HII's Supply Chain Cybersecurity Compliance and Risk Mitigation Program

"SC3RMP"

Supplier Webinar

September 24, 2019

Speakers

- **Chris Page**, Attorney, Newport News Shipbuilding
- **Andrew Pilant**, Attorney, Ingalls Shipbuilding
- **Kendra Queeney**, Manager, SCM Compliance, Newport News Shipbuilding

Agenda

- Background – How did we get here?
- Cybersecurity Requirements/Regulations
- SC3RMP Scope
- SC3RMP Overview
- SC3RMP Process
- Resources
- Questions and Answers

The content discussed in this presentation is provided for informational purposes only and does not constitute legal advice or counsel. For legal advice related to issues discussed in this presentation, please consult your attorney.

Background

- Common Methods of Cyber Intrusion:
  - Credential Stuffing
    - Stealing user name and password from one site and using on another
  - Collaboration App Security (Slack, Dropbox, SharePoint)
    - Apps installed without security precautions being taken first
  - Ransomware
    - Files/Servers locked until payment of ransom for unlock code
  - Phishing
    - Clicking on an emailed link downloads malware leading to network breach
  - Internet of Things
    - Use weak or no security on one device to breach/enter network

EVERYONE IS AT RISK

Background – Recent Cyber Attacks

- **August 2019**
  - China used compromised websites to distribute malware through Apple, Google, and Windows phones.
  - Chinese hackers target U.S. cancer institutes to steal cutting edge cancer research
  - Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning.
  - Russian hackers used vulnerable IoT devices like a printer, VOIP phone, to break into high-value corporate networks
  - Chinese hackers conducted a spear-phishing campaign against employees of U.S. utility companies
- **July 2019**
  - Capital One reveals that a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers.
  - Encrypted email service provider ProtonMail was hacked by a state-sponsored group looking to gain access to accounts held by reporters and former intelligence officials conducting investigations of Russian intelligence activities.
  - Several major German industrial firms including BASF, Siemens, the Chinese government
  - A Chinese hacking group was discovered to have targeted government agencies across East Asia involved in information technology, foreign affairs, and economic development.
  - The U.S. Coast Guard issued a warning after it received a report that a merchant vessel had its networks disrupted by malware while traveling through international waters
  - Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, NGOs, and other political organizations around the world, with the majority of attacks originating in Iran, North Korean, and Russia.

Background

- Cyber intrusion can be for espionage, sabotage, theft, ransom, disruption
- Foreign Governments have breached Contractor networks to steal sensitive U.S. defense plans and designs, including:
  - F-35 Joint Strike Fighter
  - Advanced Patriot PAC-3 missile system
  - Army's Terminal High Altitude Area Defense (ballistic missile defense)
  - Navy's Littoral Combat Ship
  - Navy's Sea Dragon super-sonic anti-ship missile for submarines

"There are two types of Companies: Those that have been hacked by the Chinese, and those that do not know they have been hacked by the Chinese."

Background

- The aggregate loss of **Covered Defense Information (CDI)** from the Defense Industrial Base (DIB) **increases risk to national economic security and in turn, national security.**

- The Council of Economic Advisers, an agency within the Executive Office of the President, estimates that malicious ***cyber activity costs the U.S. economy between $57 billion and $109 Billion annually.***

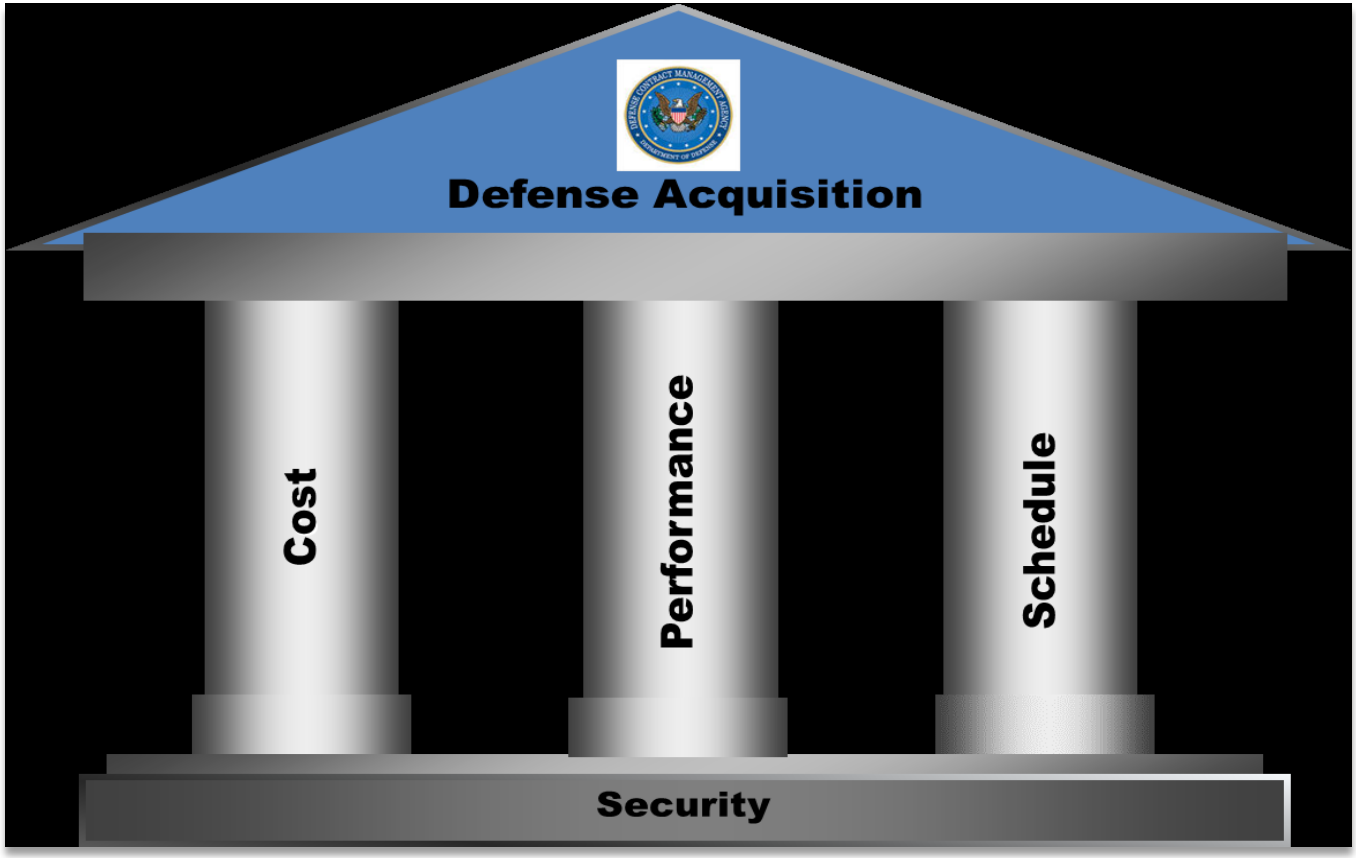
  [Ref: "The Cost of Malicious Cyber Activity to the U.S. Economy, CEA" February 2018]

- The Center for Strategic and International Studies (CSIS), in partnership with McAfee, reports that ***as much as $600 Billion, nearly 1% of global GDP, may be lost to cybercrime each year.***

  [Ref: "Economic Impact of Cybercrime - No Slowing Down" February 2018]

Background

- The Department of Defense is focused on making **SECURITY** the **FOUNDATION** of Defense Acquisition

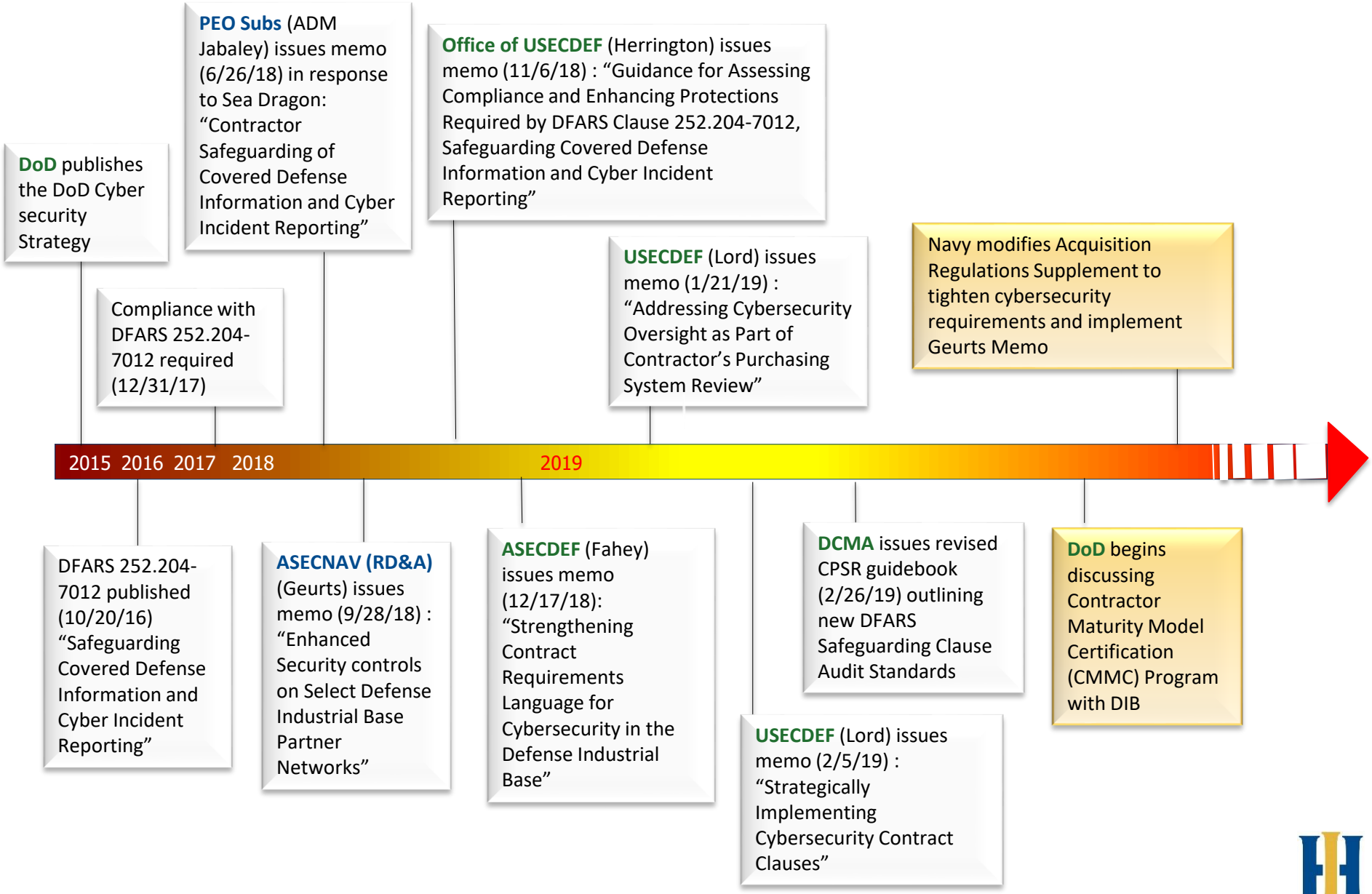


Background

- With the growing cybersecurity threat to the entire Department of Defense (DoD) supply chain, the Government is encouraging defense industry prime contractors to take action to **manage** that risk.

- HII recognizes the significance of the supply chain cybersecurity risk, and how recent events have shaped the DoD's increased emphasis on actively and efficiently mitigating the risk.

Changing Cybersecurity Landscape



DFARS 252.204-7012

Effective in prime contracts issued after October 2016

- Standard is NIST SP 800-171 *(DoD CIO must approve exceptions and alternative measures)*
- Deadline to meet NIST SP 800-171 was December 31, 2017
- Must report areas of non-compliance to DoD CIO
- Cyber incidents must be reported within 72 Hours to both:
  - DoD
  - Higher Tier Contractor
- *Required Inclusion in all DoD Contracts*
- *Mandatory Flowdown to all Subcontractor Tiers*

DFARS 252.204-7012 Applicability

- Unclassified systems owned or operated by, or for, a contractor and that processes, stores or transmits:

- "*Covered Defense Information,*" (CDI) which includes:
  - **Technical Information marked with a DoD Distribution Statement (B-F);**
  - **Export Controlled Information**; or
  - Any other information that requires safeguarding or dissemination controls, and is (a) marked or otherwise identified in the contract and provided by the Govt, or (b) developed, received, transmitted, used, stored, etc. by the Contractor in support of the contract.

"Covered Information Systems" and "Covered Defense Information" are Broad Concepts

HII's Enterprise View

- HII is taking a broad-based, coordinated enterprise approach that will help the Navy and increase cybersecurity of the supply chain
  - Preparing for the *direct* implications of the changing cyber requirements as well as the *indirect* implications on the business, suppliers of HII and ultimately the Navy
  - Aimed at addressing HII's cybersecurity posture (technical, contractual, regulatory) and meeting DoD's expectations of prime contractor responsibility for supply chain cybersecurity compliance

- HII is implementing a comprehensive, risk-based approach to supply chain cybersecurity – the **Supply Chain Cybersecurity Compliance and Risk Mitigation Program (SC3RMP)**
  - Aimed at assessing and appropriately mitigating cybersecurity risks, raising awareness, and developing proportionate and effective defenses of and across HII's supply chain.

SC3RMP - Overview

- Supplier uses the *Exostar Partner Information Manager (PIM)* solution to complete the survey regarding the extent of compliance with NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”

- Using the information provided by the supplier, HII will conduct a risk assessment of the supplier’s current cybersecurity posture, and when appropriate will undertake actions to address perceived shortfalls with Supplier, as well as provide education and proposed mitigation actions to ensure compliance

SC3RMP - Scope

- Applies to all HII suppliers who receive, develop, or transmit CDI electronically as part of their HII Purchase Order (PO).
- Program has commenced, but supplier onboarding into the program through Exostar is ongoing and will continue into 2020.
  - More specific deadlines for Exostar Questionnaire completion will be disseminated through direct email communication from HII SC representatives
- For any supplier that is expected to require access to CDI, participation in the program is mandatory to continue doing business with HII
- New clause in HII T&Cs (HII Appendix A - DoD versions) implements participation requirement:

> ***CYBERSECURITY.*** ***(back to top)***
>
> *Buyer has implemented a Supply Chain Cybersecurity Compliance and Risk Mitigation Program (SC3RMP) to help assess and appropriately mitigate cybersecurity risks, raise awareness, and develop proportionate and effective defenses of and across Buyer's suppliers. A critical element of SC3RMP is Buyer's use of Exostar's Partner Information Manager Tool (PIM), which provides a secure platform to report the status of a company's compliance with DFARS 252.204-7012, and more specifically the security requirements of NIST SP 800-171. Upon request of Buyer, Seller agrees to register and maintain an active account with Exostar PIM (located at https://my.exostar.com/pages/viewpage.action?pageId=12125152) and to complete the Exostar PIM cybersecurity questionnaire. Seller also agrees to provide Buyer with information reasonably required by Buyer to assess and address any cybersecurity risks identified by SC3RMP.*

SC3RMP – Exostar Set-up

- Supplier completes Exostar proofing process
- Exostar validates supplier POC
- Supplier receives access credentials to access NIST SP 800-171 Questionnaire
- Supplier completes NIST SP 800-171 Questionnaire

Exostar Partner Information Manager (PIM)

- Exostar PIM is a third-party platform used by many prime contractors to manage supplier compliance with DFARS requirements.
- Many of you have already been contacted by Exostar requesting the appropriate point of contact for your company to complete the Exostar NIST SP 800-171 Questionnaire.
- Exostar's tool allows your company to complete the questionnaire once and later share the results with any other participating prime contractors who request it.
- This "ask once and share" model reduces the time your company will have to spend completing multiple questionnaires and provides a standard and consistent set of minimum cybersecurity expectations.
  - You may have been asked to complete the questionnaire by a different prime contractor or may be asked to do so in the future.
  - In these cases, you should be able to use the "ask once and share" model to share your completed form with us and other contractors.

Exostar Partner Information Manager (PIM)

- A system-generated invitation email is sent including instructions for setting up accounts and includes information to obtain a security token.

- New security tokens are only required if your company does not already have one (*i.e.*, existing Exostar tokens are sufficient)
  - In order to access the Exostar PIM, where the NIST SP 800-171 questionnaire is hosted, you will be required to access it with at least a phone-based “OTP token”. The price on this is $25.00 USD for domestic suppliers and $47.00 for international. We do not require any higher level of proofing for this.

Exostar NIST SP 800-171 Questionnaire

NIST SP 800-171 Questionnaire

3.1 Access Control | 3.2 Awareness and Training | 3.3 Audit and Accountab...

21%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.2)

- [ ] 3.2.1.Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
- [ ] 3.2.2.Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- [ ] 3.2.3.Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Guidance

You are in the '3.2 Awareness and Training' section of this questionnaire.

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

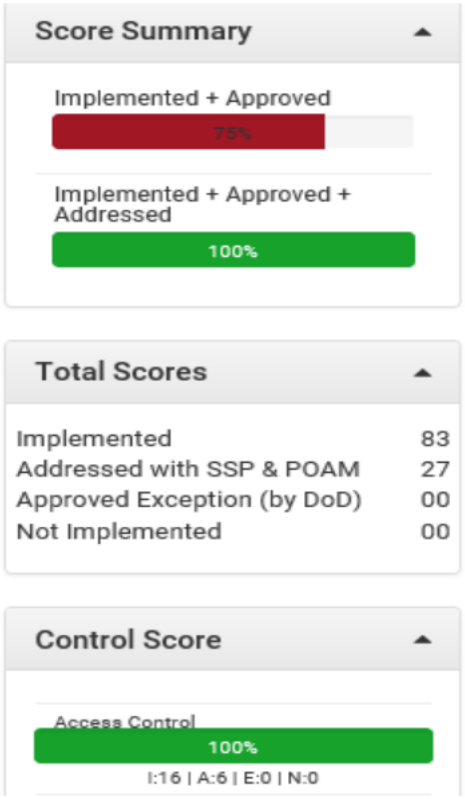
1. The supply chain representative for the company with which you are working.

2. The NIST special publication NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

3. The US Department of Defense Frequently Asked Questions regarding NIST SP 800-171

Exostar NIST SP 800-171 Questionnaire

- The NIST SP 800-171 Questionnaire covers the following sections:
  - 3.1 Access Control
  - 3.2 Awareness and Training
  - 3.3 Audit and Accountability
  - 3.4 Configuration Management
  - 3.5 Identification and Authentication
  - 3.6 Incident Response
  - 3.7 Maintenance
  - 3.8 Media Protection
  - 3.9 Personnel Security
  - 3.10 Physical Protection
  - 3.11 Risk Assessment
  - 3.12 Security Assessment
  - 3.13 System and Communications Protection
  - 3.14 System and Information Integrity
  - Additional Details



- The completed questionnaire will result in a risk rating from 1-100% as depicted in the screen print above. A score will also be provided on each control.
- Your answers to the questionnaire will be treated as your company's proprietary information by Exostar and HII and can only be changed by your company

SC3RMP

- Upon completing the Exostar Questionnaire, HII SC3RMP team members will analyze your company's responses.
- Based on your responses, you may be contacted by HII SC3RMP cybersecurity representatives for follow-up phone discussions
  - additional clarification on certain responses or cyber/risk awareness education
  - mitigation actions based on data sensitivity and gaps in compliance
- HII will **NOT** be receiving/reviewing supplier SSPs or POAMs.
- HII will require all suppliers that will be handling CDI to complete all SC3RMP phases to obtain an acceptable risk assessment decision prior to execution of any POs within the scope of the DFARS 252.204-7012 clause
- **HII expects that annual certification of cybersecurity compliance will be required within the next 1-2 years**

Resources – Getting Help

- Additional Exostar resources are available in the links below:
  - http://www.myexostar.com/PIM
  - https://my.exostar.com/pages/viewpage.action?pageId=12125152
  - https://exostar.atlassian.net/wiki/spaces/EN8/overview
  - https://www.exostar.com/contract/nist800171/
- NIST 800-171 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
- DFARS 252.204-7012 - https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
- *Cybersecurity Evaluation Tool (CSET) - d*ownload at: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
- CMMC - https://www.acq.osd.mil/cmmc/index.html

QUESTIONS AND ANSWERS


Huntington
Ingalls
Industries
Hard Stuff Done Right ™