Cyber Security Challenges

Navigating Unclassified Information System Security Protections

Vicki Michetti, DoD CIO, Director, DIB Cybersecurity Program

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

Outline

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

Cybersecurity Landscape

- **The threats facing the government unclassified information have dramatically increased**
  - **Cybersecurity incidents have surged 38% since 2014. (The Global State of Information Security® Survey 2016)**
- **Recent high-profile cyber incidents underscore the need to safeguard both government and industry information and information systems.**
- **Estimated Costs of Cyber Crime are Multiplying***
  - **2015: $400 - 500 billion a year (Lloyds)**
  - **2019: predicted to be $2.1 Trillion (Juniper)**

*** May be significantly higher as some crimes are not reported**

DoD and the Defense Industrial Base

- **The Defense Industrial Base (DIB) develops and maintains sensitive technology and intellectual property vital to protecting and defending our nation.**
  - **As a consequence, malicious cyber actors regularly target the DIB and look for ways to access company networks and obtain valuable information that may compromise our national security and warfighting capabilities.**
  - **The DoD supply chain is vulnerable to the risk of counterfeit parts, which have the potential to delay missions and ultimately endanger service members.**

What DoD is Doing

- **DoD is participating in a range of activities that include both regulatory and voluntary programs to improve the collective cybersecurity of the nation and protect U.S. interests**
  - **Contractual requirements implemented through the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS)**
  - **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"**
  - **Encouraging use of the Voluntary Cybersecurity Framework published by NIST**

Protecting the DoD's Unclassified Information

Types of Unclassified Information Systems

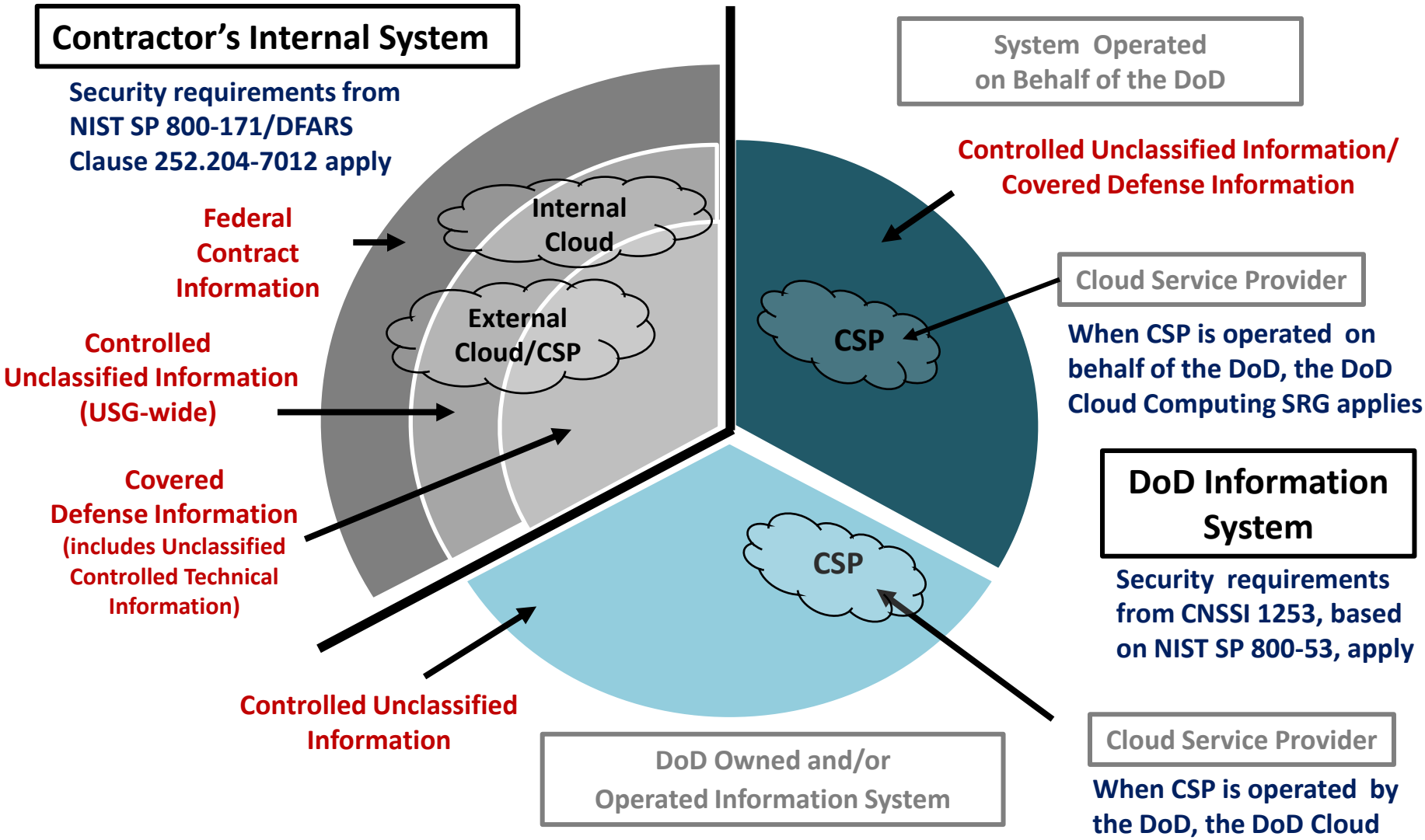
- **Contractor's Internal Information System**
- **DoD Information System**
  - **DoD Owned and/or Operated Information System**
  - **System Operated on Behalf of the DoD**

Types of Unclassified Information

- **Covered Defense Information (to include Unclassified Controlled Technical Info)**
  - ***August 26, 2015 and December 30, 2015, DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services (interim rule)***
- **Controlled Unclassified Information (CUI)**
  - ***November 4, 2010, Executive Order 13556, Controlled Unclassified Information, and September 14, 2016, 32 CFR 2002, Final CUI Federal Regulation***
- **Federal Contract Information**
  - ***May 16, 2016, FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems***

Protecting the DoD's Unclassified Information…

Information System Security Requirements



Network Penetration Reporting and Contracting for Cloud Services

DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services – 2nd interim rule effective on December 30, 2015
(publication of final rule pending)

Includes 3 clauses and 2 provisions:

Safeguarding Covered Defense Information

- **(p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information** → All solicitations/contracts
- **(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

Contracting For Cloud Services

- **(p) Section 252.239-7009, Representation of Use of Cloud Computing**
- **(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 *(Interim Rule)*	Dec 30, 2015*(Interim Rule)*
Scope – What Information?	• **Unclassified Controlled Technical Information**	• **Covered Defense Information** • **Operationally Critical Support**	• Covered Defense Information • Operationally Critical Support
Adequate Security – What Minimum Protections?	• Selected controls in **NIST SP 800-53**, Security and Privacy Controls for **Federal Information Systems** and Organizations	• **NIST SP 800-171,** Protecting Controlled Unclassified Information on **Nonfederal Information Systems** and Organizations	• NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations
When?	• Contract Award	• Contract Award • **Oct 8, 2015 Deviation** – Security Requirement 3.5.3, **within 9 months of Award**	• As soon as practical, but **NLT Dec 31, 2017**
Flowdown	• Include the substance of the clause in all subcontracts	• Requires subcontractors to rapidly report cyber incidents directly to DoD	• Include in subcontracts for operationally critical support, or when involving covered information system

What is Covered Defense Information?

Three conditions apply:	
1	Unclassified information that is provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or
	Unclassified information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract;
2	Falls in any of the categories listed, to include: – Controlled technical information – Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies
3	Is identified in the contract, task order, or delivery order

Network Security Requirements to Safeguard Covered Defense Information

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting *(effective December 30, 2015)*

(b) To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(ii) For covered contractor information systems …

(A) The security requirements in NIST SP 800-171 as soon as practical, but not later than Dec 31, 2017…

(B) Alternative but equally effective security measures …

DFARS Clause 252.204-7012 (b)(2): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Network Security Requirements to Safeguard Covered Defense Information

- 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

---

- The Contractor shall notify DoD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award

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 (published June 2015)**
  - **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 Meeting 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.**

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 or 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 give any credence to 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.

Cyber Incident Reporting

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 …

DFARS 252.204-7012 (d) Malicious Software. The Contractor or subcontractors that discover/isolate malicious software… shall submit the malicious software in accordance with instructions provided by 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**

Contracting for Cloud Services

DFARS SUBPART 239.76 and DFARS Clause 252.239-7010

- Provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements
- Ensures uniform application of DoD's policies concerning Cloud Computing Services, to include DoD Cloud Computing Security Requirements Guide (SRG)
- The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract.

What *Is* Covered?	What is *Not* Covered?
• A cloud solution is being used to process data on the DoD's behalf	• A contractor uses his own internal cloud solution or uses an external CSP to do his processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for his internal contractor system. – Example: Contractor is developing the next generation tanker, and uses his internal cloud for the engineering design.
• DoD is contracting with Cloud Service Provider to host/process data in a cloud	
• Cloud solution is being used for processing what we (the DoD) would normally do ourselves but have decided to outsource	

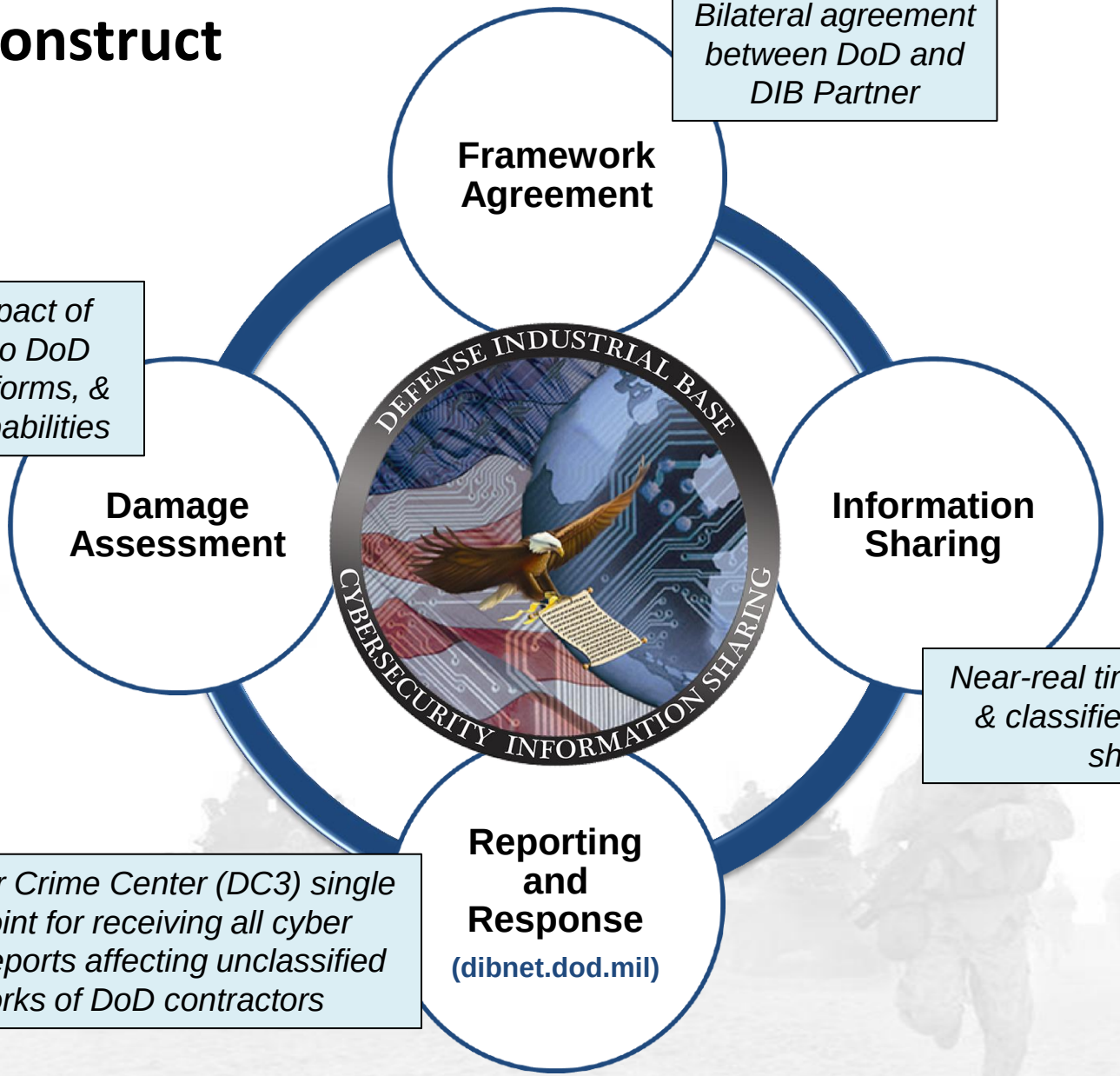
DoD's Defense Industrial Base Cybersecurity (DIB CS) Program

A Public-Private Cybersecurity Partnership

- 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 Construct



Bilateral agreement between DoD and DIB Partner

Determine impact of compromise to DoD programs, platforms, & warfighting capabilities

Near-real time unclassified & classified information sharing

DoD Cyber Crime Center (DC3) single focal point for receiving all cyber incident reports affecting unclassified networks of DoD contractors

DIB Cybersecurity 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/DARS/DFARS and PGI**
  (http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html)
  - **DFARS Subpart 204.73 and PGI 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting**
  - **SUBPART 239.76 and PGI 239.76 – Cloud Computing**
  - **252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.**
  - **252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information**
  - **252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting**
  - **252.239-7009 Representation of Use of Cloud Computing**
  - **252.239-7010 Cloud Computing Services**
  - **Frequently Asked Questions**
- **NIST SP 800-171 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf)**
- **Cloud Computing Security Requirements Guide (SRG)**
  (http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf)

Resources Available to Industry

- **United States Computer Emergency Readiness Team (US-CERT)**
  http://www.us-cert.gov
- **FBI InfraGard**
  https://www.infragard.org
- **DHS Cybersecurity Information Sharing and Collaboration Program (CISCP)**
  https://www.dhs.gov/ciscp
- **DHS Enhanced Cybersecurity Services (ECS)**
  https://www.dhs.gov/enhanced-cybersecurity-services
- **DoD's Defense Industrial Base Cybersecurity program (DIB CS program)**
  http://dibnet.dod.mil
- **Defense Security Information Exchange (DSIE)**
  www.DSIE.org

Summary

- **Understand the cyber threat targeting your company's networks and information systems**
- **If eligible, participate in DoD's DIB CS program to enhance and supplement your company's cybersecurity and to better comprehend the cyber threat**
- **Ensure your company is implementing cybersecurity best practices and standards**

Questions?

Backup

FAR Clause 52.204-21

FAR Clause 52.204-21, Basic Safeguarding of Contractor Information Systems *(Final Rule, effective June 2016)*

- **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 109 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.

Information System Security Protections Required by DFARS Clause 252.204-7012 and FAR Clause 52.204-21

NIST SP 800-171 Security Requirements (required by DFARS Clause 252.204-7012)

	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
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	None	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												3.13.15	
	3.1.16												3.13.16	
	3.1.17													
	3.1.18													
	3.1.19													
	3.1.20													
	3.1.21													
	3.1.22													

FAR Clause 52.204-21 maps to these NIST SP 800-171 requirements

32 CFR Part 2002 – Controlled Unclassified Information *(effective November 14, 2016)*

The Big Picture: A three-part plan for the protection of CUI

- **32 CFR Part 2002 establishes required controls/markings for CUI government-wide.**
- **NIST SP 800-171 defines security requirements for protecting CUI in nonfederal information systems and organizations.**
- **Federal Acquisition Regulation (FAR) clause to apply the requirements of the federal CUI rule and SP 800-171 to nonfederal organizations (planned for 2017).**

What is Controlled Unclassified Information?

Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. — Executive Order 13556

- **CUI Basic - All CUI that does not have specific protections set out in a law, regulation, or Government-wide policy falls into CUI Basic categories.**
- **CUI Specified - Recognizes the types of CUI that have required or permitted controls included in their governing authorities.**