Protecting DoD's Unclassified Information in Contractor Systems

Implementing DFARS Case 2013-D018 – Network Penetration Reporting and Contracting for Cloud Services

Outline

DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, *effective December 30, 2015*

Protecting DoD's Unclassified Information in Contractor Systems

- **Defining the Landscape**
- **What is Covered Defense Information?**
- **Safeguarding Covered Defense Information**
- **Cyber Incident Reporting**
- **Contracting for Cloud Services**
- **Resources**

Protecting DoD's Unclassified Information…

Defining the Landscape

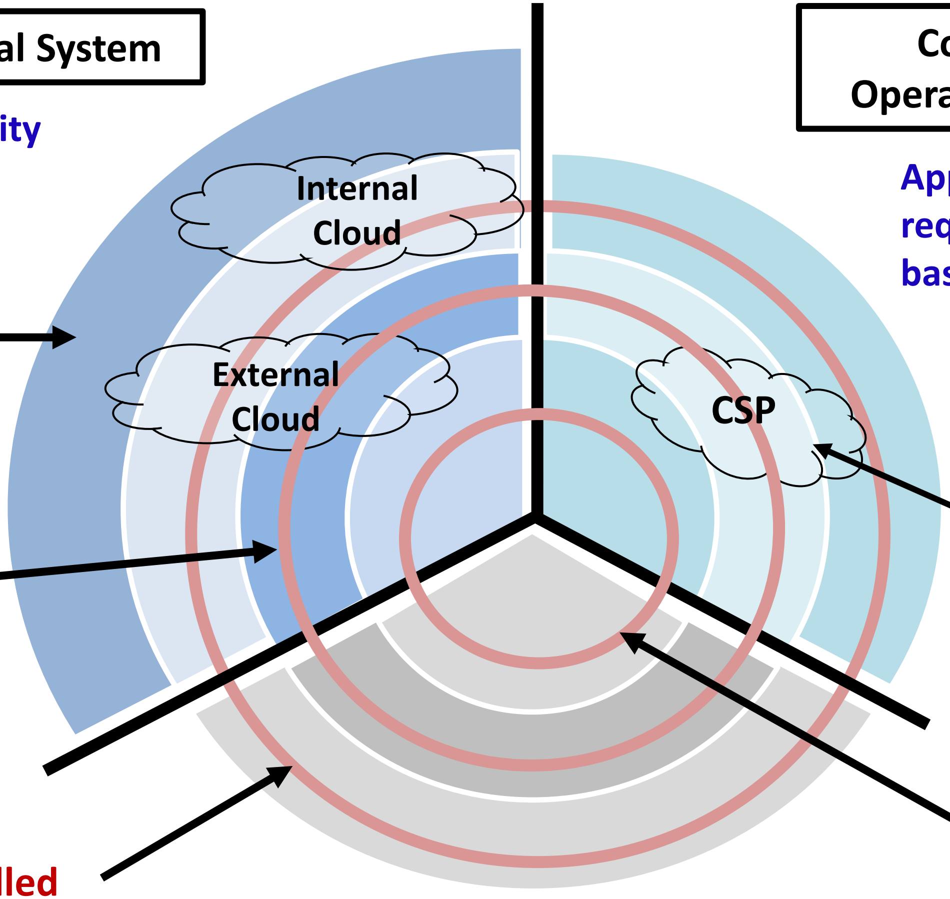
Types of Unclassified Information Systems

- Contractor's Internal Information Systems
- Contractor System Operated on the Government's Behalf
- DoD Information System

Types of Unclassified Information

- Unclassified Controlled Technical Information
  - *November 18, 2013 DFARS Case 2011-D039, Safeguarding Unclassified Controlled Technical Information*
- Covered Defense Information
  - *August 26, 2015 and December 30, 2015, DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services*
- Controlled Unclassified Information (CUI)
  - *November 4, 2010, Executive Order 13556, Controlled Unclassified Information, and May 8, 2015, 32 CFR 2002, Proposed CUI Federal Regulation*
- Federal Contract Information
  - *May 16, 2016, FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems*

Protecting DoD’s Unclassified Information…
Information System Security Requirements



Contractor’s Internal System

Applicable security requirements:
NIST SP 800-171

Contractor System Operated on DoD’s Behalf

Applicable security requirements: from CNSSI 1253, based on NIST SP 800-53

Federal Contract Information

Covered Defense Information

Cloud Service Provider

Applicable security requirements:
From the SRG

Controlled Unclassified Information (USG-wide)

Unclassified Controlled Technical Information

DoD Information System

Applicable security requirements:
From CNSSI 1253, based on NIST SP 800-53

Protecting the Contractor’s Internal Information System

Safeguarding Covered Defense Information

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting: Requires contractors and subcontractors to:

- Provide **adequate security** to safeguard **covered defense information** that resides on or transits **covered contractor information systems**
- Rapidly report all **cyber incidents** to DoD
- When using cloud computing to provide information technology services in the performance of the contract:
  - Implement and maintain safeguards and controls in accordance with the **DoD Cloud Computing Security Requirements Guide (SRG)**
  - Report all **cyber incidents** that are related to the cloud computing service provided under this contract to DoD

What is Covered Defense Information?

Covered Contractor Information System –

An unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits **covered defense information**

Covered Defense Information – Unclassified information that

1	Is provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or
	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 following categories: – Controlled technical information – Critical information (operations security) – Export control – 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

Safeguarding Covered Defense Information

To provide **adequate security,** the Contractor shall, at a minimum—

- As soon as practical, but not later than Dec 31, 2017 — Implement the security requirements in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- Notify DoD CIO within 30 days of contract award of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award

The Contractor need not implement any security requirement deemed to be non-applicable by an authorized representative of the DoD CIO.

The Contractor may substitute an alternative security measure deemed to be equally effective by an authorized representative of the DoD CIO.

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

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

- 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 in original DFARS Clause 252.204-7012 *(November 18, 2013)*
- Enables contractors to comply using systems and practices likely already in place
  - Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI when existing systems comply
  - Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.
- Provides <u>standardized/uniform set</u> 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

Reporting a Cyber Incident

Cyber Incident — Actions 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

- 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—
  - Conduct a review for evidence of compromise
  - Rapidly report cyber incidents to DoD at http://dibnet.dod.mil
- Subcontractors subject to the clause are required to report cyber incidents directly to DoD, and to provide the incident report number to their prime Contractor

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

DFARS Clause 252.204-7012 and FAR Clause 52.204-21

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting *(2nd Interim Rule, effective December 30, 2015)*

- **Requires the contractor/subcontractor to safeguard covered defense information on the Contractor's internal information system**
  - **Required Information Security Protections: NIST SP 800-171 (109 requirements)**
- **Requires the contractor/subcontractor to rapidly report cyber incidents**

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

- **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)**
- **No reporting**

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**

Protecting a Contractor System Operated on DoD's Behalf

Contracting for Cloud Services

DFARS Clause 252.239-7010, Cloud Computing Services: Requires contractors and subcontractors to, when using cloud computing to provide information technology services in the performance of a contract:

- Implement policy developed within DoD CIO and the DoD Cloud Computing Security Requirements Guide (SRG)
- Report all cyber incidents that to DoD via http://dibnet.dod.mil.

Cloud Computing — A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.
- Also includes commercial offerings for software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS)

Resources

- **DPAP Website** **(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**
  - **DFARS 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 (FAQs)**
- **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://www.dibnet.dod.mil

- **Defense Security Information Exchange (DSIE)**
  www.DSIE.org