Cybersecurity Challenges

Protecting DoD's Unclassified Information

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

August 15, 2018

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

- Protecting DoD's Unclassified Information
- DFARS Clause 252.204-7012 — Safeguarding covered Defense Information and Cyber Incident Reporting
- Compliance
  - Demonstrating Implementation of the Security Requirements in NIST SP 800-171
  - Compliance with DFARS Clause 252.204-7012
  - Considering a Contractor's Internal Information System in Source Selection
- 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

61% of breach victims are businesses with <1,000 employees

80% of breaches leverage stolen, weak, and/or guessable passwords

2017 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.

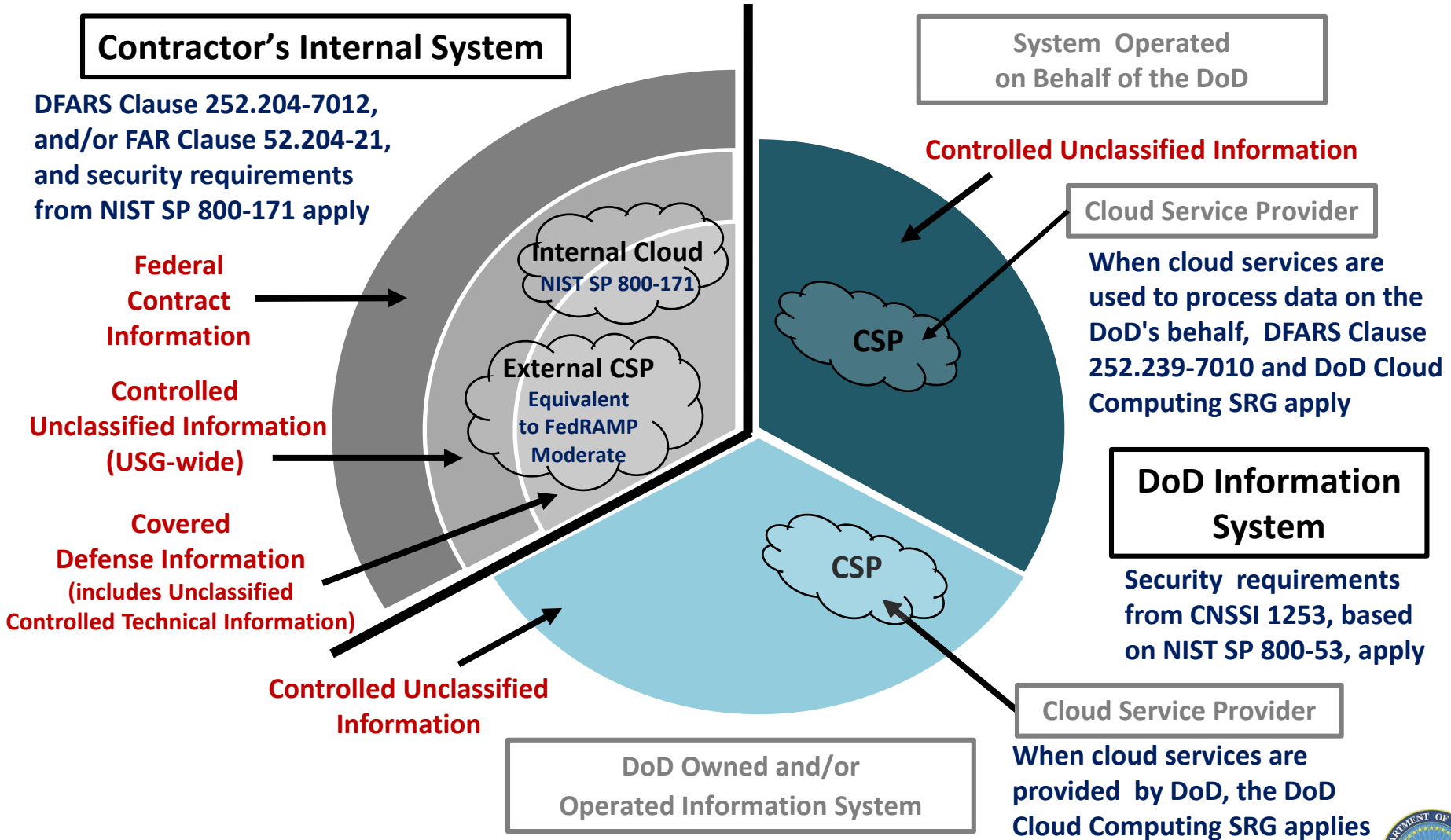
NYSE Governance Services and security vendor Veracode

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**
- **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



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**

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 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

DFARS 252.204-7012 directs <u>how</u> the contractor shall protect covered defense information; The requirement <u>to</u> protect it is based in law, regulation, or Government wide policy.

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 requirements can readily be accomplished by in-house IT personnel and which require additional research or assistance**
3. **Develop a plan of action and milestones to implement the requirements**

Cyber Incident Reporting

DFARS 204.7302 (d)

A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- **Contractors/subcontractors must submit a cyber incident report via https://dibnet.dod.mil/**
- **Upon receipt of a cyber incident report —**
  - **DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s)**
  - **The contracting officer(s) provides the report to the requiring activity(ies)**
  - **DC3 analyzes report to identify cyber threat vectors and adversary trends**
  - **DC3 contacts the reporting company if the report is incomplete**

Cyber Incident Damage Assessment Activities

DoD decision to conduct a cyber incident damage assessment —

- **The DoD Component damage assessment office (DAMO) and Requiring Activity will determine if a cyber incident damage assessment is warranted**
- **Once the decision to conduct an assessment is made - the Requiring Activity will notify the contractor via the Contracting Officer, and the Contracting Officer will request media from the contractor**

Purpose of the cyber incident damage assessment —

- **Determine impact of compromised information on U.S. military capability underpinned by the technology**
- **Consider how the compromised information may enable an adversary to counter, defeat, or reverse engineer U.S. capabilities**
- **Focus on the compromised intellectual property impacted by the cyber incident – not on the compromise mechanism**

Subcontractor Flowdown

When should DFARS Clause 252.204-7012 flow down to subcontractors?

- **The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information**
- **The contractor shall determine if the information required for subcontractor performance is, or retains its identify as, covered defense information and requires safeguarding**
- **Flowdown is a requirement of the terms of the contract with the Government, which must be enforced by the prime contractor as a result of compliance with these terms**
  - **If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not be shared with the subcontractor or otherwise reside on it's information system**

The Department's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flowdown of information requiring protection.

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

- **To document implementation of NIST SP 800-171, companies should have a system security plan in place, in addition to any associated plans of action:**
  - **Security Requirement 3.12.4 (System Security Plan): Requires the contractor to 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**
  - **Security Requirement 3.12.2 (Plans of Action): Requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems, and to describe how and when any unimplemented security requirements will be met**

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
- It is the contractor's responsibility to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)
  - DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements
  - Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD

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

- Per 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
- "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" was drafted to facilitate the consistent review of system security plans and plans of action
- "Assessing the State of a Contractor's Internal Information System in a Procurement Action" was drafted to illustrate how the DoD may choose to assess/consider submitted System Security Plans and Plans of Action

How Can a Contractor's System Security Plan and/or Internal System Impact a Procurement Action?

	Acquisition Scenario	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
Pre Award → Post Award	1. Evaluate implementation of NIST SP 800-171 at source selection – Alternative 1A: Go/No Go decision based on implementation status of NIST SP 800-171 – Alternative 1B: Assess NIST SP 800-171 implementation as a separate technical evaluation factor 2. In addition to the security requirements in NIST SP 800-171, also evaluate any added protections that my be required 3. Assess/track implementation of NIST SP 800-171 security requirements after contract award – The government may also monitor compliance of NIST SP 800-171 with continuous monitoring or an independent government review 4. Contractors 'self-attest' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171			

Defense Contract Management Agency (DCMA) Oversight of DFARS Clause 252.204-7012

Actions DCMA will take in response to DFARS Clause 252.204-7012:

- **Encourage industry to adopt corporate, segment, or facility-level system security plans as may be appropriate in order to ensure more consistent implementations and to reduce costs**
- **Verify that system security plans and any associated plans of action are in place (DCMA will not assess plans against the NIST 800-171 requirements)**
- **If potential cybersecurity issue is detected –notify contractor, DoD program office, and DoD CIO**
- **During the normal Contract Receipt and Review process -verify that DFARS Clause 252.204-7012 is flowed down to sub-contractors/suppliers as appropriate**
- **For contracts awarded before October 2017 -verify that contractor submitted to DoD CIO notification of security requirements not yet implemented**
- **Verify contractor possesses DoD-approved medium assurance certificate to report cyber incidents**
- **When required, facilitate entry of government assessment team into contractor facilities via coordination with cognizant government and contractor stakeholders**

Resources

- Cybersecurity in DoD Acquisition Regulations page - Regulations, Policy, Frequently Asked Questions (FAQs), and Resources *https://dodprocurementtoolbox.com/*
- NIST Manufacturing Extension Partnership (MEP) - "Cybersecurity Self-Assessment Workbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements" *https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf*
- 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 *http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx*
- Cybersecurity Evaluation Tool (CSET) - No-cost application, developed by DHS, provides step-by-step process to evaluate information technology network security practices *https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET*

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

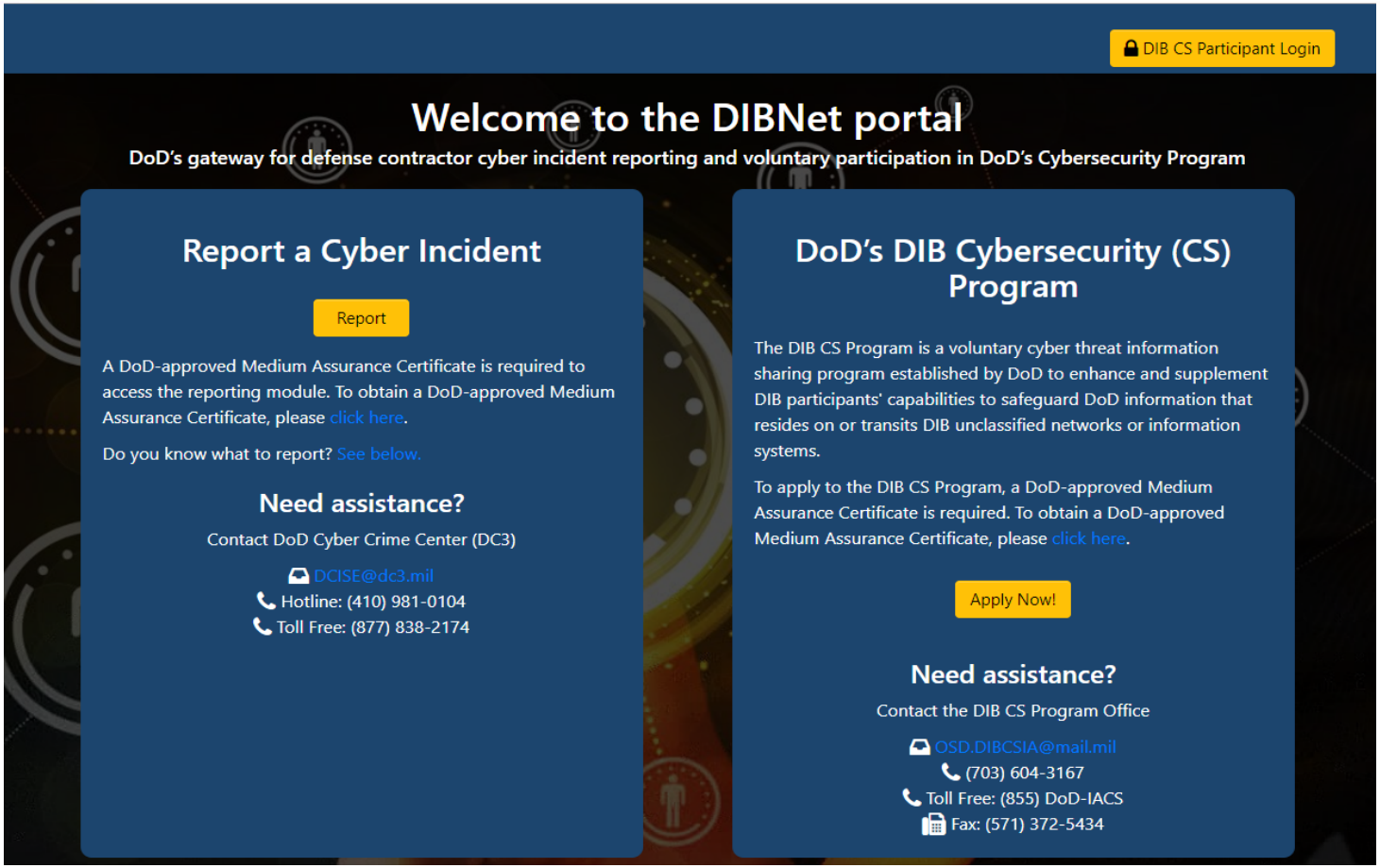
DoD's Defense Industrial Base (DIB) Cybersecurity Program

A public-private cybersecurity partnership that:

- **Provides a collaborative environment for sharing unclassified and classified cyber threat information**
- **Offers analyst-to-analyst exchanges, mitigation and remediation strategies**
  - **Provides companies analytic support and forensic malware analysis**
  - **Increases U.S. Government and industry understanding of cyber threat**
  - **Enables companies to better protect unclassified defense information on company networks or information systems**
  - **Protects confidentiality of shared information**

Mission: Enhance and supplement Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems

DIB CS Web Portal



Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the **ECA website**.

https://www.DIBNet.dod.mil