Cybersecurity Challenges

Protecting DoD's Unclassified Information

Implementing DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

What Happens on December 31, 2017?

Outline

- DFARS Clause 252.204-7012 — Contractor and Subcontractor Requirements
- Adequate Security — NIST SP 800-171
- Compliance — What Happens on December 31, 2017?
- Resources

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

Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%).

AT&T Cybersecurity Insights Vol. 4

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.

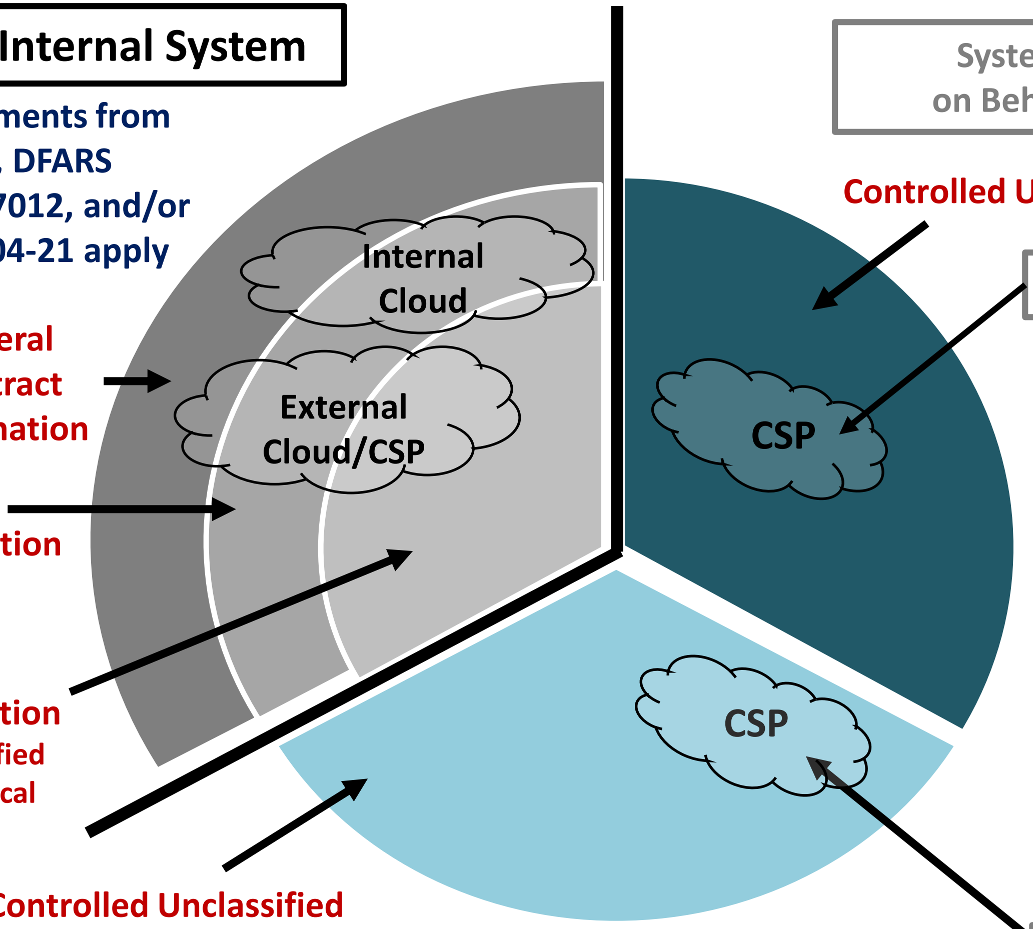
NYSE Governance Services and security vendor Veracode

Protecting DoD's Unclassified Information

DoD has a range of activities to include both regulatory and voluntary programs to improve the collective cybersecurity of the nation and protect U.S. interests

- **Securing DoD's information**
  - **Codifying cybersecurity responsibilities and procedures for the acquisition workforce in defense acquisition policy**
  - **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"** ***(Revision 1 published Dec 2016)***

Protecting the DoD’s Unclassified Information



Contractor’s Internal System

Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

Covered Defense Information (includes Unclassified Controlled Technical Information)

System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

Controlled Unclassified Information

DoD Owned and/or Operated Information System

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

Unclassified

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

DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1. **Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network**
2. **Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support**
3. **Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center**
4. **If requested, submit media and additional information to support damage assessment**
5. **Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information**

Covered Defense Information — Definition

Covered defense information – Term used to identify information that requires protection under DFARS Clause 252.204-7012

Covered defense information means:

- **Unclassified controlled technical information (CTI) or other information as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is –**
  1) **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**
  2) **Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract***

*** "In support of the performance of the contract" is not meant to include the contractor's internal information (e.g., human resource or financial) that is incidental to contract performance**

Identification and Marking of Covered Defense Information

Existing DoD policy/regulations require DoD to:

- **Identify covered defense information and mark information in accordance with DoD procedures for controlled unclassified information (CUI) found in DoDM 5200.01 Vol 4, DoD Information Security Program: Controlled Unclassified Information (CUI)**
- **Document in the contract (e.g., Statement of Work, CDRLs) information, including covered defense information, that is required to be developed for performance of the contract,**
  - **Specify requirements for the contractor to mark, as appropriate, information to be delivered to DoD**

The contractor is responsible for:

- **Following the terms of the contract, which includes the requirements in the Statement of Work**

Adequate Security for Covered Defense Information

To provide adequate security to safeguard covered defense information:

DFARS 252.204-7012 (b) Adequate Security. … the contractor shall implement, at a minimum, the following information security protections:

***

(b)(2)(ii)(A): The contractor shall implement NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations, as soon as practical, but not later than December 31, 2017

***

(b)(3): Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required

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* at confidentiality impact level “moderate”, in accordance with FIPS 199 (32 CFR 2002.12)

- Consists of performance-based security requirements which significantly reduce unnecessary specificity
  - Enables contractors to comply using systems and practices already in place
  - More easily applied to existing systems

- Provides standardized/uniform set of security requirements for all CUI*
  - Allows nonfederal organizations to consistently implement one solution to protect CUI* for all customers
  - Allows contractor to implement alternative, but equally effective, security measures to satisfy CUI* security requirements

* For DoD, this applies to covered defense information as defined in DFARS 252.204-7012

Implementing NIST SP 800-171 Security Requirements

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**

   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 or assistance**
3. **Develop plans of action to implement the requirements**

Implementing NIST SP 800-171 Security Requirements

- **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**

(see 252.204-7008(c)(2)(i) and 252.204-7012(b)(2)(ii)(B))

- **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.**

(see 252.204-7012(b)(2)(ii)(A))

Contractor Compliance — Implementation of DFARS Clause 252.204-7012

- **By signing the contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012**
- **The DFARS rule did not add any unique/additional requirements for the Government to monitor contractor implementation of required security requirements**
  - **DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements**
  - **3rd party assessments or certifications of compliance are not required, authorized, or recognized by DoD**
- **If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract**

Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

NIST SP 800-171, Revision 1, Chapter 3:

- When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements

NIST SP 800-171, Security Requirement 3.12.4:

- Develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

NIST SP 800-171, Security Requirement 3.12.2:

- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

Demonstrating Implementation of NIST SP 800-171 — System Security Plan and Plans of Action

The system security plan may also be used to document/describe:

- Situations where requirements cannot practically be applied (non-applicable)
- Alternative but equally effective security measures approved by DoD CIO
- Situations where specialized systems, such as medical devices, CNC or other shop floor equipment, cannot by their nature meet the NIST SP 800-171 requirements
- Situations when the contractor’s policy, process, etc., does not allow the circumstances addressed in the security requirements. For example:
  - Requirement 3.1.12 states that remote access must be monitored and controlled, but the organization does not allow (and positively prevents by technical or procedural means) remote access.
  - Requirement 3.1.18 requires controlling the connection of mobile devices, but the organization does not allow such connections and ensures such connections are not provisioned.
- Individual, isolated or temporary deficiencies addressed by assessing risk and applying mitigations

Implementation of NIST SP 800-171 — What Happens on December 31, 2017?

- In response to the December 31, 2017 implementation deadline, companies should have a system security plan in place, and associated plans of action to address any security requirements not yet implemented
  - If Revision 1 of NIST SP 800-171 was not "in effect" when the contract was solicited, the contractor should work with the contracting officer to modify the contract to include NIST SP 800-171, Revision 1 (December 2016)
  - DoD guidance is for contracting officers to work with contractors who request assistance in working towards consistent implementation of the latest version of DFARS Clause 252.204-7012 and NIST SP 800-171
- The contractor self-attests (by signing contract) to be compliant with DFARS Clause 252.204-7012, to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the system security plan and associated plans of action)
- The solicitation may require or allow elements of the system security plan, and any associated plans of action, to be included with the contractor’s technical proposal, and may subsequently be incorporated, by reference, as part of the contract (e.g., via Section H special contract requirement)

Role of the System Security Plan and Plans of Action in Source Selection and Contract Formation / Administration

NIST SP 800-171, Revision 1, Chapter 3: Federal agencies may consider the submitted system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization

Examples of how a requiring activity may utilize the system security plan and associated plans of action include:

- Requiring that proposals i) identify any NIST SP 800-171 security requirements not implemented at the time award and ii) include associated plans of action for implementation
- Identifying in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award
- Identifying in the solicitation that the contractor's approach to providing adequate security will be evaluated in the source selection process

Implementing NIST SP 800-171 – Where to Get Assistance

- NIST Manufacturing Extension Partnership (MEP)
  - Public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers
- Procurement Technical Assistance Program (PTAP) and Procurement Technical Assistance Centers (PTACs)
  - Nationwide network of centers/counselors experienced in government contracting, many of which are affiliated with Small Business Development Centers and other small business programs
- Cybersecurity Evaluation Tool (CSET)
  - No-cost application, developed by DHS’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides step-by-step process to evaluate industrial control system and information technology network security practices

Resources

- Cybersecurity in DoD Acquisition Regulations page at *http://dodprocurementtoolbox.com/* for Related Regulations, Policy, Frequently Asked Questions, and Resources
- DPAP Website *http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html* for DFARs, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- Cybersecurity Evaluation Tool (CSET) - Download at *https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET* or request physical copy of software at *cset@dhs.gov* — Select "Advanced Mode" to display option to select NIST 800-171
- NIST Manufacturing Extension Partnership at *https://www.nist.gov/mep*
- The Procurement Technical Assistance Program (PTAP) at *http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx*

Questions? Submit via email at osd.dibcsia@mail.mil