

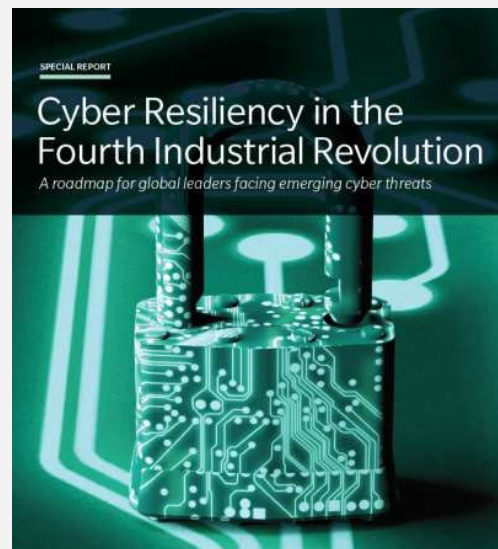
# DFARS 252.204-7012 -- SAFEGUARDING COVERED DEFENSE INFORMATION (CDI) AND CYBER INCIDENT REPORTING



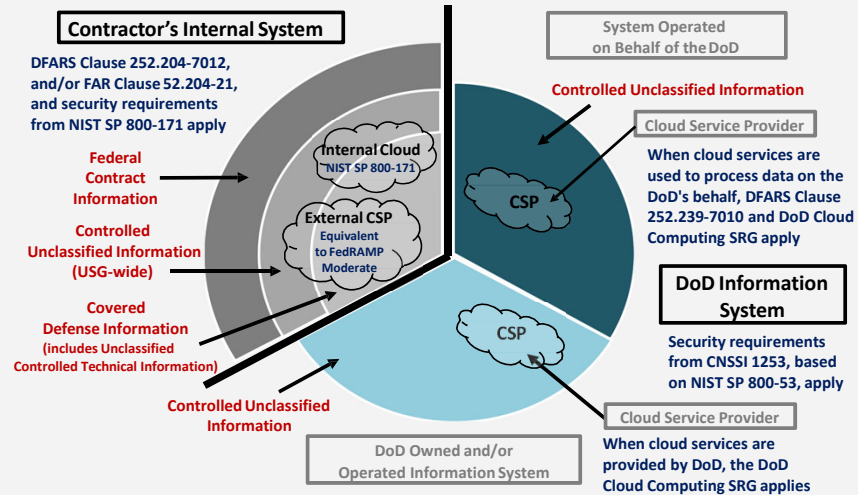
[www.DAU.mil](http://www.DAU.mil)

1

## DFARS CLAUSE OVERVIEW



# PROTECTING THE DOD'S UNCLASSIFIED INFORMATION



3

## DFARS CLAUSE 252.204-7012

- Requires the program office/requiring activity to:
  - Mark or otherwise identify in the contract, task order, or delivery order covered defense information provided to or developed by contractor by or on behalf of, DoD in support of the performance of the contract**
- Requires the contractor/subcontractor to:
  - Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network
  - 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
  - Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
  - Submit media/information as requested to support damage assessment activities
  - Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information

4

## WHAT IS THE PURPOSE OF DFARS CLAUSE 252.204-7012?

- Structured to ensure that:
  - Controlled unclassified DoD info residing on a contractor's internal info system is safeguarded from cyber incidents.
  - Any consequences associated with the loss of this info are assessed and minimized via the cyber incident reporting and damage assessment processes.
- Provides single DoD-wide approach to safeguarding contractor information systems
  - Prevent proliferation of multiple/potentially different safeguarding controlled unclassified information clauses, contract language by various entities across DoD.

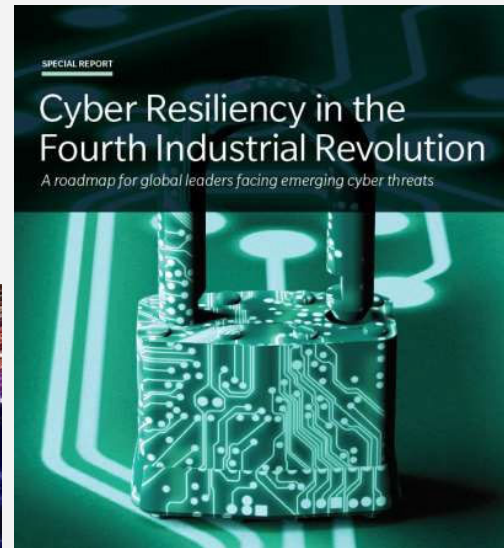
5

## CONTRACTOR COMPLIANCE — IMPLEMENTATION OF DFARS 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
- Contractor's responsibility to determine whether it has implemented NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)
  - The scope of DFARS Clause 252.205-7012 does not require DoD to 'certify' that a contractor is compliant with the NIST SP 800-171 security requirements
  - The scope of DFARS Clause 252.205-7012 does not require the contractor to obtain third party assessments or certifications of compliance
  - DoD does not recognize third party assessments/certifications of compliance
- Per NIST SP 800-171, 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 nonfederal organization

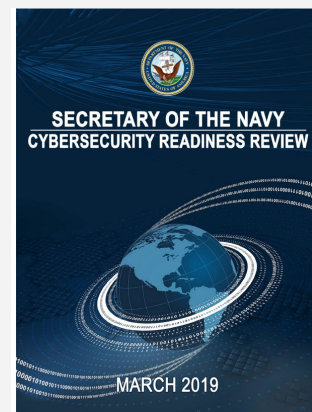
6

## WHY ARE WE HERE



## SECNAV'S CYBER READINESS REVIEW

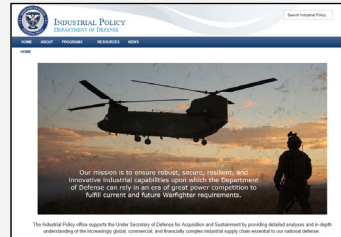
"To restate, the DON culture, processes, structure, and resources are ill-suited for this new era. The culture is characterized by a lack of understanding and appreciation of the threats, and inability to anticipate them, and a responsive checklist behavior that values compliance over outcomes, antiquated processes and governance structures that are late to respond to dynamic threats, and an enterprise whose resources are consumed by force structure and platforms that deprive the information systems and capabilities required for warfighting and defense in this environment."



## OBSERVATIONS

### Small and Medium Sized Manufacturers:

- Are not adequately incentivized to implement the 109 security requirements of the NIST SP 800-171 Rev 1 for the protection of CDI on their contractor networks
- There will be cost for implementation of these 109 security requirements. They don't believe DoD fully appreciates the magnitude of their effort. Industry is struggling with how to best fold these costs into their pricing strategy or receive reimbursement for their costs.
- While they have basic security knowledge, on-going operations for detection and response continues to be a more foreboding challenge.
- Flow down of security requirements to the subs and vendors is a huge issue for the entire industrial base.



9

## STATISTICS

This report analyzes data compiled from two years of compliance assessments to identify areas where defense contractors typically fall short in implementing DFARS 252.204-7012 and the associated NIST 800-171 requirements.

### **KEY FINDINGS:** Of the companies assessed (averages):

- Zero companies were 100% compliant.
- Companies implemented only 39% of the controls.
- Large companies successfully implemented nearly 60% of the controls.
- Small to mid-sized companies successfully implemented 34% of the controls.
- 61% of the controls were either not implemented or only partially implemented.
- Over 80% of companies assessed failed to implement 16 specific controls.



<https://sera-brynn.com/press-release-report-on-defense-industry-implementation-of-nist-800-171-security-controls-is-now-out/>

10

## LEARNING OBJECTIONS

- Differentiate CDI/CTI/CUI terminology to implement into applicable product and/or service contract
- Determine level of protection based on threat
- Evaluate security control implementation to meet CDI adequate security requirements
- Evaluate incident response policy and plan
- Ensure documentation availability for audits and compliancy

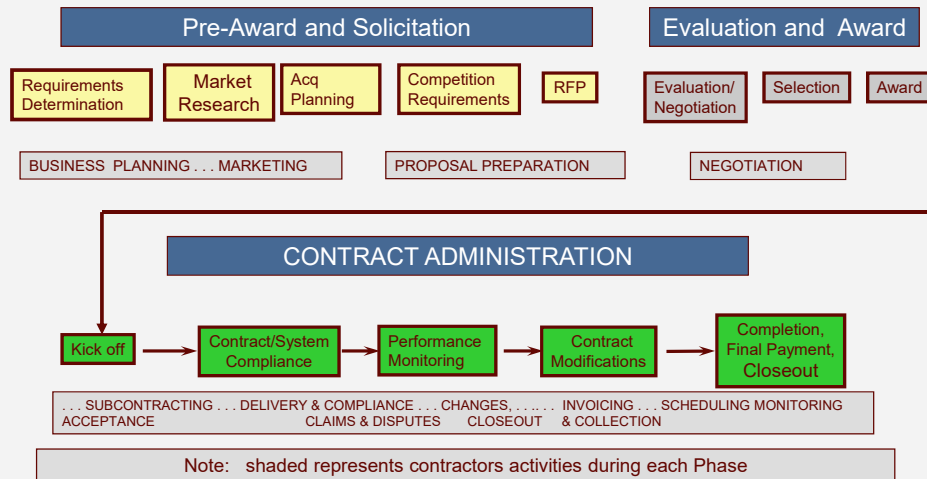
11

## BEHAVIORS

- Differentiate CDI/CTI/CUI terminology and correctly implement into applicable product and/or service procurement request
- Determine CDI level of protection based on threat
- Evaluate security control implementation to meet CDI adequate security requirements
- Evaluate incident response policy and plan

12

# THE CONTRACTING PROCESS



13

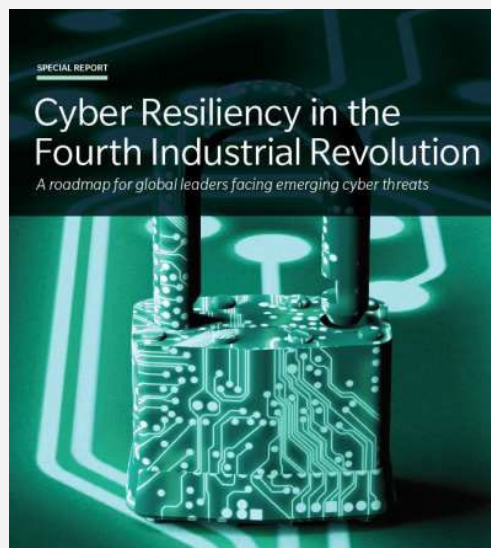
## OBJECTIVE OUTCOMES (1)

Successfully implement DFARS clause 252.204-7012 on current and future procurements that:

- Safeguard CDI that resides on or is transiting through a contractor/subcontractor internal information system or network, and
- Report cyber incidents that affect the contractor/subcontractor ability to perform requirements designated as operationally critical

14

## DEFINING THE TERMS



## COVERED DEFENSE INFORMATION

**Covered Defense Information**—Term used to identify information that requires protection under DFARS Clause 252.204-7012

- Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry,<sup>1</sup> 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<sup>2</sup>

<sup>1</sup> Referenced only to point to information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, government-wide policies.

<sup>2</sup> "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.



## CTI DEFINITION

Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

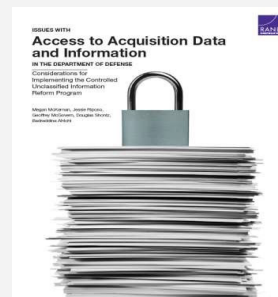
Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.” (NARA, 2017)

17

## CUI DEFINITION

The CUI Program covers any information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that is required to be protected under law, regulation, or Government-wide policy. This information does not include:

- Classified information
- Information a non-executive branch entity possesses or maintains in its own systems that did not come from
- Created or possessed by or for, an executive branch agency or an entity acting for an agency

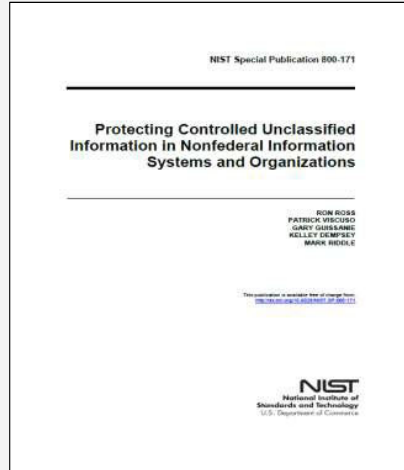


18

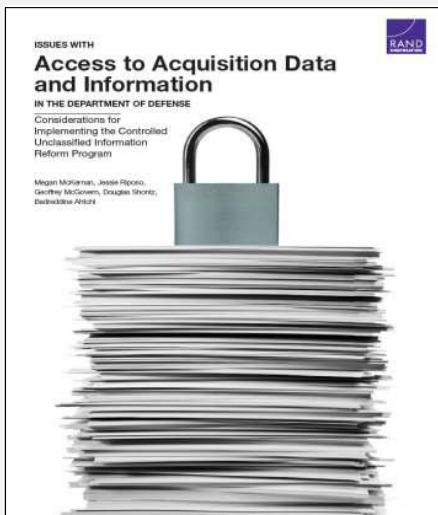
# PROTECTING CUI

**NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations**  
(Revision 1, December 2016)

- Recommended requirements for protecting the confidentiality of CUI when:
  - CUI is resident in nonfederal information systems/ organizations
  - Information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies



# CUI HISTORY



## The 24 Approved CUI Categories

Agriculture	Legal
Controlled Technical Information	North Atlantic Treaty Organization
Critical Infrastructure	Natural and Cultural Resources
Emergency Management	Nuclear
Export Control	Patent
Financial	Privacy
Geodetic Product Information	Procurement and Acquisition
Immigration	Proprietary Business Information
Information Systems Vulnerability Information	SAFETY Act Information
International Agreements	Statistical
Intelligence	Tax
Law Enforcement	Transportation

SOURCE: NARA, "CUI Registry—Categories and Subcategories," webpage, last reviewed November 15, 2017.

(p. 11)

**Note:** There are 24 NARA CUI Categories – the DFARS clause Subpart 204.73 covers CDI instantiated as either Unclassified CTI or Other Information

# NEW CUI LABELS

**Table S.2**  
Legacy DoD Labels and New NARA CUI Labels

Legacy DoD Labels	NARA Compliant?	Potential Action Required
Business Sensitive	NO	Can no longer be used; New label could be PROPIN, Procurement and Acquisition (PROCURE), or Proprietary Business Information–Manufacturer (MFC)
Competition Sensitive	NO	Can no longer be used; Could be PROPIN, PROCURE, or MFC
For Official Use Only (FOUO)	NO	<del>Can no longer be used</del> ; likely switches to CUI Basic (unless covered by specific regulation)
Pre-Decisional	NO	Can no longer be used as a banner marking or portion marking <sup>3</sup>
Proprietary Information (PROPIN)	ALMOST	Must determine whether CUI Basic or CUI Specified label applies
Source Selection Sensitive	ALMOST	New label is likely CUI–SP/SSEL
Technical Distribution Statement (TDS)	ALMOST	TDSs are now called Limited Dissemination Control Markings (LDCMs) and are required in addition to CUI banner markings for some types of CUI

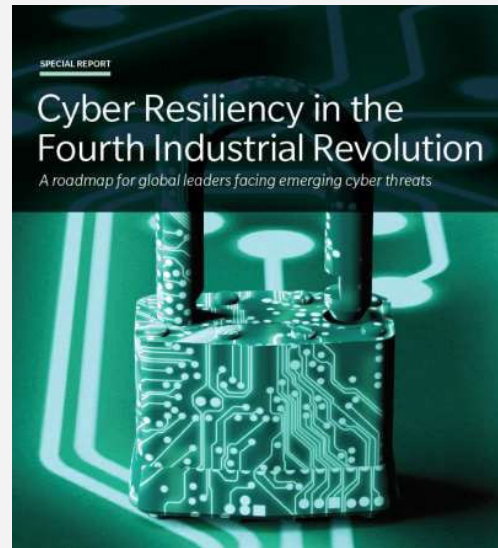
Several commonly used labels on acquisition information are ~~no longer~~ permitted, which will leave DoD employees and contractors looking for the next “FOUO.”

CUI includes personally identifiable information; proprietary business information; and law enforcement investigations, among others.

21

FOUO continues to be a valid marking within DoD. Do not begin using CUI markings until you are instructed to do so.

## LEVEL OF PROTECTION: ADEQUATE SECURITY (PART 1)



## OMB A-130: MANAGING INFORMATION AS A STRATEGIC RESOURCE

'Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

23

## THREAT CONCERNS

### Core Questions:

- What is the potential loss from a successful attack?
- What is the likelihood?
- What is the tolerance for such a loss?
- What is the strategy to mitigate or manage this loss?

24

## NIST SP 800-53 & NIST SP 800-171

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4, April 2013)	NIST SP 800-171, Protecting CUI in Nonfederal Systems and Organizations (Revision 1, December 2016)
<ul style="list-style-type: none"> <li>• Catalog of security and privacy controls for <u>federal information systems and organizations</u> to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors</li> </ul>	<ul style="list-style-type: none"> <li>• Recommended requirements for protecting the confidentiality of CUI when:               <ul style="list-style-type: none"> <li>– CUI is resident in <u>nonfederal information systems/ organizations</u></li> <li>– Information systems where the CUI resides are <u>not used or operated by contractors of federal agencies or other organizations on behalf of those agencies</u></li> </ul> </li> </ul>

25

## 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 to implement the requirements**

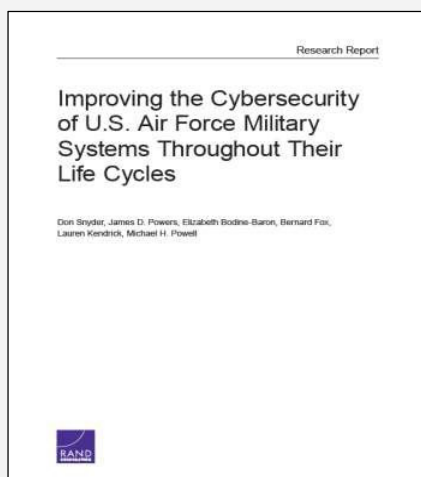
26

## ALTERNATIVE BUT EQUALLY EFFECTIVE SECURITY MEASURES

- If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, 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
- When DoD CIO receives a request from a contracting officer, representatives in DoD CIO review the request to determine if the proposed alternative satisfies the security requirement, or if the requirement for non-applicability is acceptable:
  - Documented and provided to the contracting officer, generally within 5 working days
  - Favorably adjudicated, the assessment should be included in the contractor's system security plan

27

## POOR DESIGN/SYSTEMS ENGINEERING

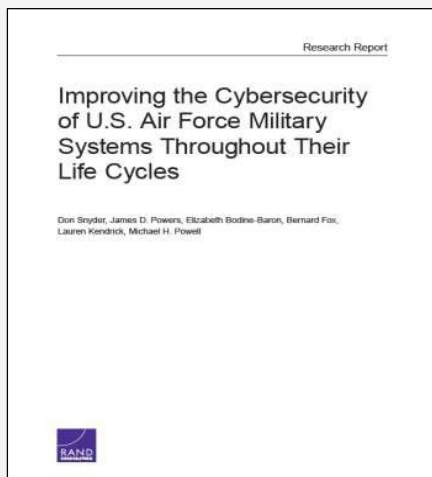


“Poor system security engineering is very difficult to mitigate by overlaying security controls, whereas security controls overlaid on a sound, secure design can be quite effective. For systems that are fielded and no longer in production, design changes to improve cybersecurity generally necessitate a modification program and can be cost-prohibitive. It is especially important in this phase that a mission assurance perspective be adopted that examines the full spectrum of options for cybersecurity, including after-design protective measures, changes in operational procedures, and modifications, if necessary and affordable.” (Rand, p. 8)

[https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1000/RR1007/RAND\\_RR1007.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf)

28

## HOW MUCH IS ENOUGH

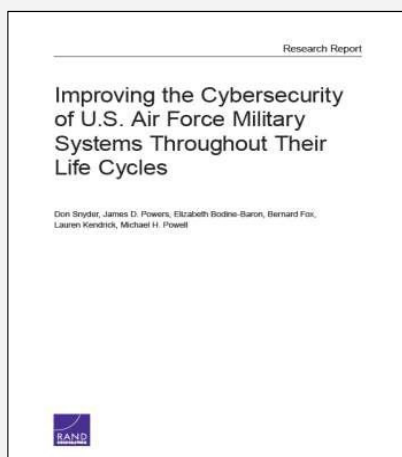


[https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1000/RR1007/RAND\\_RR1007.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf)

Imbalance between the offense and defense in the cyber domain implies that it is unwise to assume that complete cybersecurity can be achieved. Some potential vulnerabilities that can be exploited or attacked will always persist. The goals of counter cyber exploitation are, for example, controlling critical information by identifying it, restricting access to it, and preventing its theft. It is not possible to reduce the amount of critical information to zero. Nor does it appear safe to assume that access can be unequivocally denied. The question is how much security is enough given finite resources and mission needs. (p 7)

29

## FUNCTIONALITY SECURITY TRADES

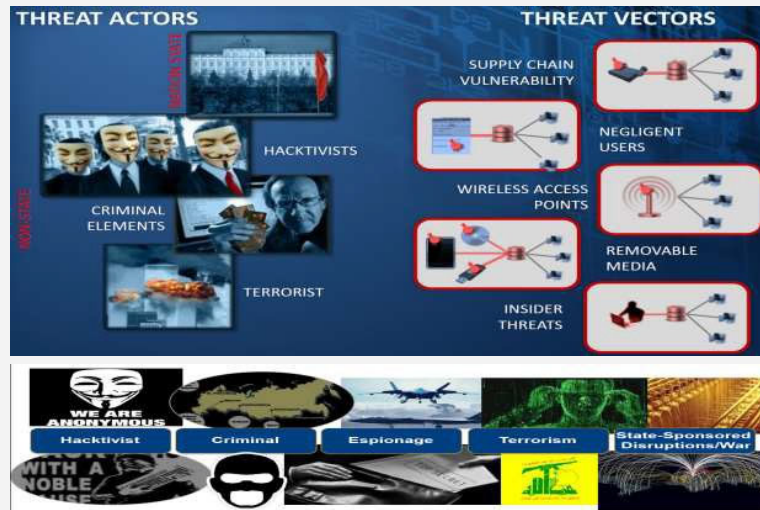


[https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1000/RR1007/RAND\\_RR1007.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf)

Functionality and cybersecurity are intertwined. Quite a number of cyber vulnerabilities are the result of features deliberately designed into systems. That is not to say that engineers aim to make vulnerable systems, but during design, engineers make trades between functionality and security and are willing to accept certain levels of vulnerabilities in order to achieve some functionality, often knowingly, and sometimes unknowingly ... Much of the commercial world is so driven by introducing new functionality that security is a lesser priority, and, when addressed, security is introduced by overlays on an insecure design rather than by an inherently secure design. (p. 6)

30

## UNDERSTAND DIFFERENT CYBERSECURITY THREATS



31

## QUESTIONS TO ASK

- At what cybersecurity threat/tier level is the contractor or sub protecting against?
- Is this identified in the contract?

32



## QUESTIONS TO ASK

- Did the contractor or sub request threat or intelligence information?
- Should this be covered under a DD Form 254?

33

## TYPES OF THREATS

- External Attacker
- Insider Threat
- Supply Chain Risk

34

## THREAT

### Cyber Threat

- Destruction
- Disclosure
- Denial of Service
- Modification of Information
- Unauthorized Access



**The cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).**

The global cost of cybercrime continues to increase, this isn't a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

<https://securityaffairs.co/wordpress/category/cyber-crime>

35

## WAYS TO BE ATTACKED

- Via external boundaries to include encryption & authentication
- Exploiting software vulnerabilities (such as buffer overflow)
- Using interfaces & communication between components in an unintended way
- Misusing authorizations

36

## UNDERSTANDING THREAT

- Assists with requirements development
- Is an input to numerous acquisition documents (e.g. Program Protection Plan, Cybersecurity Strategy, etc..)
- Assists with understanding consequence(s)
- Can be used in modeling & simulation for tradeoffs

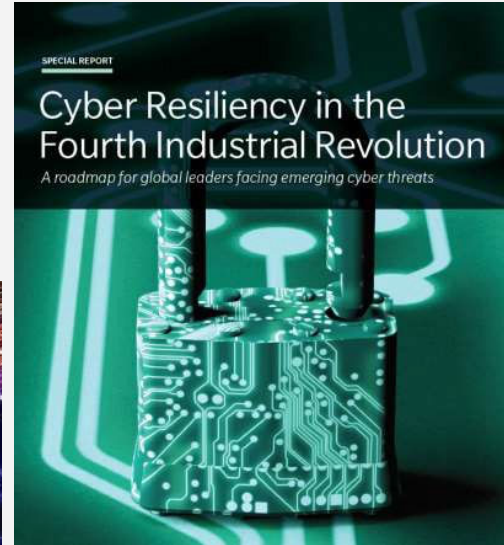
37

## THREAT SUMMARY

- Cyber threat is real & growing
- Purpose of warning about cyber threats is not to scare or cause despair, but change behavior
- Understanding threat is critical for critical thinking & better risk management
- Cyber threat is co-evolving & dynamic, we need you to be the same

38

## THE NEXT STEP



## OBJECTIVE OUTCOMES (2)

- Evaluate & Monitor the Security of Sensitive Information
- Manage Cyber Risk not just Compliance
- Partner with the Workforce (Industry/ Government)

## STRATEGIES TO ENHANCE CYBERSECURITY MEASURES PROVIDED BY DFARS 252.204-7012 & NIST SP 800-171

- DPC Memo (Nov 6, 2018), Subject: Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012
  - Provides acquisition personnel with framework of tailorable actions to assess the contractor's approach to protecting DoD CUI
  - Provides guidance for reviewing system security plans and any NIST SP 800-171 security requirements not yet implemented
  - Includes sample Contract Data Requirements Lists (CDRLs) and associated Data Item Descriptions (DIDs)
- ASD(A&S) Memo (Dec 17, 2018), Subject: Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base
  - Provides program offices and requiring activities with sample Statement of Work (SOW) language to be used in conjunction with DPC guidance
  - Addresses access to/delivery of the contractor's system security plan, access to/delivery of the contractor's plan to track flow down of DoD CUI and plan to assess of compliance of Tier 1 Level suppliers

41

## STRATEGIES TO ENHANCE CYBERSECURITY MEASURES PROVIDED BY DFARS 252.204-7012 & NIST SP 800-171

### USD(A&S) Memo (Jan 21, 2019), Subject: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review


- DCMA will leverage review of contractor purchasing systems in accordance with DFARS Clause 252.244-7001, Contractor Purchasing System Administration, to:
  - Review contractor procedures to ensure contractual requirements for identifying/ marking DoD CUI flow down appropriately to their Tier 1 Level Suppliers
  - Review contractor procedures to assess compliance of Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171

### USD(A&S) Memo (Feb 5, 2019), Subject: Strategically Implementing Cybersecurity Contract Clauses


- DCMA will apply a standard DoD CIO methodology to recognize industry cybersecurity readiness at a strategic level.
- DCMA will pursue, at a corporate level, the bilateral modification of contracts administered by DCMA to strategically (i.e., not contract-by-contract) obtain/assess contractor system security plans

See DPC Website at [https://www.acq.osd.mil/dpap/pdi/cyber/guidance\\_for\\_assessing\\_compliance\\_and\\_enhancing\\_protections.html](https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html)

42




## Cybersecurity Maturity Model Certification (CMMC)




---

- The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.
- The new standard and maturity model will be named Cybersecurity Maturity Model Certification (CMMC)
- The CMMC levels will range from basic hygiene to “State-of-the-Art” and will also capture both security control and the institutionalization of processes that enhance cybersecurity for DIB companies.
- The required CMMC level (notionally between 1 – 5) for a specific contract will be contained in the RFP sections L & M, and will be a “go/no-godecision”.
- The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.
- The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.
- The CMMC will include a center for cybersecurity education and training.
- The CMMC will include the development and deployment of a tool that 3rd party cybersecurity certifiers will use to conduct audits, collect metrics, and inform risk mitigation for the entire supply chain.

4

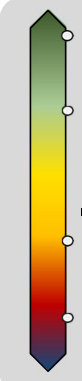


## DIB Cybersecurity Posture



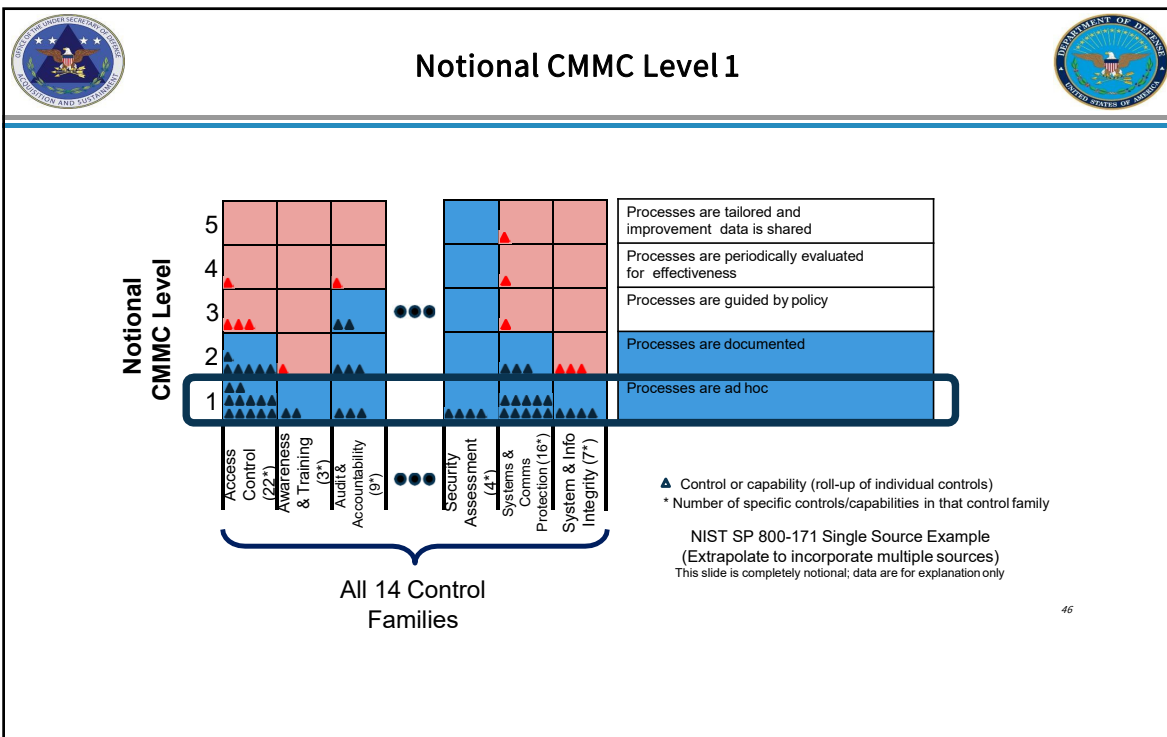
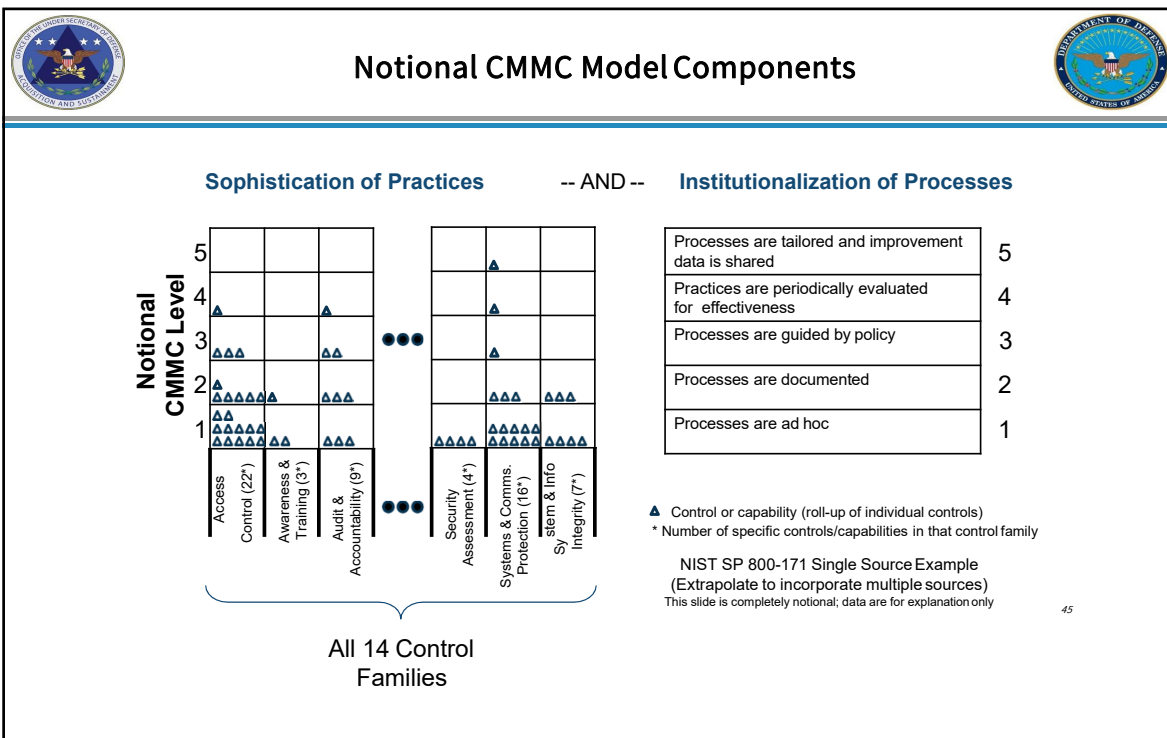
---

Hypothesis:  
< 1% of DIB companies



- **State-of-the-Art**
  - Maneuver, Automation, SecDevOps
- **Nation-state**
  - Resourcing: Infosec dedicated full-time staff ≥ 4, Infosec ≥ 10% IT budget
  - Sophisticated TTPs: Hunt, white listing, limited Internet access, air-gapped segments
  - Culture: Operations-impacting InfoSec authority, staff training and test
- **Good cyber hygiene**
  - NIST SP 800-171 compliant, etc.
  - Consistently defends against Tier I-II attacks
- **Ad hoc**
  - Inconsistent cyber hygiene practices
  - Low-level attacks succeed consistently

Vast majority of DIB companies →





## Industry Days / Listening Sessions



We are looking at 12 collaborative sessions across the country and we want to ensure, we give all an equal voice for participation.

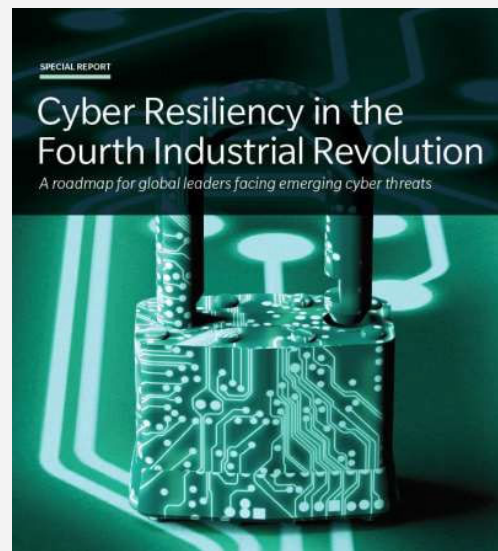
Time Frame: July – Aug 2019

Locations:

- San Diego, CA
- San Antonio, TX
- Huntsville, AL
- Tampa, FL
- Boston, MA
- Washington D.C.
- Phoenix, AZ
- Detroit, MI
- Colorado Springs, CO
- Seattle, WA
- Kansas City, KA

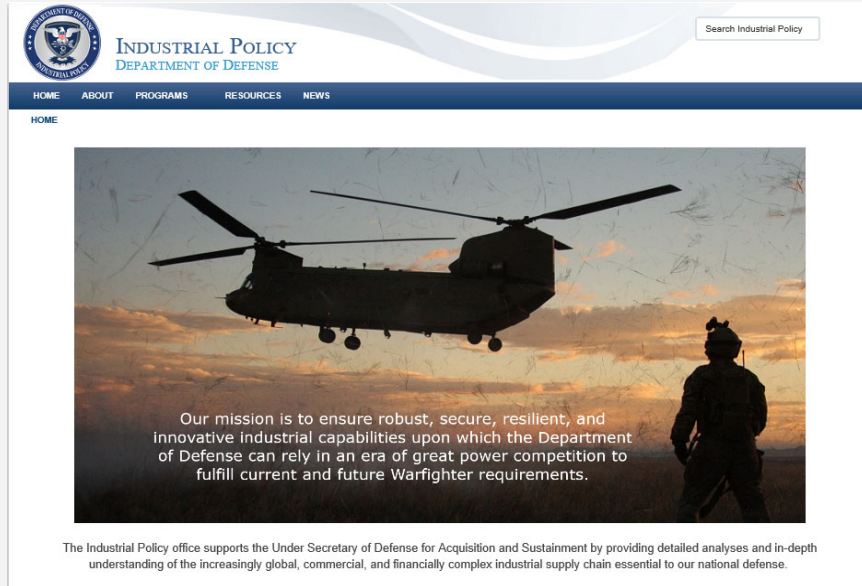
47

## SUMMARY





# MANUFACTURING & INDUSTRIAL BASE POLICY



INDUSTRIAL POLICY  
DEPARTMENT OF DEFENSE

Search Industrial Policy

HOME ABOUT PROGRAMS RESOURCES NEWS

HOME

Our mission is to ensure robust, secure, resilient, and innovative industrial capabilities upon which the Department of Defense can rely in an era of great power competition to fulfill current and future Warfighter requirements.

The Industrial Policy office supports the Under Secretary of Defense for Acquisition and Sustainment by providing detailed analyses and in-depth understanding of the increasingly global, commercial, and financially complex industrial supply chain essential to our national defense.

49

# Questions?