Navigating Unclassified Cyber/Information Security Protections

Network Penetration Reporting and Contracting for Cloud Services

Agenda

- Overview of DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services
- Definitions
- Safeguarding
  - NIST SP 800-171
  - Alternative Security Measures
- Flowdown to Subcontractors
- Cyber Incident Reporting and Damage Assessment
- Contracting for Cloud Services
- Questions

Overview

Navigating Unclassified Cyber/Information (System) Security Protections

Elements that drive appropriate protections: The information system and the information

Contractor's Internal System

Applicable controls:
NIST SP 800-171

Contractor System Operated on DoD's Behalf

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

Federal Contract Information

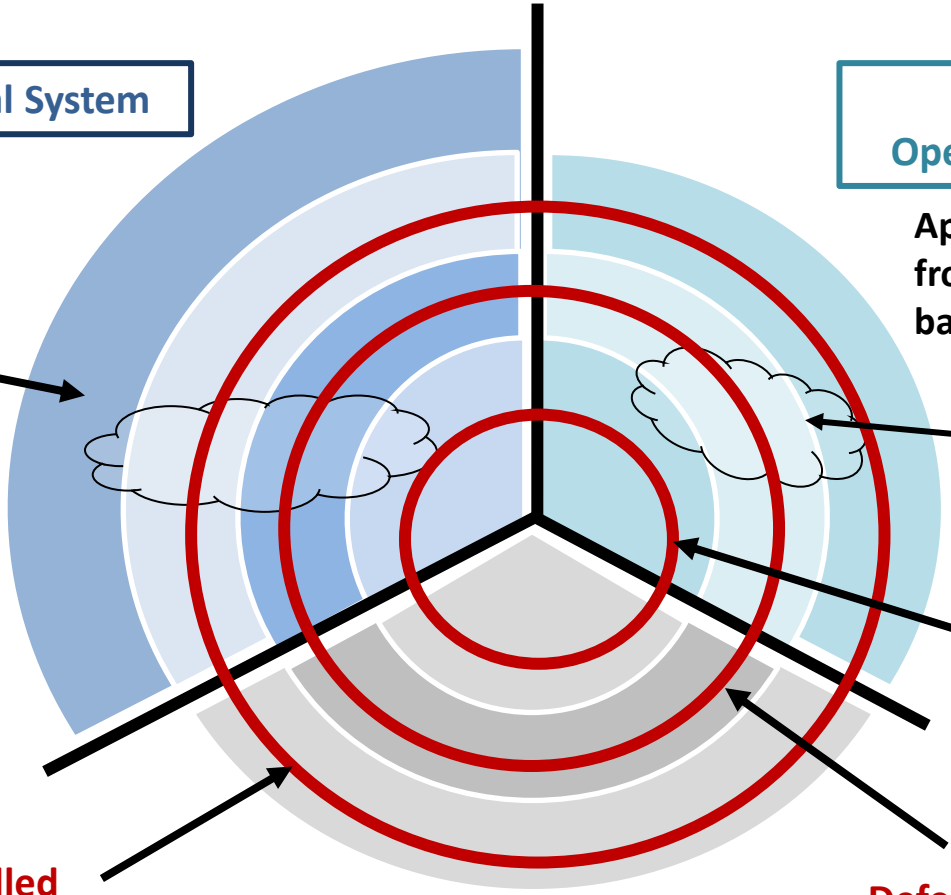
Cloud Service Provider

Applicable controls:
From the SRG

Unclassified Controlled Technical Information

Covered Defense Information

Controlled Unclassified Information (USG-wide)



DoD Information System

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

Unclassified

Protecting Unclassified Information on a Contractor's Internal System

DFARS Subpart 204.73 and DFARS Clause 252.205-7012		
	Published November 18, 2013	Published August 26, 2015
Scope – What Information?	• Applies to contracts and subcontracts requiring safeguarding of **unclassified controlled technical information** resident on or transiting through contractor unclassified information systems	• Applies to contracts and subcontracts requiring contractor and subcontractors to safeguard of **covered defense information** that resides in or transits through covered contractor information systems
Adequate Security – What Minimum Protections?	• Selected security controls in **NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**	• Security requirements in **NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations**

Network Penetration Reporting and Contracting for Cloud Services

- **DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, interim rule effective on Aug 26, 2015**
  - Revises the DFARS to implement Section 941 of NDAA for FY13 and Section 1632 of NDAA for FY15 (codified at 10 U.S.C. §§ 932 & 933)
  - Implements DoD policy and procedures for use when contracting for cloud computing services
- **Includes 3 clauses and 2 provisions:**

Safeguarding Covered Defense Information

- (p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information
- (c) Section 252.204-7009, Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- **(c) Section 252.204-7012, Safeguarding ~~of Unclassified Controlled Technical~~ Covered Defense Information and Cyber Incident Reporting**

Contracting For Cloud Services

- (p) Section 252.239-7009, Representation of Use of Cloud Computing
- **(c) Section 252.239-~~7999~~-7010, Cloud Computing Services**

Unclassified

Class Deviation - Safeguarding Covered Defense Information and Cyber Incident Reporting

Section 252.204-7008, Compliance with Safeguarding Covered Defense Information

- **Deviation 2016-O0001 (Oct 8, 2015): If the Offeror anticipates that additional time will be necessary to implement derived security requirement 3.5.3 in NIST SP 800-171, Use of multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts, the Offeror shall notify the Contracting Officer that they will implement the requirement within 9 months of contract award.**

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

- **Deviation 2016-O0001 (Oct 8, 2015): Allows offerors to request up to nine (9) months, after contract award, to comply with the multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts security requirement in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."**

Why was DFARS Case 2013-D018 published as an interim rule?

- A determination was made under the authority of the SECDEF that urgent and compelling reasons exist to promulgate the interim rule without prior opportunity for public comment in order to:
  - Increase and ensure uniform application of cyber security requirements placed on DoD information in contractor systems
  - Mitigate the risk of compromise of covered defense information
  - Ensure uniform application of policies and procedures for the acquisition of cloud computing services across DoD
  - Gain awareness of the full scope of cyber incidents being committed against defense contractors.
  - Implement Section 941 of the NDAA for FY 2013 and Section 1632 of the NDAA for FY 2015 (codified at 10 U.S.C. §§ 932 & 933)
- The public comment period ended November 20, 2015. Public comments will be considered in the formation of a final rule.

Definitions

Definitions

- **Covered Defense Information**
  - **Controlled Technical Information**
  - **Critical information (operations security)**
  - **Export controlled information**
  - **Other type of information that require protection**
- **Operationally Critical Support**
- **Cyber Incident**
- **Compromise**

Definitions

Covered defense information

- **Unclassified information that:**
  - **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;**

and

- **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 (e.g., privacy, proprietary business information)**

Definitions

Controlled technical information

- **Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.**

Critical information (operations security)

- **Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of the Operations Security process).**

Definitions

Export control

- **Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. Includes dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.**

Other types of information that require protection:

- **This category of Covered Defense Information is consistent with the definition of Controlled Unclassified Information (CUI) – information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified.**

Definitions

Operationally Critical Support

- **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.**
  - **Operationally Critical Support is an "activity"– not an information type – performed by the contractor. DFARS does not require protections for contractor information systems that are used to provide operationally critical support – only the requirement for the contractor to report a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.**
  - **Operationally Critical Support is not related to "Critical information (operations security)"**

Operationally Critical Support

Examples include but are not limited to the following:

(i) Operationally critical support for mobilization: Addressed under (ii) and (iii).	
(ii) Operationally critical support for distribution	**(iii) Operationally critical support for sustainment**
• Airlift, sealift, aeromedical, intermodal transportation services and associated material handling and ground handling labor or stevedore services. • U.S. railroad, truck, barge, ferry, and bus services provided by passenger & freight carriers, associated material/ground handling labor services. • Third party logistics (3PL) services provided by non-equipment owned brokers and freight-forwarders. • Transportation Protection Services for arms, ammunition, and explosives (AA&E) and courier materiel. • Transportation and packaging of hazardous material. • Information technology systems and network providers essential to the command, control operation, and security of contingency transportation mission functions delineated above.	• Local acquisition of Liquid Logistics; Cl I, Fresh Fruits, Vegetables; Meat/bread products, bottled gases. • Supply chain for rare earth metals. • Procurement/Product Support for critical weapons systems identified by the requiring activity. • Prime contractors/subcontractors for critical weapons systems in dev/sustainment fielded to AOR. • Contractor Logistics Support. Examples include Unmannned Aerial Systems maintenance, (aviation) training command maintenance spt, or performance based logistics/performance based arrangements. • Depot-level maintenance for critical items, particularly in Public-Private Partnerships. • IT systems and network providers essential to the command, control operation, and security of contingency supply and maintenance mission functions delineated above.

Unclassified

Definitions

Cyber Incident

- **As defined in DFARS 252.204-7012: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.**
- **As defined in DFARS 252.204-7009 and 252.239–7010: 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.**
- **Consistent use of the term "compromise" will be addressed in Final Rule**
  - **Inclusion of term "compromise" is intended to clarify, not to expand, the intended scope of "cyber incident"**

Compromise (DFARS Definition is from CNSSI 4009)

- **Disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.**
- **DFARS use of "Compromise" addresses information *and* system security**

Safeguarding

NIST SP 800-171

Why NIST SP 800-171?

NARA and NIST objected to DFARS' use of selected subset of the 800-53 controls

- Asserted the full 'moderate baseline' of 263 controls required for protection of CUI

Concern regarding implementation challenges for non-Federal systems

- 800-53 controls developed for Federal systems – 'build-to' vice 'performance' specs
  - Overly granular and difficult to apply to an 'as-built' contractor's system
  - Many baseline controls unnecessary (e.g., Availability controls) for protection of CUI
  - Many controls/elements should not apply outside the US Government (Federal-centric)

Some of the 'selected' 800-53 controls also problematic

- Individual controls often include unnecessary elements
- Some controls 'bundle' together disparate requirements unrelated to protecting CUI

Solution - Develop a dedicated NIST Special Publication for protection of CUI in nonfederal organizations

- Performance-based to be applicable to existing nonfederal systems
- Eliminate Federal-centric requirements
- Focus on the essentials – providing CUI confidentiality protection
- Based on FIPS 200 with essential control language from 800-53 to meet moderate impact level

Comparing NIST SP 800-53 to NIST SP 800-171

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*	NIST SP 800-171, *Protecting CUI in Nonfederal Information Systems and Organizations, Jun 15*
• Facilitates consistent and repeatable approach for selecting/specifying security controls – Federal focused (i.e., Systems operated by or for the federal government) – Controls address diverse set of security and privacy requirements across federal government/critical infrastructure	• Developed for use on contractor and other nonfederal information systems to protect CUI. • Tailored to eliminate requirements that are – Uniquely federal – Not related to CUI (e.g., availability controls) – Expected to be satisfied without specification (i.e., policy and procedural controls)
• "Build It Right" strategy provides flexible yet stable catalog of security controls to meet current information protection needs and the demands of future needs based threats, requirements, and technologies	• Enables contractors to comply using systems and practices they already have in place – Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI
• Provides recommended security controls for information systems categorized in accordance with FIPS 199 – Allows organizations to tailor relevant security control baseline to align with their mission/business environment	• 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 every CUI security requirement

Structure of NIST SP 800-171 Security Requirements

800-171 security requirements have a well-defined structure with the following components:

- **Basic security requirements section.**
  - **Essentially FIPS 200 requirements applicable to protection of CUI**
- **Derived security requirements section.**
  - **"Derived" from NIST 800-53 moderate baseline controls that are applicable to protection of CUI**
  - **Includes only the essentials – most 'procedural' elements have been eliminated**

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions authorized users are permitted to execute.	**AC-2 ACCOUNT MANAGEMENT** **The organization:** a. Identifies/selects the following types of information system accounts to support organizational missions/ business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **AC-3 ACCESS ENFORCEMENT** **The information system** enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **AC-17 REMOTE ACCESS** **The organization:** a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.8.9 Protect the confidentiality of backup CUI at storage locations.	**CP-9 INFORMATION SYSTEM BACKUP** **The organization:** a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. **Protects the confidentiality**, integrity, and availability **of backup** information **at storage locations.**
3.5.5 Prevent reuse of identifiers for a defined period. **3.5.6** Disable identifiers after a defined period of inactivity.	**IA-4 IDENTIFIER MANAGEMENT** **The organization manages information system identifiers by:** a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. **Preventing reuse of identifiers for** [*Assignment: organization-**defined** time **period***]; and e. **Disabling the identifier after** [*Assignment: organization-**defined** time **period of inactivity***].

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
3.10.3 Escort visitors and monitor visitor activity. **3.10.4** Maintain audit logs of physical access **3.10.5** Control and manage physical access devices	**PE -3 PHYSICAL ACCESS CONTROL The organization:** a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems/devices*]; *guards*]; b. **Maintains physical access audit logs** for [*Assignment: organization-defined entry/exit points*]; c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible; d. **Escorts visitors and monitors visitor activity** [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*]; **e. Secures keys, combinations, and other physical access devices;** **f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and** **g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.**

Replacing NIST SP 800-53 based controls with NIST SP 800-171

Derived Security Requirement:

- Most substantial addition is requirement for multifactor authentication
- NOT a requirement to use PIV/CAC, but any method described in NIST SP 800-63-2, Electronic Authentication Guideline (e.g., password plus cell-phone txt message)

Annex D, Mapping Tables

- Maps 800-171 requirements to 800-53 and ISO/IEC 27001 controls
- INFORMATIONAL ONLY– tables NOT intended to convey or impart ANY additional CUI security requirements beyond Basic/Derived requirements in Chapter 3
- Agencies shall NOT require the mapped 800-53 control
  - The 800-171 Basic or Derived Requirement IS the requirement
- Agencies may, in special circumstances, require additional security controls and then reference an additional 800-53 control
  - Additional control should NOT be a control included in the mapping table

Annex E, Tailoring Tables

- Provides rationale for not including a 800-53 moderate control in 800-171
- NFO: Expected to be routinely satisfied by Nonfederal Org without specification – agencies may ask 'how' these are implemented by the contractor (e.g., "what mechanisms does the company employ to ensure requirement xx is properly implemented and sustained?")

Alternative Security Measures and Non-applicable Requirements

- If the offeror proposes to deviate from any of the security requirement in NIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of -
    1. Why a particular security requirement is not applicable; or
    2. How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and to achieve equivalent protection
- An authorized representative of the DoD CIO will provide an assessment of the proposed deviation to the contracting officer

Flowdown to Subcontractors

- **The Contractor shall include the substance of DFARS Clause 252.204-7012 in all subcontracts**
- **The requirements of DFARS Clause 252.204-7012 will create obligations only in subcontracts for operationally critical support, or for which subcontract performance will involve a covered contractor information system**
  - **The subcontractor need only provide adequate security when effort will involve a covered contractor information system, i.e., their information system will process, store, or transmit covered defense information**
- **This is the same approach that is used at the prime contractor level**

Cyber Incident Reporting and Damage Assessment Activities

Cyber Incident Reporting

- **Contractors are required to rapidly report cyber incident directly to DoD at http://dibnet.dod.mil.**
- **A medium assurance certificate is required to access the reporting module.**
- **When the contractor completes the on-line form and submits the report, the DoD Cyber Crime Center (DC3) receives the report. DC3 sends an unclassified encrypted email to the contracting officer with the reported information.**
- **DC3 is the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DoD contractors.**

Network Penetration Reporting - Reporting a Cyber Incident

What is a cyber incident?

- Defined as "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"

Who should report and why?

- DoD contractors report cyber incidents in accordance with the DFARS Clause 252.204-7012
- DoD contractors report in accordance with other reporting requirements identified in a contract or other agreement.
- DoD Cloud Service Providers report cyber incidents in accordance with DFARS Clause 252.239-7010 as specified in the Cloud Security Requirements Guide
- DoD-DIB CS/IA Participants report cyber incidents in accordance with the Framework Agreement (FA)

Where to report?

- DC3 is the single DoD focal point for receiving all cyber incident reporting from unclassified networks of DoD contractors through the DIBNet portal at http://dibnet.dod.mil

ALL reporting will be via the Incident Collection Format (ICF) found at http://dibnet.dod.mil

Network Penetration Reporting - Damage Assessment

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

Contracting for Cloud Services

DFARS subpart 239.76, Cloud Computing:

- **Implements policy developed within the DoD CIO and the DoD Cloud Computing Security Requirements Guide (SRG) for the acquisition of cloud computing services**
- **Directs use of new provision 252.239-7009, Representation of Use of Cloud Computing in solicitations for information technology services**
  - **Allows the offeror to represent their intention to utilize cloud computing services in performance of the contract or not.**
- **Directs use of new clause 252.239-7010, Cloud Computing Services in solicitations and contracts for information technology services**
  - **Provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements**
  - **Implements DoD's policies concerning Cloud Computing Services to ensure uniform application when DoD entities contract for cloud services across the DoD.**

DFARS 252.239-7010(d) The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted to the Department of Defense via http://dibnet.dod.mil/.

Covered Defense Information on the "Cloud"

- When an information system is being operated on the DOD's behalf, it is considered a DoD system, and needs to meet the same requirements as if it were operated by DoD. The DoD Cloud Computing Security Requirements Guide (SRG) applies when:
  - A cloud solution is being used to process data on the DoD's behalf
  - DoD is contracting with Cloud Service Provider to host/process data in a cloud
  - A cloud solution is being used for processing that we (the DoD) would normally do ourselves but have decided to outsource
- NIST SP 800-171 is designed to be used by nonfederal organizations to protect Controlled Unclassified Information (CUI). The NIST SP 800-171 applies when:
  - A cloud solution is used by the contractor to do his own 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.

Questions?

For follow-up questions regarding the content of this brief,
email: osd.dibcsia@mail.mil