Introduction to Cybersecurity Issues for Government Contractors

Thursday, February 14, 2019| 12:00 PM Eastern

Sponsored by the ABA Center for Professional Development

Introduction to Cybersecurity Issues for Government Contractors

Jeffery Chiow

Co-Chair, Government Contracts

Rogers Joseph O'Donnell

Kristin Grimes

Corporate Counsel (Cyber + Security) for Leidos

Townsend Bourne

Partner, Government Contracts, Investigations, and International Trade Practice Group

Sheppard Mullin LLP

Agenda

- Cybersecurity Landscape
- Compliance with FAR 52.204-21
- Compliance with DFARS 252.204-7012
- September 2017 DPAP Guidance
- Government Audit Rights
- Potential Risks – Noncompliance and Cyber Incidents
- Key Learning Points

Cybersecurity Landscape

Cybersecurity Legal Landscape

U.S. Federal Law and Regulation

- No overarching U.S. federal law for cybersecurity standards or breach notification
- Sector- or Regulator-specific guidance
  - E.g., Financial Institutions (GLBA) / Healthcare (HIPPA) / Government Contracting (FAR/DFARS/K specific) /Energy (NERC CIP) / Publicly traded (SEC) /Consumer Products (FTC)
- Other federal laws (e.g., CFAA, SCA, Wiretap)

U.S. State Data Security Laws and Regulations

- Data breach notification (individuals and attorneys general)
- Cybersecurity standards ("reasonable security")

Standards and Best Practices (U.S. based)

- NIST, ISO, CIS CSC 20

Ex-U.S. Law and Regulation

- EU, China, etc.

Evolving Threats and Technology

- Threat Actors
  - U.S. Adversaries
    - Nation States
    - Non-State Terrorists
  - Criminals
  - Activists
  - Insider Threats

- Threat Actor Motives
  - Espionage
  - Military Advantage
  - Publicity
  - Political Activism
  - Monetary

- Technology rapidly increasing in sophistication

Key Government Roles

OMB — Sets acquisition policy

NIST — Develops guidance for security controls

GSA — Lead agency for FAR rule

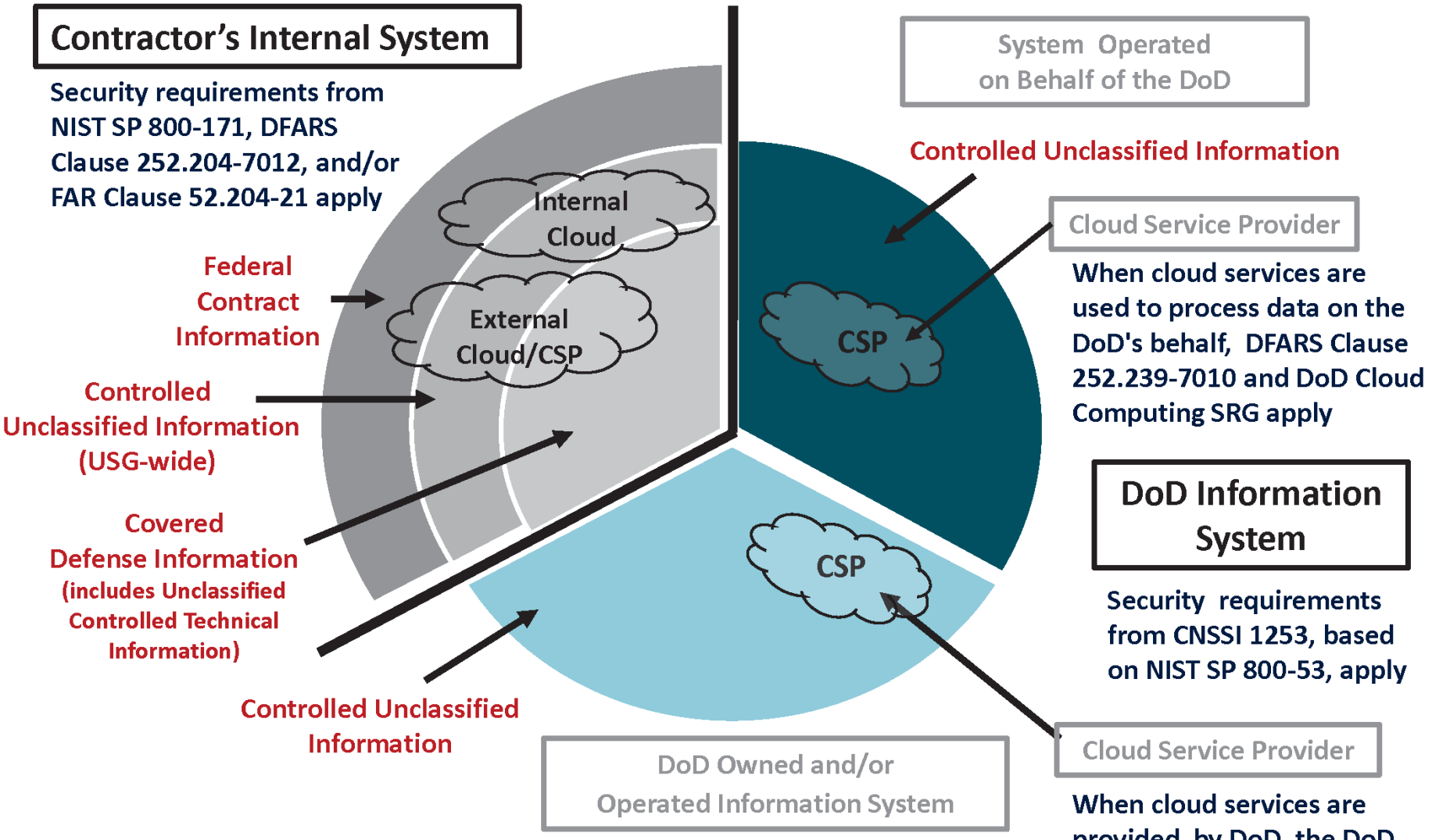
DoD — Defines defense contract requirements

DHS — Key agency for reporting and infrastructure

NARA — Defines CUI

Protecting the DoD's Unclassified Information…

Information System Security Requirements



*From DoD Industry Day June 23, 2017

Compliance with FAR 52.204-21

Compliance with FAR 52.204-21

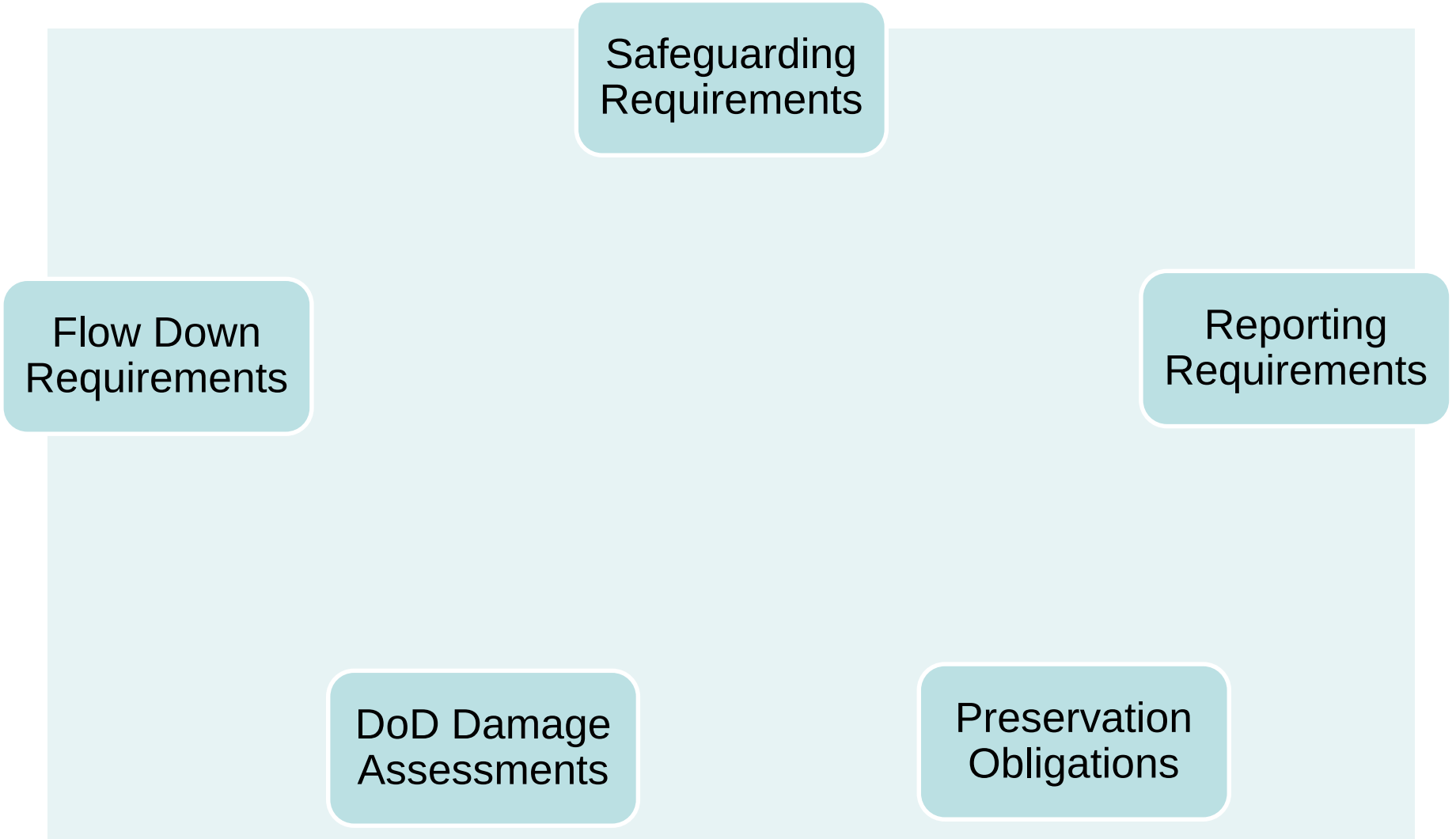
- Applies to contractor information systems that process, store, or transmit "federal contract information" or FCI
  - FCI is nonpublic information "that is *provided by or generated for* the Government under a contract to develop or deliver a product or service to the Government"
- Imposes a baseline of 15 security controls for federal contractors that are *"reflective of actions a prudent business person would employ"*
  - Not explicitly tied to NIST SP 800-171
- Must flow down to all subcontractors that "may have Federal contract information residing in or transiting through its information system"
- Must comply NOW; no grace period for implementation; controls mandatory at the time of award
- No reporting requirement - yet

FAR 52.204-21 Security Requirements

Limit system access to authorized users	Identify users, devices, or processes	Identify, report, and correct information and information system flaws in a timely manner
Limit system access to the types of transactions/functions users are permitted to execute	Authenticate or verify user identifies prior to permitting access to information systems	Monitor and protect organization communications at external and key internal boundaries
Verify/control/limit connections to external systems	Sanitize or destroy information system media	Implement subnetworks for publicly accessible system components that are physically/logically separated from internal networks
Control publicly accessible information	Limit physical access to authorized individuals	Protect from malicious code
Escort visitors and monitor visitor activity; maintain audit logs of access	Update malicious code protection mechanisms	Perform periodic/real-time scans of information system and files

Compliance with DFARS 252.204-7012

Compliance with DFARS 252.204-21

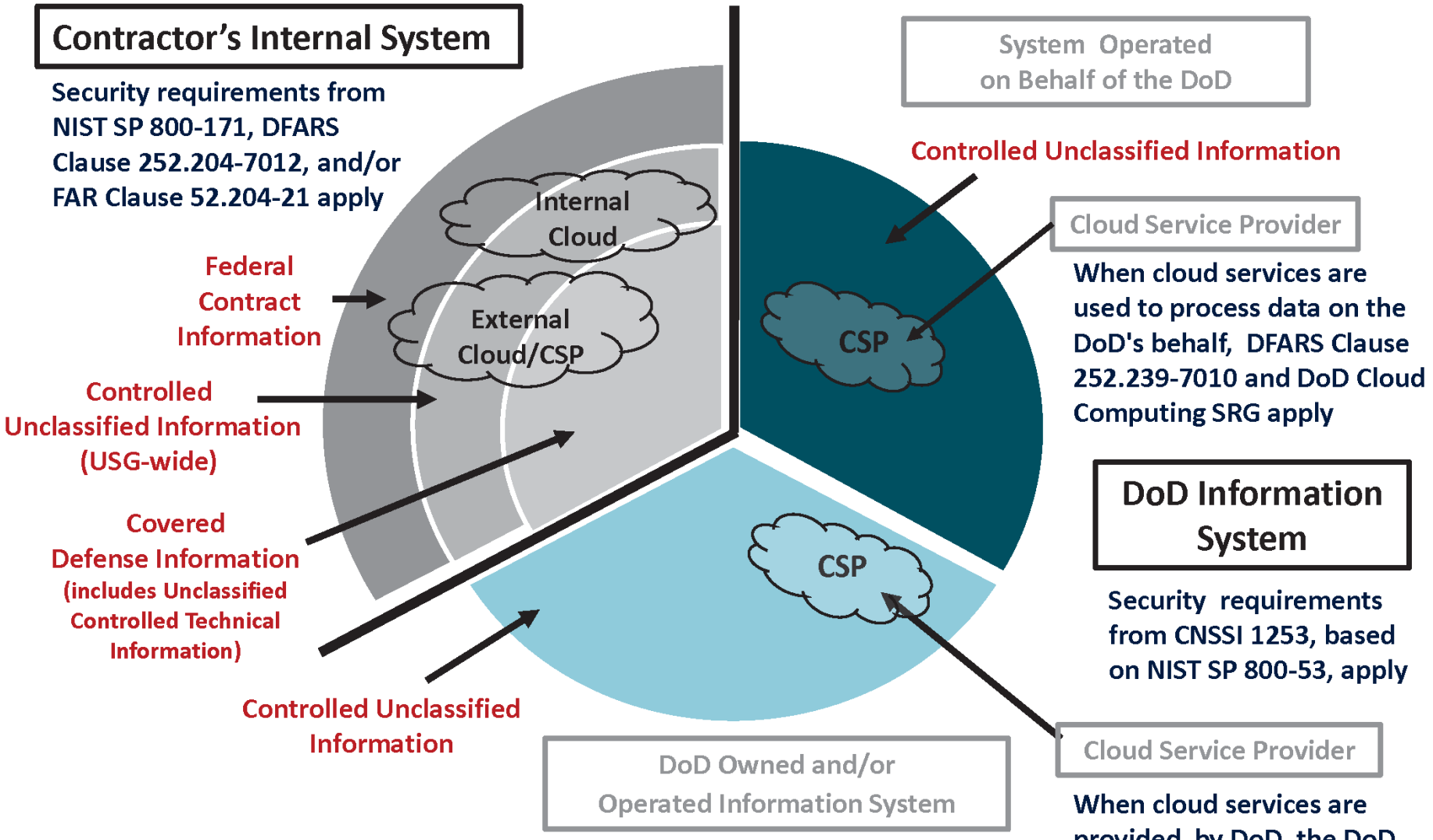


DFARS Clauses re Safeguarding and Network Penetration

- 252.204-7302 (Policy)
  - Contractors and subs are to provide “adequate security” & must “rapidly report” cyber incidents directly to DoD.
- 252.204-**7008**: Compliance clause; all **solicitations** except COTS
- 252.204-7009: Limitation on Use/Disclosure of Contractor Reported Cyber Incident Information
- **252.204-7012: Safeguarding CDI and Cyber Incident Reporting**
- 252.239-7009: Representation of Use of Cloud Computing
- 252.239-7010: Cloud Computing Services

Protecting the DoD's Unclassified Information…

Information System Security Requirements



*From DoD Industry Day June 23, 2017

What is CDI?
Information to be protected

Covered defense information means:

- Unclassified controlled technical information or other information as described in the Controlled Unclassified Information (CUI) Registry … that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
  - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the 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."

What is a Covered Contractor Information System?

- DFARS Clause 252.204-7012 applies to “covered [DoD] contractor information systems”
  - A “covered contractor information system” means:
    - an unclassified information system
    - that is owned, operated by or for, a DoD contractor and
    - that processes, stores or transmits covered defense information.

-7008 Compliance Clause

- Requirements of -7012 must be "implemented for all covered defense information on all covered contractor information systems that support the performance of this contract."
- By submission of offer, contractor commits to implement the requirements of SP 800-171 no later than Dec. 31, 2017.

"If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract."

-7012 Safeguarding Clause

Requires "adequate security" on all covered contractor information systems and requires prompt (72-hour) cyber incident reporting

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

- Implement the security requirements in NIST SP 800–171 NLT Dec. 31, 2017.
- Submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO.
- Apply other security measures when the Contractor reasonably determines that such 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. These measures may be addressed in a system security plan.

NIST SP 800-171 Security Control Families

1. Access Control
2. Awareness and Training
3. Auditing and Accountability
4. Configuration Management
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System and Communication Protection
14. System and Information Integrity

Implementing NIST SP 800-171 Requirements

	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													

41

*From DoD Industry Day June 23, 2017

Implementing NIST SP 800-171 Requirements

- Only limited “exceptions” to full implementation of NIST SP 800-171
  - COTS
  - DoD CIO adjudication that alternate security measure is equally effective
  - A security requirement is not applicable
  - Enduring exception
  - No “covered contractor information system”
  - No “covered information system”
- NIST SP 800-171, Rev. 1 (Dec 20, 2016): Requires “System Security Plan & Plan of Action & Milestones”
  - Rev. 2 Feb. 14, 2019: Enhancements for high value targets and critical programs
- Not automatically applicable retroactively
- Subcontractor flow down requirement
  - But prime contractor has increased discretion (in consultation with the contracting officer, if necessary) to decide if CDI is not involved

Safeguarding CDI in the Cloud

- Per -7012(b)(1)(i), cloud services "operated by or on behalf of" the federal government are subject to DFARS 252.239-7010 … which requires "administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG)."
- The SRG adds more obligations that must be met by CSPs for cloud service offerings, depending on the nature of DoD information involved. The Oct. 21 revision adds new provision -7012(b)(2)(ii)(D):

> (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 … FedRAMP Moderate baseline … and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber i**ncident reporting, malicious software, media preservation and protection, access** to additional information and equipment necessary for forensic analysis, and cyber incident **damage assessment.**

Cyber Incident Reporting

What is a cyber incident?

- Compromise or an actual or potential adverse effect on an information system or the information residing therein
- Compromise broadly defined to include disclosure or unauthorized access or violation of a security policy of a system where:
  - unauthorized intentional or unintentional disclosure, modification, destruction or loss of an object
  - copying of information to unauthorized media may have occurred

When must you file a report?

- Within 72 hours of determining that a cyber incident has affected (i) a covered contractor information system (one where CDI is stored, transits, or resides); (ii) CDI residing therein; and/or (iii) the contractor's ability to provide "operationally critical support"

Cyber Incident Reporting

What must be submitted to DoD?

- an Incident Collection Form (ICF) via https://dibnet.dod.mil/
- malware, if detected and isolated
- images of affected systems or access to covered contractor systems if requested

What obligations are imposed on subcontractors?

- Subcontractors must report directly to DoD and, absent additional language in the subcontract, provide only the ICF number to the prime
- Primes can negotiate for additional notification requirements

Cyber Incident Reporting

What information must be reported to DIBNET via ICF form?

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident.

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information

Cyber Incident Reporting

What Happens After Submission of the ICF?

- DoD Cyber Crime Center (DC3) processes and notifies all COs identified in the ICF (DSS will be notified if classified contracts at issue)
- DoD designates a lead Damage Assessment Management Office (DAMO) and CO to determine if a damage assessment is warranted and to seek additional information from the contractors

What is the purpose of a damage assessment?

- Determine impact on US military capabilities
- Consider how the compromised information could be used against the US
- Focus is on the data compromised rather than the mechanism of the compromise

Cyber Incident Reporting

What other notifications may be required?

- Regulatory notifications (DIB, DC3, DSS, DHS)
- Individuals whose PII was compromised
- Law enforcement and IC engagement
- Customers (including USG Programs, NATO, and foreign programs)
- Employees
- SEC
- Insurance brokers and insurers
- Contractual third parties or vendors
- Press

What if the agency wants more information about the incident and I am concerned about a privilege waiver of my internal investigation?

- Consider Voluntary Sharing Under CISA if Agency seeks more information

Preservation Obligations

Preservation: Following a cyber incident, contractors must preserve images of all known affected information and systems for at least 90 days (while DoD determines whether it will conduct a damage assessment).

- Have in place existing agreements with forensic experts so that you are not negotiating in the first 72 hours.
- Ensure that IRP includes preservation requirements so that IT personnel do not "fix" issues before you can preserve.

Handling Malware: If contractor discovers any malicious software related to the cyber incident, it must submit to DC3. Do not send the malicious software to the Contracting Officer.

Confidential & Proprietary Info: DoD has not offered specifics as to how it will protect confidential or proprietary information that it accesses following a breach; underscores need to appropriately mark proprietary data and PII if possible.

Government Audit Rights

- DFARS 252.204-7012(e-f)

(e) **Media preservation and protection.** When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) **Access to additional information or equipment necessary for forensic analysis**. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(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.

- DFARS 252.204-7012(b)(2)(ii)(D)

The contractor shall require and ensure…the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause

DoD Guidance

DoD Memos

- Sept 2017 – DFARS -7012 implementation (DPC; Assad)
- May 2018 – Role of DSS in CUI oversight (USD(I); Kernan)
- June 2018 – DoDIG cyber audits (DoDIG; Gorman)
- June 2018 – Navy submarine program review (PEO Subs; Jabaley)
- Sept 2018 – Enhanced cyber controls for Navy programs (RDA; Guerts)
- Oct 2018 – Protecting Critical Technology Task Force (DoD; Mattis)
- Nov 2018 – Reviewing SSPs/POAMs during acquisition & supply chain security (DPC; Herrington)
- Dec 2018 – Strengthened contract requirements for cyber (Acquisition; Fahey)
- Jan 2019 – Cyber oversight as part of contractor's purchasing system review (A&S; Lord)
- Feb 2019 – Strategically implementing cyber contract clauses (A&S; Lord)

DFARS -7012 Implementation Guidance

- Sept 17, 2017 – *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*
- Guidance to DoD elements as to how contractors may interpret, apply and satisfy NIST SP 800-171
  - **DoD "must mark, or otherwise identify in the contract …any [CDI]"**
  - No single or prescribed manner that contractor may choose to implement;
  - Suggestions and tools for how companies can approach compliance;
- Contractor is responsible to determine whether it has satisfied -171
- Third party assessments/certs "not required, authorized, or recognized"

DFARS -7012 Implementation (cont.)

- Emphasizes 3.12.4 and 3.12.2 (System Security Plan and Plans of Action)
- An SSP and plan of action can serve to document timely implementation of -171
- Solicitations may require SSP submission, review, incorporation or evaluation
- Agencies may use SSP and plan to evaluate overall risk of contractor's security

Role of DSS in CUI Oversight

- May 17, 2018 – *Controlled Unclassified Information (CUI) Implementation and Oversight for the Defense Industrial Base (DIB)*
- Designates Defense Security Service (DSS) as lead for implementing procedures for oversight of CUI for the DIB
- Tasks Director of DSS to execute a plan and produce a report regarding resource constraints, policy, and program improvements
- Still TBD?

DoDIG cyber audits

- June 22, 2018 - *Audit of the Protection of DoD Information Maintained on Contractor Systems and Networks*
- DoDIG announces audits to begin June 2018
- Goal to determine whether DoD contractors have security controls in place to protect DoD CUI maintained on their systems and networks from internal and external cyber threats

Overlapped with Navy program audits of Team Submarine contractor systems

Navy Enhanced Cyber Controls

- Sept 28, 2018 – *Implementation of Enhanced Security Controls on Select DIB Partner Networks*
- High risk programs to include new Contract Data Requirement Lists
  - SSP delivery and Gov't ability to validate contractor submission
  - Full implementation of certain NIST 800-171 requirements that were previously acceptable with POAM
  - Delivery of cyber incident information to DC3
  - Segregation of Navy CUI in some cases
- SOW contract requirements
  - Encryption at rest
  - NCIS installation of network sensors
- Requirement in future solicitations for SSP data as part of competitive source selection

Protecting Critical Technology Task Force

- Oct 24, 2018 – *Establishment of the Protecting Critical Technology Task Force*
- Secretary of Defense announces task force to protect DoD's critical technology
- Cross-functional task force to report to the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff

Reviewing SSPs/POAMs & supply chain security

- Nov 6, 2018 – *Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012*
- Intended to assist acquisition personnel to enhance -7012 protections
- "DoD Guidance for Reviewing SSPs and the NIST SP 800-171 Security Requirements Not Yet Implemented"
  - Enables consistent review of SSPs/POAMs
  - Guidance on impact if requirement isn't met
- "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System"
  - Tailorable framework to assess contractor approach to providing adequate security
  - Solicitation language and source selection guidance
- Includes CDRLs and Data Item Descriptions as attachments

Strengthening Contract Requirements

- Dec. 17, 2018 - *Strengthening Contract Requirements Language for Cybersecurity in the DIB*
- Provides two sample SOWs to be used with Nov. 6 DPC guidance
- Addresses access to/delivery of SSP and CDI flow down plans; assess compliance of Tier 1 suppliers

DCMA Oversight via Purchasing System Review

- Jan. 21, 2019 - *Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review*
- DCMA to leverage review of purchasing systems to review contractor procedures to:
  - ensure contractual DoD requirements for marking and distribution statements flow to Tier 1 Level Suppliers
  - assess DFARS/NIST compliance of Tier 1 Level suppliers

Implementing Cyber Contract Clauses

- Feb. 5, 2019 - *Strategically Implementing Cybersecurity Contract Clauses*
- DCMA to use its authority under FAR Part 42 and 43 and DFARS 242.302 to modify DCMA-administered contracts
- Limited to bilateral mods that do not result in change to contract price, obligated amount, or fee arrangement
- To be a strategic, not contract-by-contract, approach
  - Assess SSPs/POAMs; determine industry readiness and confidence levels; communicate to DoD Components
- Directs engagement with industry
- Considers leveraging DCMA's contracting officers authority to incorporate a repeatable strategic process/discussion to pursue no-cost bilateral block change

NIST Updates

NIST Updates

- NIST 800-171: *Protecting CUI in Nonfederal Systems and Organizations*
  - Rev 2 expected Feb. 14, 2019
    - To cover enhanced security requirements to protect CUI in high value assets and critical programs from advanced persistent threats (APT)
- NIST 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - Rev 5 (Final Public Draft) cleared Joint Task Force review early 2019; next OMB review and approval
    - To cover supply chain, privacy, cyber resiliency, and security engineering controls
- NIST 800-37: *Risk Management Framework for Information Systems and Organizations*
  - Rev 2 published Dec 2018
  - Addresses security, privacy, and supply chain risk in an integrated manner at the organization, mission/business process, and system levels

NIST SP 800-171A Assessment Guide

- Published June 2018
- Primary source of guidance for organizations conducting assessments of CUI security requirements in NIST SP 800-171
- “[A] starting point for developing assessment plans and approaches that can produce the level of evidence needed for risk-based decisions or to determine compliance”

NIST SP 800-171A (Cont.)

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- Chapter Two describes the fundamental concepts associated with assessments of CUI security requirements including assessment procedures, methods, objects, and assurance cases that can be created using evidence produced during assessments.

- Chapter Three provides a catalog of assessment procedures for the fourteen families of CUI security requirements in NIST Special Publication 800-171, including assessment objectives and potential assessment methods and objects for each procedure.

- Supporting appendices provide additional assessment-related information including general references; definitions and terms; acronyms; and a description of the assessment methods used in assessment procedures.

NIST SP 800-171A Example

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.3[a] *information flow control policies are defined.*
	3.1.3[b] *methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c] *designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d] *authorizations for controlling the flow of CUI are defined.*
	3.1.3[e] *approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

And back to the memos…

- June 2018 DoDIG cyber audit memo
- Jan 2019 DCMA oversight memo
- Plus program reviews/audits and CDRLs with review authority

Potential Risks – Noncompliance and Cyber Incidents

Risks - Noncompliance and Cyber Incidents

Material U.S. Gov't Contracts Risks

- Negative past performance evaluation
- Contract price adjustment
- Termination for default / convenience
- False Claims Act suits
- Responsibility determination - referral to SDO
- Disputes with teaming partners

Security / DSS Risks

- Suspension or revocation of facility security clearance, resulting in contract breaches
- Novation of classified contracts to another contractor with costs born by company
- Termination of classified contracts performed and denial of new classified contracts
- Revocation of certain personnel security clearances

Commercial Risks

- Third party notification requirements
- Privilege waiver
- State laws imposing data security requirements
- Litigation based on inadequate security controls
- Violations of data protection requirements in third party agreements
- Third party claims for the improper release of PII and/or PHI
- Insurance coverage disputes

Key Learning Points

Key Learning Points

- Cybersecurity Program:
  - Is similar to other corporate compliance programs
    - Top management support and responsibility
    - Good policies and employee awareness
    - Accountability
    - Adequate resources
  - Is a “Team Sport”
    - Legal IT, Security, Public Affairs, Contracts, etc.
  - Should be regularly monitored, tested and updated
    - Tabletops, Penetration Testing, and Outside Auditors
  - Involves industry and government partnering
- Appropriately incorporate cyber security into Board of Director oversight, activities and documents
- Subcontractor and vendor vetting and contract terms are essential
- Thoughtfully approach government disclosures and reporting
- Learn how to speak and translate “IT”

Introduction to Cybersecurity Issues for Government Contractors

Jeffery Chiow
Co-Chair, Government Contracts
Rogers Joseph O'Donnell
jchiow@rjo.com
(202) 777-8952

Kristin Grimes
Corporate Counsel (Cyber + Security) for Leidos
kristin.m.grimes@leidos.com
(571) 526-6326

Townsend Bourne
Partner, Government Contracts, Investigations, and International Trade Practice Group
Sheppard Mullin LLP
tbourne@sheppardmullin.com
(202) 747-2184