Cybersecurity Challenges

Protecting DoD's Unclassified Information

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

April 2018

What DoD Is Doing

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

- Securing DoD's information systems and networks

- Codifying cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy

- Contractual requirements implemented through the Defense Federal Acquisition Regulation Supplement (DFARS)

- DoD's DIB Cybersecurity Program for voluntary cyber threat information sharing

- Leveraging security standards such as those identified in National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" *(Revision 1 published Dec 2016)*

Protecting the DoD's Unclassified Information
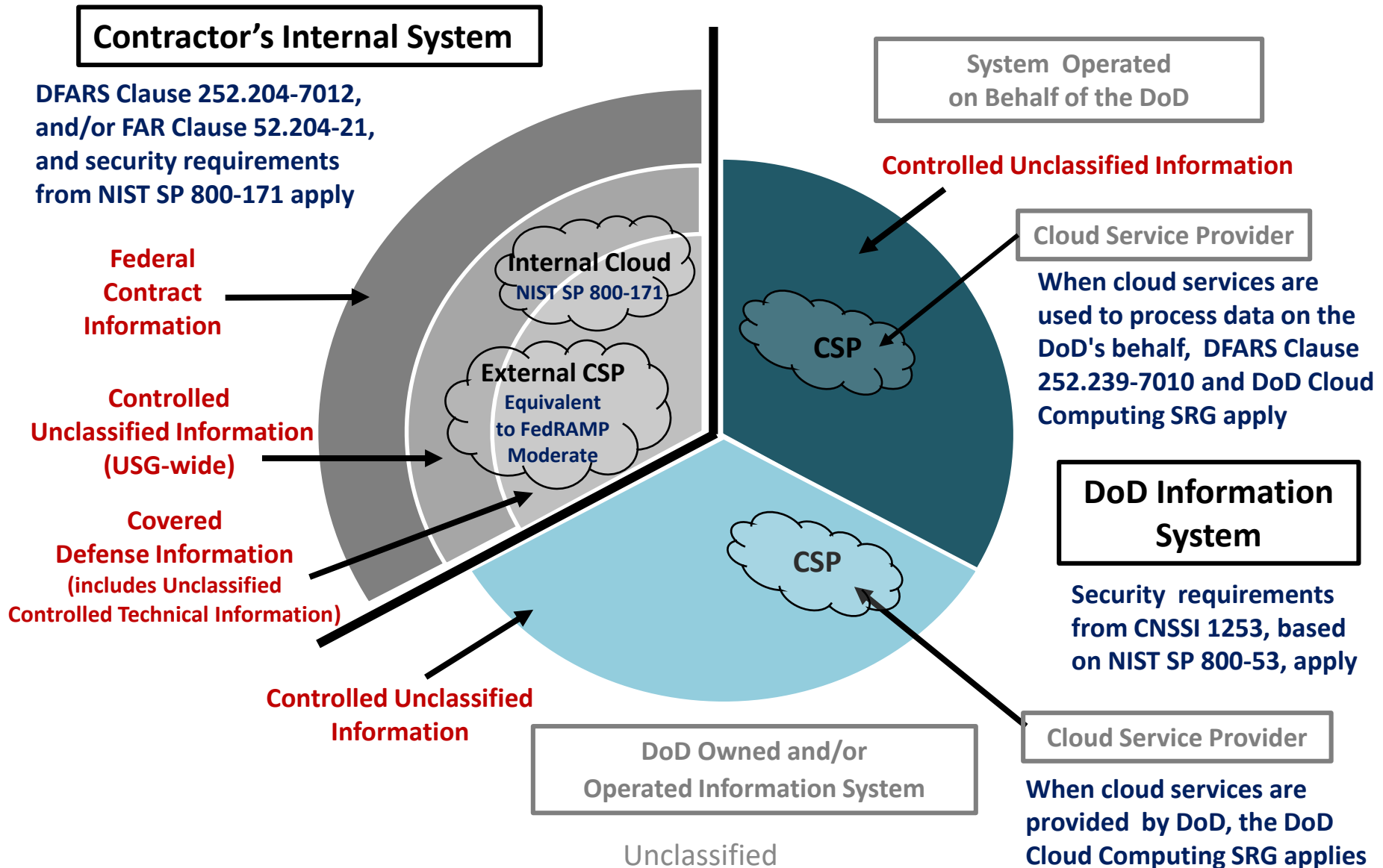
DFARS Clause 252.204-7012 requires contractors/subcontractors to:

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 – 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

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.

To provide adequate security to safeguard covered defense information:

DFARS 252.204-7012 (b) Adequate Security. … the contractor shall implement, at a minimum, the following information security protections:

***

(b)(2)(ii)(A): The contractor shall implement NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations, as soon as practical, but not later than December 31, 2017

***

(b)(3): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required

Cloud Computing

Cloud Computing Services
48 CFR Parts 239 and 252, DFARS Clause 252.239-7010

- Applies when a cloud solution is being used to process data <u>on the DoD's behalf</u> or DoD is contracting with Cloud Service Provider to host/process data in a cloud

- Requires the cloud service provider to:
  - Comply with the **DoD Cloud Computing Security Requirements Guide**
  - Comply with requirements for **cyber incident reporting and damage assessment**

Safeguarding Covered Defense Information and Cyber Incident Reporting
48 CFR Parts 202, 204, 212, and 252, DFARS Clause 252.204-7012

- Applies when a contractor uses an external cloud service provider to store, process, or transmit Covered Defense Information <u>on the contractor's behalf</u>
- 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**

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**

Implementing NIST SP 800-171 Security Requirements

- **If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, a written explanation of -**

  - Why security requirement is <u>not applicable;</u> or

  - How an <u>alternative but equally effective</u> security measure is used to achieve equivalent protection

  (see 252.204-7008(c)(2)(i) and 252.204-7012(b)(2)(ii)(B))

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

  (see 252.204-7012(b)(2)(ii)(A))

Implementing NIST SP 800-171 – Where to Get Assistance

- **NIST MEP Handbook Cybersecurity Handbook (HB-162) (20 Nov 2017)**
  - The Handbook provides a step-by-step guide to assessing a small manufacturer's information systems against the security requirements in NIST SP 800-171 rev 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

- **Draft NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information,** *(in Final Public Draft with expected May publication)*
  - This document is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

- **Cybersecurity Evaluation Tool (CSET)**
  - No-cost application, developed by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control system and information technology network security practices

- **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**

- **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 is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)**
  - **DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements**
  - **Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD**

- **If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract**

DoD Assessment of a Contractor's Internal Information System in a Procurement Action

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
Pre Award	1. **Evaluate implementation of NIST SP 800-171 at source selection** – **Alternative 1A: Go/No Go decision based on implementation status of NIST SP 800-171** – **Alternative 1B: Assess NIST SP 800-171 implementation as a separate technical evaluation factor** 2. **Require protections in addition to the security requirements in NIST SP 800-171 and evaluate at source selection**			
Post Award	3. **Assess/track implementation of NIST SP 800-171 security requirements after contract award** – **The government may also monitor compliance of NIST SP 800-171** 4. **Contractors 'self-attest' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171**			

- **DoD Guidance for Reviewing System Security Plans – Developed to:**
  - **Facilitate the consistent review of System Security Plans and Plans of Action, and the impact that NIST SP 800-171 Security Requirements "not yet implemented" have on an information system**
  - **Assist in prioritizing the implementation of security requirements not yet implemented**
  - **Address the method(s) to implement the security requirements**
  - **When applicable, provides clarifying information for security requirements that are frequently misunderstood.**

- **NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information** *(in Final Public Draft with expected May publication)*

Cyber Incident Reporting

> **DFARS 204.7302 (d)**
>
> A cyber incident that is reported by a contractor or subcontractor <u>shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security</u> 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

- Contractors/subcontractors must submit a cyber incident report via https://dibnet.dod.mil/

- Upon receipt of a cyber incident report —
    - DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s)
    - The contracting officer(s) provides the report to the requiring activity(ies)
    - DC3 analyzes report to identify cyber threat vectors and adversary trends
    - DC3 contacts the reporting company if the report is incomplete

Cyber Incident Damage Assessment Activities

DoD decision to conduct a cyber incident damage assessment —

- The DoD Component damage assessment office (DAMO) and Requiring Activity will determine if a cyber incident damage assessment is warranted

- Once the decision to conduct an assessment is made - the Requiring Activity will notify the contractor via the Contracting Officer, and the Contracting Officer will request media from the contractor

Purpose of the cyber incident damage assessment —

- Determine impact of compromised information on U.S. military capability underpinned by the technology

- Consider how the compromised information may enable an adversary to counter, defeat, or reverse engineer U.S. capabilities

- Focus on the compromised intellectual property impacted by the cyber incident – not on the compromise mechanism

DIB CS Web Portal

Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the **ECA website**.

https://www.DIBNet.dod.mil

Resources

- **Cybersecurity in DoD Acquisition Regulations** page at *https://dodprocurementtoolbox.com/* for Related Regulations, Policy, Frequently Asked Questions, and Resources

- DPAP Website *https://www.acq.osd.mil/dpap/dars/dfarspgi/* for DFARs, Procedures, Guidance and Information (PGI), and Frequently Asked Questions

- Cybersecurity Evaluation Tool (CSET) - Download at *https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET* or request physical copy of software at *cset@dhs.gov* — Select "Advanced Mode" to display option to select NIST 800-171

- NIST Manufacturing Extension Partnership at *https://www.nist.gov/mep*

- The Procurement Technical Assistance Program (PTAP) at *http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx*

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

Questions?