information</li> </ul>  |
| <b>Adequate Security - Minimum Protections</b> | <ul style="list-style-type: none"> <li>Selected controls in NIST SP 800-53</li> </ul>                            | <ul style="list-style-type: none"> <li>Aug 2015</li> <li>NIST SP 800-171 (June 2015)</li> </ul>   | <ul style="list-style-type: none"> <li>NIST SP 800-171 (currently Revision 1, published Dec 2016)</li> </ul>  |
| <b>Deadline for Adequate Security</b>          | <ul style="list-style-type: none"> <li>Contract Award</li> </ul>   | <ul style="list-style-type: none"> <li>Dec 2015 – As soon as practical, but NLT 31 Dec 17</li> </ul>  | <ul style="list-style-type: none"> <li>As soon as practical, but NLT 31 Dec 2017</li> </ul>   |
| <b>Subcontractor/Flowdown</b>                  | <ul style="list-style-type: none"> <li>Include the substance of the clause in <u>all</u> subcontracts</li> </ul> | <ul style="list-style-type: none"> <li>Include in subcontracts for operationally critical support, or when involving covered contractor information system</li> </ul> | <ul style="list-style-type: none"> <li>Contractor to determine if information required for subcontractor performance retains identity as CDI</li> </ul> |

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





# Prescription for DFARS Clause 252.204-7012

## DFARS 204.7304 Solicitation provision and contract clauses.

(a) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, **in all solicitations, ... except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.**

(b) Use the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Information, **in all solicitations and contracts, ... for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.**

(c) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, **in all solicitations and contracts, ... except for solicitations and contracts solely for the acquisition of COTS items.**





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

See FAQ 1

- COTS is a commercial item that has been sold in the commercial marketplace in substantial quantities, and is offered to the government in a contract or subcontract without modification
  - Procurements solely for the acquisition of COTS items are extremely unlikely to involve covered defense information or operationally critical support
- Commercial items include COTS, but also other commercial items that are or about to be available in the marketplace, but which also can be modified to meet Government requirements.
  - If a commercial item must be modified to meet Government requirements, such modification may require the use and safeguarding of covered defense information, or the resulting service could be operationally critical for DoD





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

**DFARS Clause 252.204-7012 requires contractors/subcontractors to:**

- 1. Provide adequate security to safeguard covered defense information that resides on or is transiting through a 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

See FAQs 19 - 30

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

- **Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry,<sup>1</sup> 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<sup>2</sup>**

<sup>1</sup> Referenced only to point to information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, government-wide policies

<sup>2</sup> “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





# 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.**





# Subcontractor Flowdown – International Suppliers

- Because the DFARS is generally written for U.S. contractors, there may be conflicts between DFARS Clause 252.205-7012 and foreign national law, regulation, or bilateral country agreements.
- OUSD(A&S) and DoD CIO will work with the Defense Technology Security Administration (DTSA), under OUSD(Policy) to:
  - Resolve conflicts as they are identified
  - Issue deviations on a country-by-country basis as may be required to implement the rule within national law, regulation, and country agreements

**DoD Contracting Offices should work with DPAP to resolve concerns with international suppliers**







# 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 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.**





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

## Why NIST SP 800-171?

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

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





# NIST SP 800-53 and NIST SP 800-171

See FAQ 33

## NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4, April 2013)

- Catalog of security and privacy controls for federal information systems and organizations to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors

## NIST SP 800-171, Protecting CUI in Nonfederal Systems and Organizations (Revision 1, December 2016)

- Recommended requirements for protecting the confidentiality of CUI when:
  - CUI is resident in nonfederal information systems/ organizations
  - Information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies



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

| NIST SP 800-171 Requirement  | NIST SP 800-53 Requirement (from November 2013 DFARS, table 1)  |
|--|---|
| <p><b>3.1.1</b> Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</p> <p><b>3.1.2</b> Limit information system access to the types of transactions and functions authorized users are permitted to execute.</p> | <p><b>AC-2 ACCOUNT MANAGEMENT</b> <u>The organization:</u></p> <ul style="list-style-type: none"><li>a. Identifies/selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];</li><li>b. Assigns account managers for information system accounts;</li><li>c. Establishes conditions for group and role membership;</li><li>d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;</li><li>e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;</li><li>f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];</li><li>g. Monitors the use of, information system accounts;</li><li>h. Notifies account managers:<ul style="list-style-type: none"><li>1. When accounts are no longer required;</li><li>2. When users are terminated or transferred; and</li><li>3. When individual information system usage or need-to-know changes;</li></ul></li><li>i. Authorizes access to the information system based on:<ul style="list-style-type: none"><li>1. A valid access authorization;</li><li>2. Intended system usage; and</li><li>3. Other attributes as required by the organization or associated missions/business functions;</li></ul></li><li>j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and</li><li>k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</li></ul> <p><b>AC-3 ACCESS ENFORCEMENT</b> <u>The information system</u> enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.</p> <p><b>AC-17 REMOTE ACCESS</b> <u>The organization:</u></p> <ul style="list-style-type: none"><li>a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and</li><li>b. Authorizes remote access to the information system prior to allowing such connections.</li></ul> |

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

| NIST SP 800-171 Requirement   | NIST SP 800-53 Requirement (from November 2013 DFARS, table 1)  |
|---|---|
| <p><b>3.8.9</b> Protect the confidentiality of backup CUI at storage locations.</p> | <p><b>CP-9 INFORMATION SYSTEM BACKUP</b> <u>The organization:</u></p> <ul style="list-style-type: none"><li>a. Conducts backups of user-level information contained in the information system [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>];</li><li>b. Conducts backups of system-level information contained in the information system [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>];</li><li>c. Conducts backups of information system documentation including security-related documentation [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>]; and</li><li>d. <b>Protects the confidentiality</b>, integrity, and availability <b>of backup</b> information <b>at storage locations</b>.</li></ul> |
| <p><b>3.5.5</b> Prevent reuse of identifiers for a defined period.</p>              | <p><b>IA-4 IDENTIFIER MANAGEMENT</b> <u>The organization manages information system identifiers by:</u></p> <ul style="list-style-type: none"><li>a. Receiving authorization from [<i>Assignment: organization-defined personnel or roles</i>] to assign an individual, group, role, or device identifier;</li><li>b. Selecting an identifier that identifies an individual, group, role, or device;</li><li>c. Assigning the identifier to the intended individual, group, role, or device;</li><li>d. <b>Preventing reuse of identifiers for</b> [<i>Assignment: organization-defined time period</i>]; and</li><li>e. <b>Disabling the identifier after</b> [<i>Assignment: organization-defined time period of inactivity</i>].</li></ul>   |
| <p><b>3.5.6</b> Disable identifiers after a defined period of inactivity.</p>       |   |



# 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     |
|-----------------------------|--------|-------|-------|-------|----------|----------------|--------------|----------------------|---------------------------------------|--------|--------|----------|---------|--------|
| <b>Basic<br/>(FIPS 200)</b> | 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) |         |        |
| <b>Derived<br/>(800-53)</b> | 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 |                      |                                       |        |        |          |         | 23     |



# NIST SP 800-171 Security Requirement

## 3.5.3 – Multifactor Authentication

See FAQs 69, 74 - 79

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







# NIST SP 800-171 Security Requirement

## 3.5.3 – Multifactor Authentication

See FAQs 69, 74 - 79

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





# NIST SP 800-171 Security Requirement

## 3.13.11 – FIPS Validated Encryption

See FAQ 68

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





# NIST SP 800-171 Security Requirement

## 3.13.11 – FIPS Validated Encryption

See FAQ 68

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





# 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





# DFARS 252.204-7012 Requirements for Cloud Computing

- Per DFARS 252.204-7012 (b)(2)(ii)(D), the contractor shall require and ensure that the cloud service provider (CSP) meets:
  - Security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) “moderate” baseline and
  - Complies with requirements in paragraphs (c) through (g) for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment
- In most cases, the contractor will not actually ‘flow down’ the DFARS clause to the CSP, but must ensure, when using a CSP as part of its covered contractor information system, that the contractor can continue to meet the DFARS clause requirements, including the requirements in DFARS 252.204-7012 (c)-(g)
- If the CSP is considered a subcontractor for the contract effort and will be handling covered defense information, then DFARS clause 252.204-7012 would flow down, but this would not be typical





# DFARS Clause 252.204-7012 – “Security requirements equivalent to FedRAMP Moderate baseline”

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





# 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

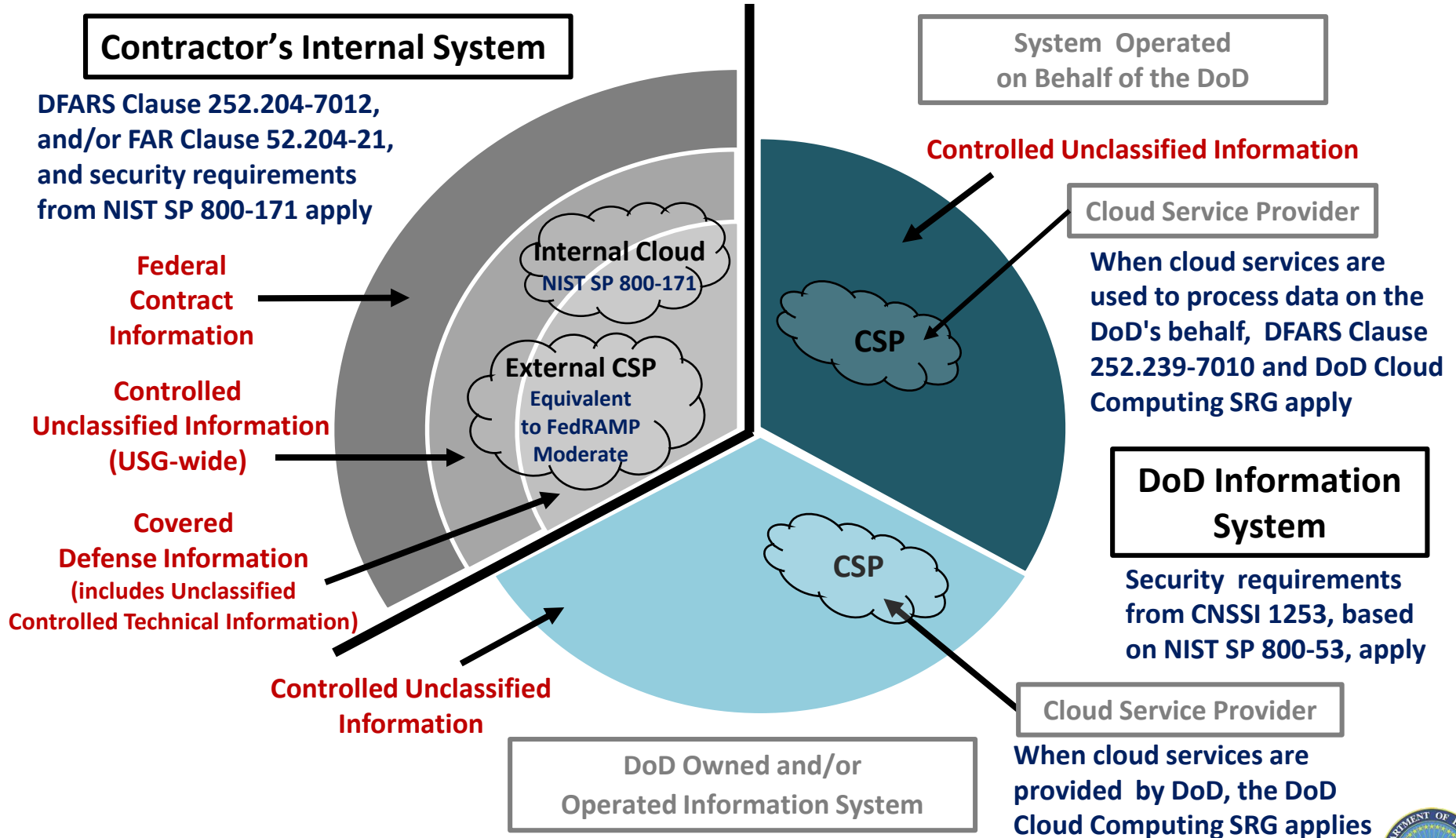
- Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud
- Requires the cloud service provider to:
  - Comply with the DoD Cloud Computing Security Requirements Guide
  - Comply with requirements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





# Protecting the DoD's Unclassified Information

See FAQ 32







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

## Implementation

- **Identification and Marking of Covered Defense Information**
- **Cyber Incident Reporting and Damage Assessment**





# Identification and Marking of Covered Defense Information

## Government/Requiring Activity is required to:

- Use DoDM 5200.01 Vol 4, DoD Information Security Program: CUI and DoDI 5230.24 DoDI 5230.24, Distribution Statements on Technical Documents to **identify and mark covered defense information**
- Use Section C, e.g., Statement of Work, of the contract to require development and delivery of covered defense information from the contractor
- **Direct appropriate marking and dissemination for covered defense information in the contract (e.g., Block 9 of Contract Data Requirements List (CDRL) DD Form 1423). Additional markings (e.g., Export Control) can be placed in Block 16.**
- Verify that covered defense information is appropriately marked when provided to the contractor as Government Furnished Information

## The contractor is responsible for:

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





# DoDI 5230.24 – Distribution Statements on Technical Documents

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

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

### Example of Marking for Distribution Statement E

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

### Example of Marking for Export Control Warning (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.





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

## Statement of Work (Section C)

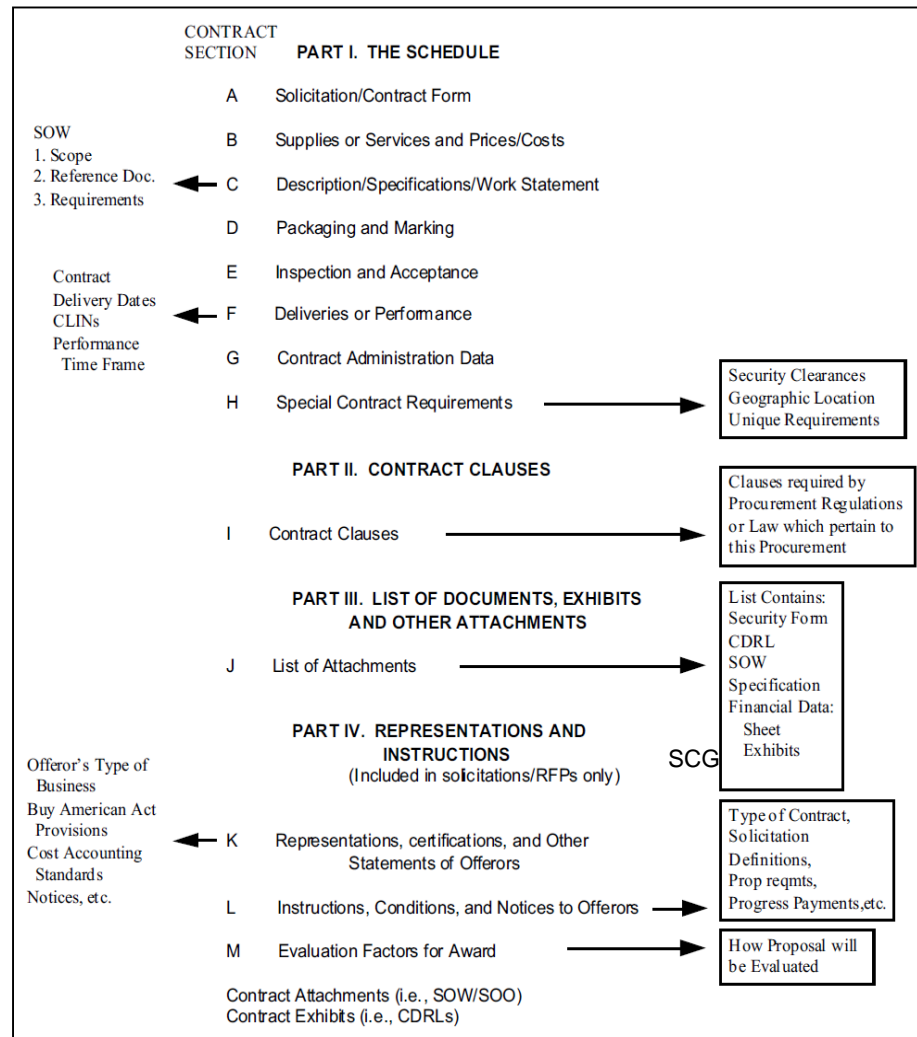
- Prepared by Requiring Activity when DoD requires development and delivery of covered defense information

## Contract Clauses (Section I), includes

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

## List of Attachments (Section J)

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

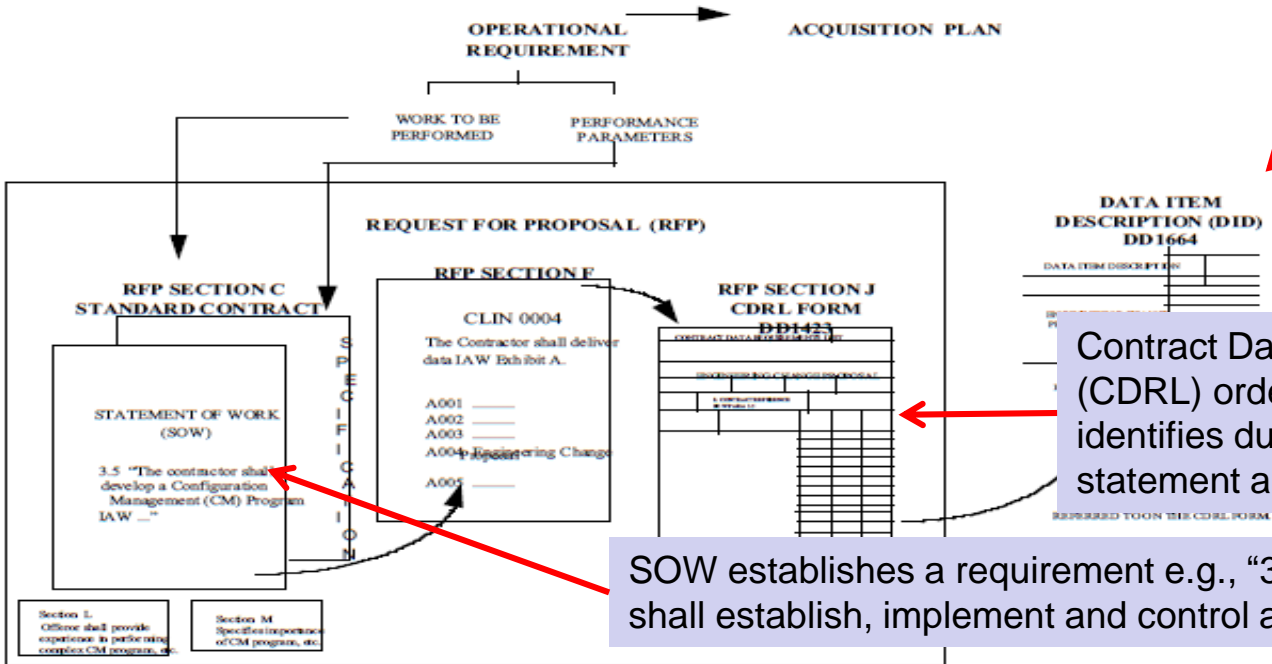




# Identification and Marking of Covered Defense Information Preparation of Statement of Work (SOW)

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

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



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


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

Example of Specification – SOW – CDRL - DID Relationship





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



**Department of Defense  
INSTRUCTION**

NUMBER 5230.24  
August 23, 2012  
*Incorporating Change 1, Effective April 28, 2016*  
USD(AT&L)

SUBJECT: Distribution Statements on Technical Documents  
References: See Enclosure 1

1. **PURPOSE** This Instruction:

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

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

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

2. **APPLICABILITY** This Instruction:

a. Applies to:

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

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

**DoDI 5230.24**

| CONTRACT DATA REQUIREMENTS LIST<br>(1 Data Item)   |  | Form Approved<br>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 Project Director (0704-0188), Washington, DC 20503.  |  |  |   |
| CONTRACT DATA REQUIREMENTS LIST<br>(1 Data Item)   |  | Form Approved<br>OMB No. 0704-0188                                     |   |
| Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please DO NOT RETURN your form to the above address. Send completed form to the Government Printing Contracting Officer for the Contract PR No. listed in Block E. |  |  |   |
| CONTRACT DATA REQUIREMENTS LIST<br>(1 Data Item)   |  | Form Approved<br>OMB No. 0704-0188                                     |   |
| Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please DO NOT RETURN your form to the above address. Send completed form to the Government Printing Contracting Officer for the Contract PR No. listed in Block E. |  |  |   |
| A. CONTRACT LINE ITEM NO.  |  | B. EXHIBIT<br>A  | C. CATEGORY:<br>TDP ___ TM ___ OTHER IPSC |
| D. SYSTEM/ITEM<br>Distributed Common Ground System - Army  |  | E. CONTRACT/PR NO.<br>TBD  | F. CONTRACTOR<br>TBD                      |
| 1. DATA ITEM NO.<br>A002   | 2. TITLE OF DATA ITEM<br>Software Transition Plan (STRP) |  | 3. SUBTITLE                               |
| 4. AUTHORITY (Data Acquisition Document No.)<br>DI-IPSC-81429A   |  | 5. CONTRACT REFERENCE<br>PWS Para 4.3.15                               |   |
| 7. DD 250 REQ<br>LT  |  | 12. DATE OF FIRST SUBMISSION<br>SEE BLOCK 16                           |   |
| 8. APP CODE<br>D   |  | 13. DATE OF SUBSEQUENT SUBMISSION<br>SEE BLOCK 16                      |   |
| 16. REMARKS<br>BLOCK 16 The Government requires thirty (30) working days for review and completion. Final copy shall be submitted NLT thirty (30) working days after   |  | 14. DISTRIBUTION<br>SF AE-I EW-DC                                      |   |
|  |  | a. ADDRESSEE<br>SF AE-I EW-DC<br>*ELECTRONIC SUBMITTAL<br>SEE BLOCK 16 |   |
|  |  | b. COPIES<br>Draft Final<br>Reg Repr<br>2                              |   |

**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**





# Cyber Incident Reporting

## What is a cyber incident?

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

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

### DFARS 204.7302 (d)

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





# Cyber Incident Reporting

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

- **Review contractor network(s) for evidence of compromise of covered defense information using contractor's available tools, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts**
- **Identify covered defense information that may have been affected in the cyber incident**
- **If contract contains requirement for operationally critical support, determine if the incident affects the contractor's ability to provide operationally critical support**
- **Rapidly report (within 72 hours of the discovery of an incident) directly to DoD**
  - **Subcontractors provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable**

*DFARS Clause 252.204-7012(c)(1)*







# Cyber Incident Reporting

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

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

**Upon receipt of a cyber incident report —**

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





# Cyber Incident Reporting

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

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

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





# DIB CS Web Portal

[DIB CS Participant Login](#)

## Welcome to the DIBNet portal

DoD's gateway for defense contractor cyber incident reporting and voluntary participation in DoD's Cybersecurity Program

### Report a Cyber Incident

[Report](#)

A DoD-approved Medium Assurance Certificate is required to access the reporting module. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).

Do you know what to report? [See below](#).

#### Need assistance?

Contact DoD Cyber Crime Center (DC3)

- [DCISE@dc3.mil](mailto:DCISE@dc3.mil)
- Hotline: (410) 981-0104
- Toll Free: (877) 838-2174

### DoD's DIB Cybersecurity (CS) Program

The DIB CS Program is a voluntary cyber threat information sharing program established by DoD to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems.

To apply to the DIB CS Program, a DoD-approved Medium Assurance Certificate is required. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).

[Apply Now!](#)

#### Need assistance?

Contact the DIB CS Program Office

- [OSD.DIBCSIA@mail.mil](mailto:OSD.DIBCSIA@mail.mil)
- (703) 604-3167
- Toll Free: (855) DoD-IACS
- Fax: (571) 372-5434

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

<https://www.DIBNet.dod.mil>





# Malicious Software (Malware) Submission

**When a contractor discovers and isolates malicious software, the contractor will submit malware to DoD as follows (in accordance with instructions provided by the Contracting officer or DC3) —**

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





# 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**





# Cyber Incident Damage Assessment Activities

## Conducting the cyber incident damage assessment

- **When 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**
- **Media is submitted to the DoD Cyber Crime Center, who will confirm receipt in writing to the contractor and requesting Contracting Officer**
- **Component DAMO may assemble a team of experts, including Program Office representatives, to evaluate data files from the contractor and determine the impact to the acquisition program and the warfighting capability it supports**





# Cyber Incident Damage Assessment Activities

## Completing the cyber incident damage assessment —

- When Requiring Activity determines that the damage assessment activities are complete, the Requiring Activity will provide the Contracting Officer with a report documenting the findings affecting covered defense information
- The Contracting Officer shall include the report documenting the findings in the contract file(s) and provide a copy to the contractor

## Further cyber incident damage assessment related activities—

- The mission of the Joint Acquisition Protection and Exploitation Cell (JAPEC) is to integrate protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten U.S. military advantage
- JAPEC is another source of technology protection assessment available to the Program Office





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

## Compliance

- **Demonstrating Implementation of the Security Requirements in NIST SP 800-171**
- **Compliance with DFARS Clause 252.204-7012**
- **Considering a Contractor's Internal Information System in Source Selection**







# 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**





# Contractor Compliance — Implementation of 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 scope of the requirements**





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

- **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**
- **Per 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**





# Facilitating the Consistent Review of System Security Plans and Contractor Systems

## DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

- This draft document was developed to:
  - Facilitate the consistent review of system security plans and plans of action, specifically:
    - The impact that NIST SP 800-171 security requirements “not yet implemented” have on an information system, and the risk that system poses to DoD
  - Assist in prioritizing the implementation of security requirements
  - Address the method(s) to implement the security requirements
  - When applicable, provide clarifying information for security requirements that are frequently misunderstood





# How Can a Contractor's System Security Plan and/or Internal System Impact a Procurement Action?

## Assessing the State of a Contractor's Internal Information System in a Procurement Action

- This draft document was developed to:
  - Illustrate when/where 'DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented' might be used in a procurement/source selection
  - Illustrate how the DoD may choose to assess/consider submitted System Security Plans and Plans of Action
  - Illustrate when/where 'NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information' may be used to develop system assessment plans and conduct assessments of systems where the security requirements in NIST SP 800-171 have been implemented (*in Final Public Draft with expected July publication*)





# How Can a Contractor’s System Security Plan and/or Internal System Impact a Procurement Action?

## Assessing the State of a Contractor’s Internal Information System (continued)

- This document does not introduce new requirements into the procurement/ source selection process but addresses, for a variety of acquisition scenarios:
  - Review of the system security plan
  - Assessment of the contractor’s internal information system
- For each acquisition scenario, the document illustrates actions to be addressed in the solicitation/RFP, during source selection, and in the contract, as shown in the matrix extract below:

|    | OBJECTIVE  | SOLICITATION/RFP  | SOURCE SELECTION   | CONTRACT  |
|----|--|---|--|---|
| 1. | Evaluate implementation of NIST SP 800-171 at source selection                       | <ul style="list-style-type: none"> <li>• DFARS Provision 252.204-7008</li> <li>• DFARS Clause 252.204-7012</li> </ul>   |  | <ul style="list-style-type: none"> <li>• DFARS Clause 252.204-7012</li> </ul>   |
|    | Alternative 1A.: Go/No Go decision based on implementation status of NIST SP 800-171 | <ul style="list-style-type: none"> <li>• RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) with the contractor’s technical proposal ...</li> </ul> | <ul style="list-style-type: none"> <li>• Evaluate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action, in accordance with ...</li> </ul> | <ul style="list-style-type: none"> <li>• Incorporate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action as part of contract ...</li> </ul> |





# How Can a Contractor's System Security Plan and/or Internal System Impact a Procurement Action?

|   | ACQUISITION SCENARIO  | SOLICITATION/RFP | SOURCE SELECTION | CONTRACT |
|---|---|------------------|------------------|----------|
| <p>Pre Award</p> <p style="text-align: center;">↓</p> <p>Post Award</p> | <ol style="list-style-type: none"> <li>1. Evaluate implementation of NIST SP 800-171 at source selection               <ul style="list-style-type: none"> <li>– Alternative 1A: Go/No Go decision based on implementation status of NIST SP 800-171</li> <li>– Alternative 1B: Assess NIST SP 800-171 implementation as a separate technical evaluation factor</li> </ul> </li> <li>2. In addition to the security requirements in NIST SP 800-171, also evaluate any added protections that may be required</li> <li>3. Assess/track implementation of NIST SP 800-171 security requirements after contract award               <ul style="list-style-type: none"> <li>– The government may also monitor compliance of NIST SP 800-171 with continuous monitoring or an independent government review</li> </ul> </li> <li>4. Contractors 'self-attest' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171</li> </ol> |                  |                  |          |





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

## **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**







## Additional Regulations, Policy and Guidance

- **32 CFR Part 236, “DoD Defense Industrial Base Cybersecurity Activities”**
- **32 CFR 2002, “Controlled Unclassified Information”**
- **FAR Case 2017-016, “Controlled Unclassified Information,”**
- **NIST Cybersecurity Framework**
- **FedRAMP and the DoD Cloud Computing Security Requirements Guide**
- **DoDI 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems,”**
- **DoDM 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information”**
- **DoDI 5000.02, Enclosure 14, “Cybersecurity in the Defense Acquisition System”**





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

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

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





# 32 CFR 2002, Controlled Unclassified Information

## 32 CFR Part 2002, “Controlled Unclassified Information,” *Final rule effective November 14, 2016*

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





# FAR Case 2017-016

## Controlled Unclassified Information

### FAR Case 2017-016, “Controlled Unclassified Information”

- **Open case to implement the National Archives and Records Administration (NARA) Controlled Unclassified information (CUI) program of E.O. 13556**
- **Will apply to all Federal Agencies**
- **Publication as a proposed rule expected in 2018/2019**





# NIST Cybersecurity Framework

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

## NIST "Framework for Improving Critical Infrastructure Cybersecurity" (Version 1.0 published Feb 12, 2014, Draft Version 1.1, published Jan 10, 2017)

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

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

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





# FedRAMP and the DoD Cloud Computing Security Requirements Guide

## Federal Risk and Authorization Management Program (FedRAMP)

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

## DoD Cloud Computing Security Requirements Guide

*Version 1 Release 3 | 6 March 2017*

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





# DoDI 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems”

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

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

### Revision currently in final coordination

- Cites current DFARS and FAR safeguarding clauses to be used in contracts
- Requires NIST SP 800-171 for DoD CUI





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

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

\* Per USD(I) Memo, dated April 11, 2017, “Guidance on Implementation of Controlled Unclassified Information”







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

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

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





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

## Program Responsibilities:

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





# 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*
- **DPAP Website** (<http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>) for DFARS, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- **NIST SP 800-171, Revision 1** (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf>)
- **Cloud Computing Security Requirements Guide (SRG)** (<http://iasecontent.disa.mil/cloud/SRG/>)
- **DoD's Defense Industrial Base Cybersecurity program (DIB CS Program)** (<https://dibnet.dod.mil>)

**Questions? Submit via email at [osd.dibcsia@mail.mil](mailto:osd.dibcsia@mail.mil)**

