Cyber Security Challenges

Protecting DoD's Unclassified Information

Vicki Michetti, DoD CIO, Director, DIB Cybersecurity Program

Mary Thomas, OUSD(AT&L), Defense Procurement and Acquisition Policy

Outline

- Cybersecurity Landscape
- Protecting the DoD's Unclassified Information
- DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services
  - Safeguarding Covered Defense Information (CDI)
  - Cloud Computing/Contracting for Cloud Services
- Resources
- Questions

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

Cyber attacks cost companies $400 billion every year

Inga Beale, CEO, Lloyds

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

89% of breaches had a financial or espionage motive

64% of confirmed data breaches involved weak, default or stolen passwords

2016 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

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…

Information System Security Requirements

Contractor's Internal System

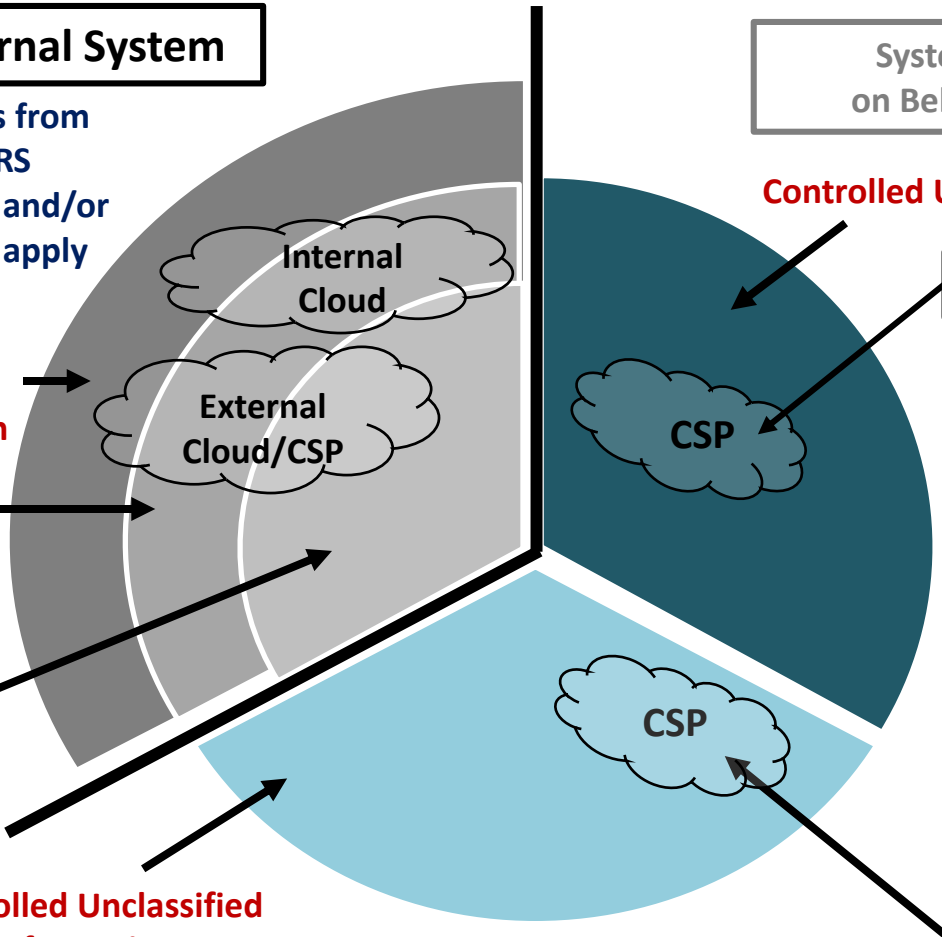
Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information



System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

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

DoD Information System

Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

DoD Owned and/or Operated Information System

Network Penetration Reporting and Contracting for Cloud Services

DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services – final rule published on October 21, 2016

Includes 3 clauses and 2 provisions:

Safeguarding Covered Defense Information

- **(p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information** → All solicitations/contracts 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 and contracts for IT services
- **(c) Section 252.239-7010, Cloud Computing Services** → Solicitations and contracts for IT services

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

	Nov 18, 2013 *(Final Rule)*	Aug 26, 2015 / Dec 30, 2015 *(Interim Rules)*	October 21, 2016 *(Final Rule)*
Scope – What Information?	• **Unclassified Controlled Technical Information**	• **Covered Defense Information** • **Operationally Critical Support**	• Covered Defense Information **(revised definition)** • Oper Critical Support
Adequate Security – What Minimum Protections?	• Selected controls in **NIST SP 800-53**, Security and Privacy Controls for **Federal Information Systems** and Organizations	• **Aug 2015 – NIST SP 800-171,** Protecting Controlled Unclassified Information on Nonfederal Information Systems & Organizations	• NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems & Organizations
When Req'd to Meet Minimum Protections?	• **Contract Award**	• **Dec 2015 – As soon as practical, but NLT Dec 31, 2017**	• As soon as practical, but NLT Dec 31, 2017
Subcontractor/ Flowdown	• **Include the substance of the clause in all subcontracts**	• **Include in subcontracts for operationally critical support, or when involving covered information system**	• **Contractor to determine if information required for subcontractor performance retains its identity as CDI**

What is Covered Defense Information?

- **Unclassified controlled technical information (CTI) or other information as described in the CUI Registry that requires safeguarding or dissemination controls*, AND is either**

- **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**

- **Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.**

* Pursuant to and consistent with law, regulations, and Governmentwide policies

Network Security Requirements to Safeguard Covered Defense Information

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting *(effective October 21, 2016)*

(b) *Adequate security.* The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government…

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than Dec 31, 2017.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified … may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

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

- **Developed for use on contractor and other nonfederal information systems to protect CUI (Revision 1 published December 2016)**
  - **Replaces use of selected security controls from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**
- **Enables contractors to comply using systems and practices likely already in place**
  - **Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.**
- **Provides standardized/uniform set of requirements for all 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**

An Approach to Implementing NIST SP 800-171

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**

   Note that the complexity of the company IT system may determine whether additional software or tools are required.
2. **Determine which of requirements can readily be accomplished by in-house IT personnel and which require additional research**
3. **Develop a plan of action and milestones to implement the requirements.**

Implementing NIST SP 800-171

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI
Basic (FIPS 200)	3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
	3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
								3.8.3			3.11.3	3.12.3		3.14.3
												(3.12.4)		
Derived (800-53)	3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.4		3.10.3			3.13.3	3.14.4
	3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.5		3.10.4			3.13.4	3.14.5
	3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.6		3.10.5			3.13.5	3.14.6
	3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.7		3.10.6			3.13.6	3.14.7
	3.1.7		3.3.7	3.4.7	3.5.7			3.8.8					3.13.7	
	3.1.8		3.3.8	3.4.8	3.5.8			3.8.9					3.13.8	
	3.1.9		3.3.9	3.4.9	3.5.9								3.13.9	
	3.1.10				3.5.10								3.13.10	
	3.1.11				3.5.11								3.13.11	
	3.1.12												3.13.12	
	3.1.13												3.13.13	
	3.1.14												3.13.14	
	3.1.15				Policy/Process			Policy or Software Requirement					3.13.15	
	3.1.16												3.13.16	
	3.1.17				Configuration			Configuration or Software						
	3.1.18													
	3.1.19				Software			Configuration or Software or Hardware						
	3.1.20													
	3.1.21				Hardware			Software or Hardware						
	3.1.22													

Frequently Asked Questions — "Compliance" with DFARS Clause 252.204-7012

Q: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A: The DFARS rule did not add any unique/additional requirement for the Government to monitor contractor implementation of required security requirements.

Q: Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?

A: The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. Nor will DoD recognize 3rd party assessments or certifications. By signing the contract, the contractor agrees to comply with the terms of the contract.

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Security Requirement 3.12.4 – System Security Plan (SSP)

3.12.4 — Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems.

- **The System Security Plan (SSP) should be used to document:**
  - **How the requirements are met or how organizations plan to meet requirements**
    - **3.12.2 addresses plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities**
  - **Situations where requirements cannot practically be applied (non-applicable)**
  - **DoD CIO approved alternative but equally effective security measures**
  - **Exceptions to accommodate special circumstances (e.g., CNC machines and/or shop floor machines)**
  - **Individual, isolated or temporary deficiencies addressed by assessing risk and applying mitigations**

- **When requested by the requiring activity, the SSP (or elements of the SSP) and any associated plans of action, should be submitted to the requiring activity/contracting officer to demonstrate implementation of NIST SP 800-171.**

Network Security Requirements to Safeguard Covered Defense Information

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

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

- **If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, a written explanation of -**
  - **Why security requirement is not applicable; or**
  - **How an alternative but equally effective security measure is used to achieve equivalent protection**

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

Cyber Incident Reporting and Malware Submission

DFARS 252.204-7012 (c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise …

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil

DFARS 252.204-7012 (d) Malicious Software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

Cyber Incident Damage Assessment Activities

DFARS 252.204-7012 (g) ***Cyber incident damage assessment activities.*** **If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e)* of this clause.**

(e) Media preservation and protection

Purpose of damage assessment:

- **To understand impact of compromised information on U.S. military capability underpinned by technology**
- **Initiated after review of reported cyber incident**
- **Focused on determining impact of compromised intellectual property, not on mechanism of cyber intrusion**
- **An assessment is not possible without access to compromised material**

Cloud Computing

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

- **Applies when** a contractor intends to use an external cloud service provider to store, process, or transmit Covered Defense Information in the performance of a contract
- **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 cyber incident damage assessment.

DFARS Clause 252.239-7010 – Cloud Computing Services

- **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
- **Ensures that the cloud service provider:**
  - Meets requirements of the DoD Cloud Computing Security Requirements Guide
  - Complies with requirements for cyber incident reporting and damage assessment

DoD's Defense Industrial Base (DIB) Cybersecurity Program

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**
  - **Protects confidentiality of shared information**

Mission: Enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

DIB CS Program Eligibility

A contractor must be a Cleared Defense Contractor (CDC) and shall:

(1) Have an existing active Facility Clearance (FCL) granted under NISPOM (DoD 5220.22-M);

(2) Execute the standardized Framework Agreement (FA) with the Government,

(3) To receive classified cyber threat information electronically:

- **(i) Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4 (DoD 5220.22-M), which provides procedures and requirements for COMSEC activities; and**
- **(ii) Have or acquire approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding; and**
- **(iii) Obtain access to DoD's secure voice and data transmission systems supporting the voluntary DoD-DIB CS information sharing program.**

DIB CS Web Portal

Report a Cyber Incident

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

Report a Cyber Incident

Apply to DIB CS Program

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

Apply to Program

Login to DIB CS Information Sharing Portal

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

DIB CS Program Participant Login

DIBNet.dod.mil

Resources

- **DPAP Website (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) for DFARS, Procedures, Guidance and Information (PGI)**
- **Frequently Asked Questions (FAQs) (http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf)**
- **NIST SP 800-171 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.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)**
- **Defense Security Information Exchange (DSIE) (https://www.DSIE.org)**
- **United States Computer Emergency Readiness Team (US-CERT) (https://www.us-cert.gov)**
- **Questions? Submit questions via email at osd.dibcsia@mail.mil**

Questions?

Back-up

Changes in Final Text, DFARS Case 2013-D018

- **Applicability to Fundamental Research:** DFARS Clause 252.204-7000, Disclosure of Information, clarifies that fundamental research, by definition, must not involve CDI
- **Applicability to COTS Items**: Provision/clause are not prescribed for use in solicitations or contracts solely for the acquisition of commercially available off-the-shelf (COTS) items.
- **Definition of Covered Defense Information**: Revised for clarity
- **Subcontractor Flowdown**: Contractor shall determine if information required for subcontractor performance retains identity as CDI, and if necessary, may consult with CO.
- **Contracting for Cloud Services:**
  - When using cloud computing to provide IT services operated on behalf of the Government, DFARS Clause 252.239-7010 allows for award to cloud service providers that have not been granted a DoD provisional authorization (PA)
  - When contractor uses internal cloud or external CSP to store/process/transmit CDI, DFARS Clause 252.204-7012 requires contractor to ensure cloud/CSP meets FedRAMP Moderate baseline and requirements in clause for reporting, etc.