Cyber Security Challenges

Protecting DoD's Unclassified Information

Melinda Reed, OUSD(AT&L), Systems Engineering

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

80 million people had their personal information stolen in a cyberattack against large U.S. health insurance company

Decoding the Adversary, AT&T

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**
- **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"**

Protecting the DoD's Unclassified Information

Types of Unclassified Information Systems

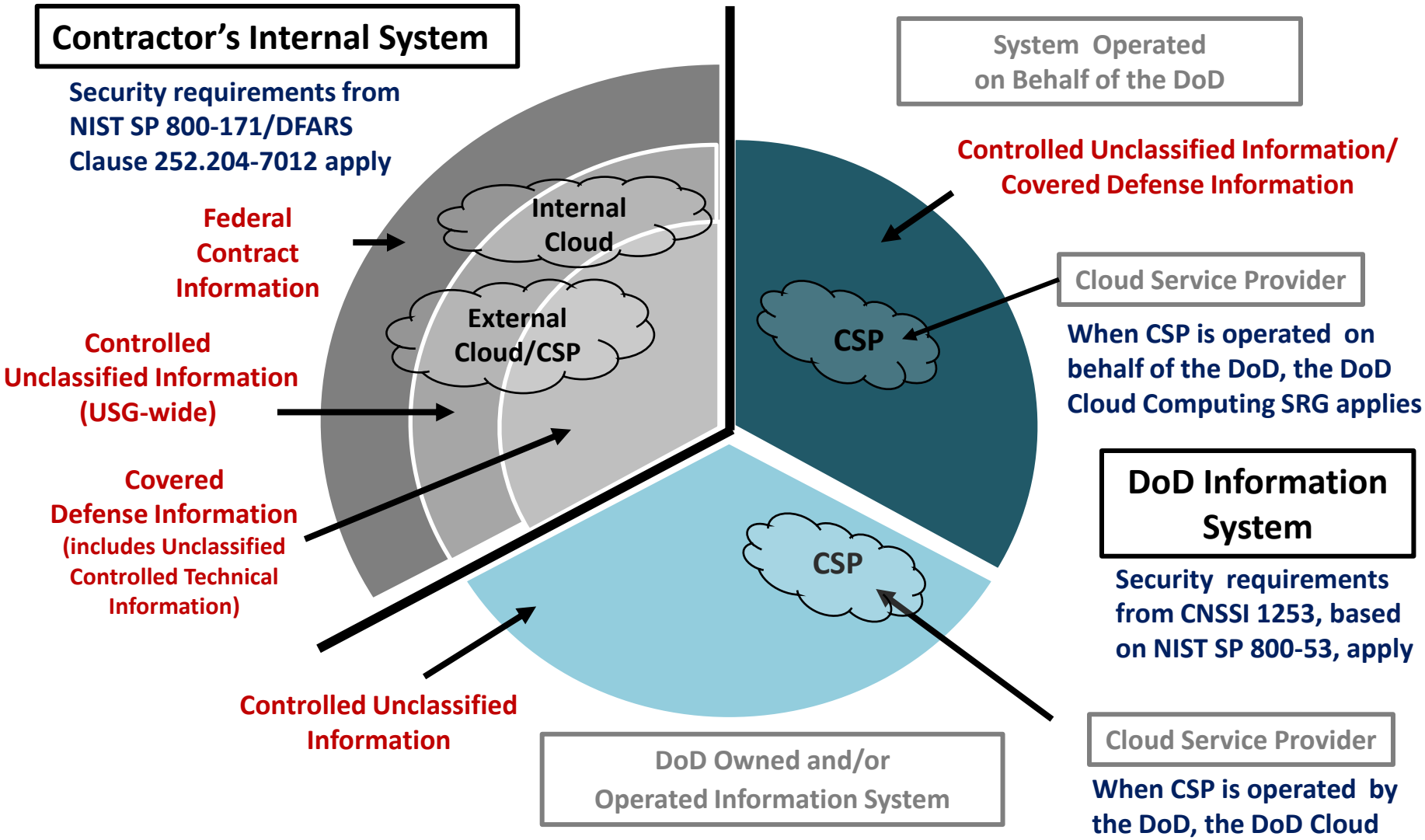
- **Contractor's Internal Information System**
- **DoD Information System**
  - **DoD Owned and/or Operated Information System**
  - **System Operated on Behalf of the DoD**

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 – 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
- **(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** → 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?	• **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**

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.

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

- 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.

FAQs on "Marked or Otherwise Identified" CDI

Q: What is the marking regime for CUI?

A: USD(I), DoD's Executive Agent for CUI, is responsible for implementing 32 CFR Part 2002 – Controlled Unclassified Information (which establishes required controls/markings for CUI government-wide) across DoD, and for revising DoDM 5200.01 Vol 4, DoD Information Security Program – CUI.

CDI is a subset of CUI, but the requirement in DFARS Clause 252.204-7012 to "mark or otherwise identify" speaks only to the identification of information for which adequate security must be provided under the contract.

Q: Who is responsible for identifying/marking CDI?

A: The requiring activity is responsible to notify the contracting officer (CO) when a contract will require CDI. The CO shall ensure CDI is marked or otherwise identified in the contract, task order, or delivery order, and ensure that the contract, task order, or delivery order includes the requirement for the contractor to mark CDI developed in the performance of the contract.

FAQs on "Marked or Otherwise Identified" CDI

Q: Is information identified as FOUO considered to be CDI?

A: Information that is identified as For Official Use Only (FOUO) alone does not indicate that it is CDI. Information identified as FOUO should only be treated as CDI when the information falls within the definition of CDI.

Q: Should export controlled information be treated as CDI?

A: Export control, a category in the CUI Registry, is considered CDI only when it meets the CDI definition. When DoD contractors hold information that is export controlled, but it is not "provided to the 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," the information is not CDI

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 (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.**

Figure 1

	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													

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

- 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.

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

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.

Public Draft NIST SP 800-171, *Revision 1* *(Aug 2016)*

- **Includes guidance on the use of system security plans (SSPs) and plans of action and milestones (POAMs) to:**
  - **Demonstrate the implementation or planned implementation of CUI requirements by nonfederal organizations**
  - **Serve as critical inputs to a federal agency's risk management decisions and decisions on whether or not to pursue agreements or contracts.**

"When requested, the SSP/associated POAMs… should be submitted… to demonstrate implementation or planned implementation of the CUI requirements. … Some specialized systems (e.g., industrial/process control systems, medical devices, or NC machines), may have restrictions/limitations on application of certain CUI requirements. The SSP should be used to describe… exceptions to the requirements to accommodate such issues."

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.

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 at http://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.

Operationally Critical Support

As defined in DFARS Clause 252.204-7012:

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

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
- Ensures uniform application of the DoD Cloud Computing Security Requirements Guide
- New under final rule – The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization (PA) when, (i) The requirement for a PA is waived by the DoD CIO; or (ii) The cloud computing service requirement is for a private, on-premises version that will be provided from U.S. Government facilities. Under this circumstance, the cloud service provider must obtain a PA prior to operational use.

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. – This is now covered by DFARS Clause 252.204-7012 (b)(2)(D).
• 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	

Contractor Use of External Cloud Service Provider for Covered Defense Information

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, *final rule, effective October 21, 2016*

(b)(2)(ii)(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause 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.

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

- **DoD's Defense Industrial Base Cybersecurity program (DIB CS program)**
  http://dibnet.dod.mil
- **Defense Security Information Exchange (DSIE)**
  www.DSIE.org
- **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

Questions?