



# 2020

---

**Missile Defense Agency**  
**Office of Small Business Programs**  
**Virtual Conference**

# Protecting DoD CUI in Nonfederal Systems

## Cybersecurity and Compliance



## MDA Small Business Conference Participants

**Ms. Diane Knight**  
**Dr. Mike Wojcik**

**Missile Defense Agency**  
**May 13, 2020**

DISTRIBUTION STATEMENT A.  
Approved for public release; distribution  
is unlimited.



# Missile Defense Evolving Threat Environment

Adversaries are fielding diverse and expansive ranges of modern offensive missile systems

- Developing new missiles & improving existing systems
  - Precision strike
  - Penetration aids (e.g. decoys, jamming devices)
- Capable of maneuvering in midcourse or terminal phase
  - Maneuvering Reentry Vehicle (MaRV)
  - Multiple Independent Reentry Vehicle (MIRV)
  - Hypersonic glide vehicles and cruise missiles



North Korea  
Hwasong-15 ICBM



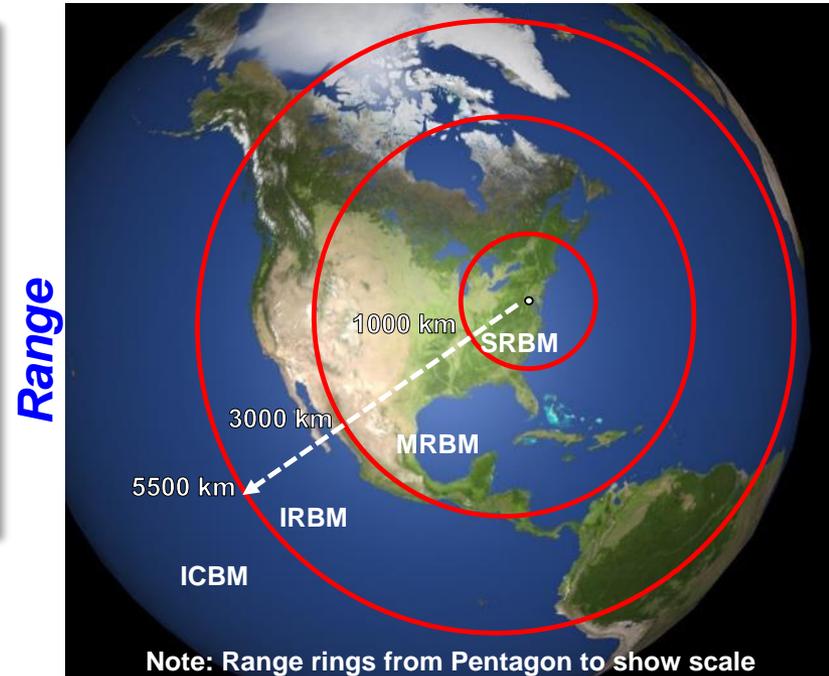
Iran  
Emad-1 MRBM with MaRV



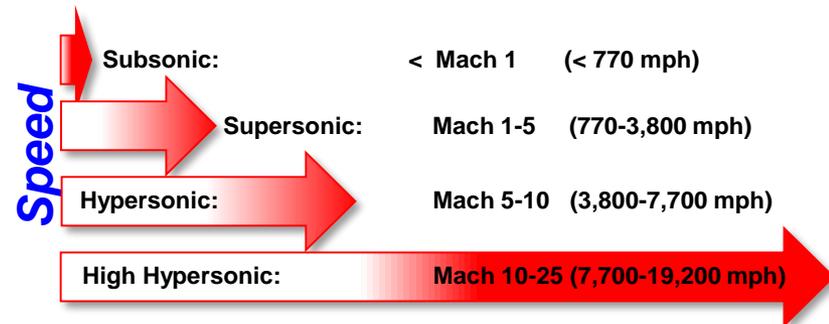
China  
Dong Feng (DF-26) IRBM



Russia  
Concept Hypersonic Glide Vehicle



SRBM: Short Range Ballistic Missile	(300-1000 km :: 621 mi)
MRBM: Medium Range Ballistic Missile	(1000-3000 km :: 1864 mi)
IRBM: Intermediate Range Ballistic Missile	(3000-5500 km :: 3418 mi)
ICBM: Intercontinental Ballistic Missile	(5500+ km :: 3418+ mi)





# Missile Defense Agency Mission

To develop and deploy a **layered** Missile Defense System to **defend** the United States, its deployed forces, allies, and friends from missile attacks in **all phases** of flight

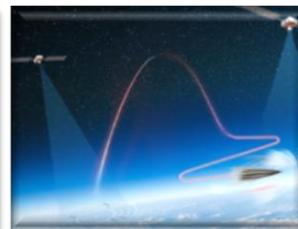


**Missile Defense Capability  
Globally Deployed**



# Missile Defense Agency Lines of Effort In Support Of The National Defense Strategy

- Build **Warfighter confidence** through focus on **readiness and sustainment**
- Increase engagement **capability and capacity** to outpace emerging threats
- Increase **speed of delivery** of new capability to address the **evolving threat**



*“A robust and credible layered missile defense system paired with our conventional and nuclear force capabilities provides the ability to deter strategic attacks, deny benefits, and impose costs against any potential adversary.”*

*-- Admiral Charles A. Richard, U.S. Strategic Command*



# Today's Layered Active Missile Defense System

**C2BMC** Command and Control, Battle Management and Communications

NMCC

USSTRATCOM

USNORTHCOM

USINDOPACOM

USEUCOM

USCENTCOM

**BOOST**  
Defense Segment

**ASCENT/MIDCOURSE**  
Defense Segment

**TERMINAL**  
Defense Segment

**The System  
Of Elements**

**GBI**  
Ground-Based  
Interceptor

**SM-3 IIA**  
Standard  
Missile

**SM-3 IA/IB**  
Standard  
Missile

**THAAD**  
Terminal High  
Altitude Area  
Defense

**SM-6**  
Standard  
Missile

**GMD**  
Ground-based  
Midcourse  
Defense

**Aegis  
Ship & Ashore**  
Ballistic Missile  
Defense

**Aegis  
Sea-Based  
Terminal**

**PAC-3**  
Patriot Advanced  
Capability

**Sensors**



Satellite Surveillance  
BMDS OPIR Architecture



Upgraded Early  
Warning Radars



Forward-Based  
Radars



AEGIS BMD  
SPY Radars



Discriminating  
Radars



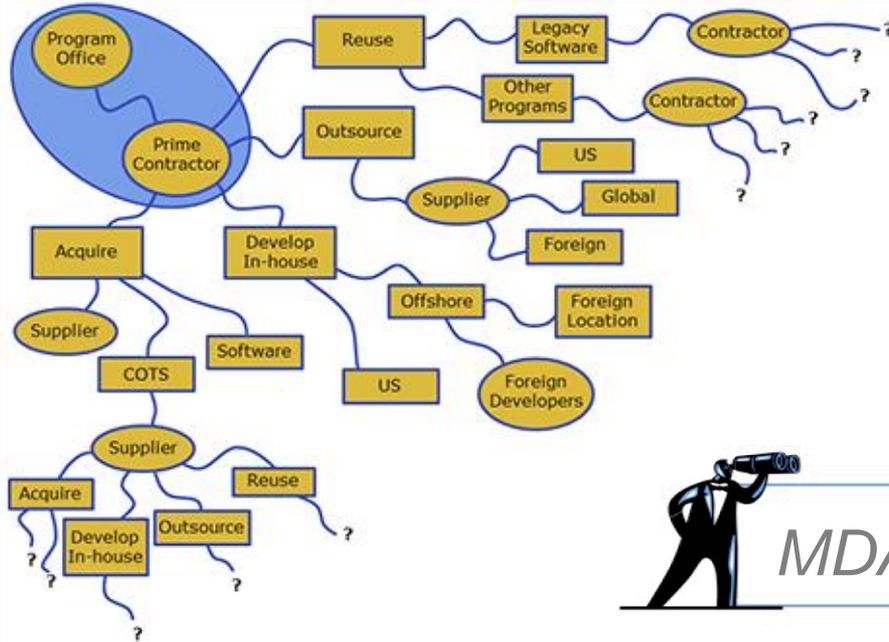
# Cybersecurity



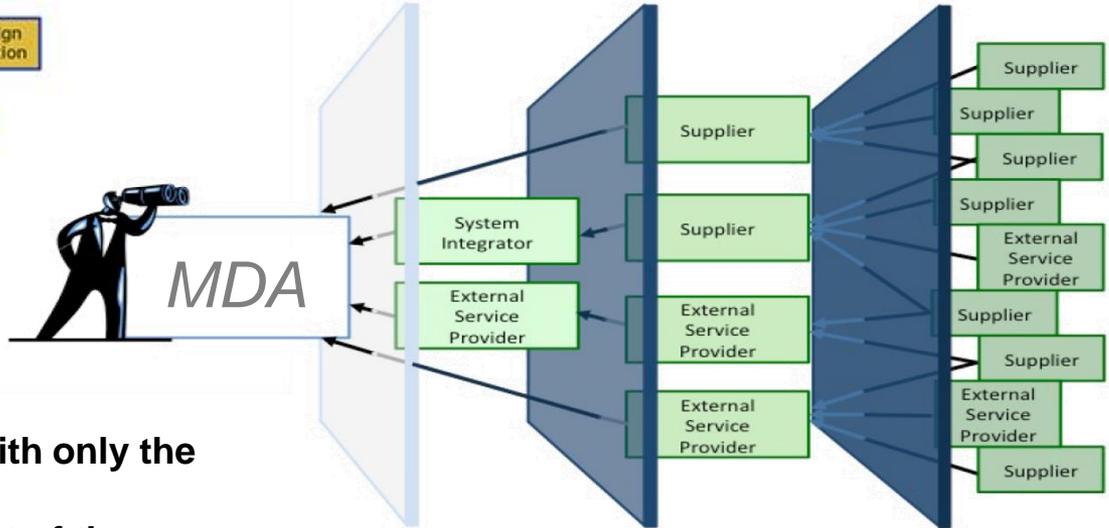
**What is Cybersecurity?** - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, **including information contained therein**, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoDI 8500.01)



# Increasingly Complex Supply Chain



Today's supply chains consist of a prime integrator and hundreds of global suppliers/developers providing custom and commercial-off-the-shelf (COTS) parts



Reduced Visibility, Understanding and Control

NIST Special Publication 800-161, SCRM, April 2015

## Government:

- Has a contractual relationship with only the prime contractor
- Has limited knowledge of the rest of the supply chain (perhaps only two or three levels down)

**Supply Chain Visibility Reduced at Lower Tiers**



# Without a Secure Foundation All Functions are at Risk

Cost, Schedule, and Performance

are only effective in a **SECURE ENVIRONMENT**





# Top MDA Cyber Focus Areas

- **Audit Missile Defense System (MDS) subsystems for cybersecurity vulnerabilities**
  - Address the advanced cyber threat at the MDS & Subsystem level
    - Manage the pace of testing to meet demand
    - Identify and budget cyber resources needed to test against evolving threats
    - Planning and programming for future complex MDS tests
- **Determining MDS Mission Risk**
  - Impact (i.e., consequence/severity) if threat actor were to exploit platform vulnerabilities with the intent to degrade the MDS mission
  - Likelihood threat actor can gain access to a MDS platform sufficient to execute an attack that impacts the MDS mission
- **Defense Industrial Base (DIB) Cybersecurity and Supply Chain Illumination**





# What DoD is Doing

- **DoD is participating in a range of activities to improve the collective cybersecurity of the nation and protect U.S. interests:**
  - Leveraging National Institute of Standards and Technology (NIST) information security standards and guidelines for federal and nonfederal information systems
  - Implementing contractual requirements to secure contractor systems and networks through the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS)
  - Promoting cyber threat awareness through information sharing opportunities
- **Implementing DoD-wide Cybersecurity Assessments and Standards**
  - Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) lead assessments of contractor systems/networks (in-progress)
  - Cybersecurity Maturity Model Certification (CMMC) assessments (over next 3-5 years)
  - CMMC v1.0, January 30, 2020: <https://www.acq.osd.mil/cmmc/>



# Stakeholders - Protecting the DoD's Unclassified Information

<b>Department of Defense</b>	
<b>DoD CIO</b> <ul style="list-style-type: none"> <li>• Cybersecurity</li> <li>• DoD Cyber Crime Center (DC3)</li> </ul>	<b>OUSD(R&amp;E)</b> <ul style="list-style-type: none"> <li>• Strategic Technology, Protection, &amp; Exploitation</li> <li>• Joint Acquisition, Protection, &amp; Exploitation Cell (JAPEC) and Damage Assessment Office (DAMO)</li> </ul>
<b>OUSD(A&amp;S)</b> <ul style="list-style-type: none"> <li>• Defense Pricing &amp; Contracting (DPC)</li> <li>• Defense Contract Management Agency (DCMA)</li> </ul>	<b>DoD Components</b> <ul style="list-style-type: none"> <li>• Program Office/Requiring Activity</li> <li>• Damage Assessment Offices (DAMOs)</li> <li>• CISOs/CIOs/IT Security Specialists</li> </ul>
<b>General Counsel</b>	<b>OUSD(I)</b> <ul style="list-style-type: none"> <li>• Defense Security Service (DSS)</li> </ul>

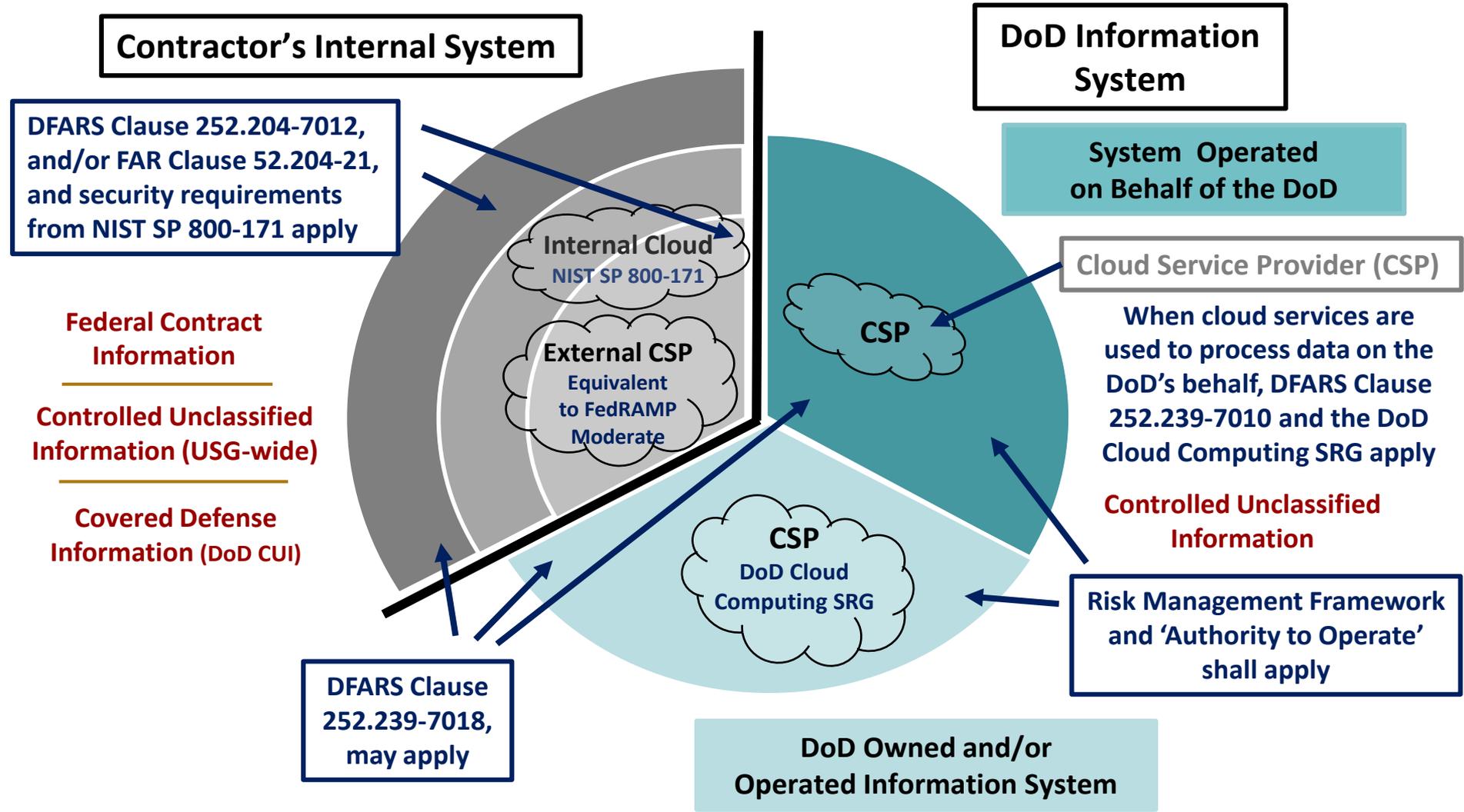
<b>Industry</b>
• Chief Information Security Officers (CISOs)
• Information Technology (IT) Security Specialists
• Contracting
• Facility Security Specialists
• Counsel
• Project Managers

### Acronyms

- DoD CIO – Department of Defense Chief Information Officer
- OUSD(A&S) - Office of the Under Secretary of Defense for Acquisition and Sustainment
- OUSD(R&E) - Office of the Under Secretary of Defense for Research and Engineering
- OUSD(I) - Office of the Under Secretary of Defense for Intelligence and Security



# Protecting the DoD's Unclassified Information





# Safeguarding MDS Information

G  
O  
V

## Unclassified Information

**-- MDA NIPRNET --**

**Information Protection**

DoD 5200.01 Vol 4 (DE/I)

**Information Systems Protection**

DoD 8500.01 / NIST 800-53 (MDA/IC)

**Certification & Accreditation**

DoD 8510 Risk Management Framework (MDA/IC)

D  
I  
B

**-- DIB UNCLASSIFIED NETWORKS --**

*Cyber ESG IPT Focus*

**Information Protection**

DoD 5200.01 Vol 4 (MDA/EIR)

**Information Systems Protection**

NIST 800-171r1 (DFARS 7012)

**Certification & Accreditation**

N/A (Self-Certification)

M  
D  
S

*Aegis BMD – US Navy*  
*C2BMC – MDA*  
*GMD – MDA /NORTHCOM*  
*SN - MDA*  
*THAAD – US Army*

## MDS (Mission) Systems

**Information Protection**

DoD 5200.01 Vol 4 (MDA/EIR)

**Information Systems Protection**

DoD 8500.01 / NIST 800-53

**Certification & Accreditation**

Risk Management Framework

*PATRIOT – US Army*  
*SBIRS – USAF*  
*UEWR – USAF*  
*CD - USAF*

## Classified Information

**-- MDA SIPRNET --**

**Information Protection**

DoD 5200.01 Vol 3 (MDA/EIR)

**Information Systems Protection**

DoD 8500.01 / NIST 800-53 (MDA/IC)

**Certification & Accreditation**

Risk Management Framework (MDA/IC)

**-- DIB CLASSIFIED NETWORKS --**

**Information Protection**

DoD 5220.22 (Defense Security Service)

**Information Systems Protection**

DoD 5220.22 Chapter 8 (Defense Security Service)

**Certification & Accreditation**

DoD 5220.22 Chapter 8 (Defense Security Service)



# Security Related Contractual Requirements in the FAR & DFARS

- **Implementing contractual requirements through the FAR and DFARS:**

- FAR Clause 52.204-2, Security Requirements (classified information)
- FAR Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
- FAR Clause 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
- DFARS Provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls
- **DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**
- DFARS Clause 252.239-7010, Cloud Computing Services
- DFARS Clause 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System
- DFARS Clauses 252.246-7008, Sources of Electronic Parts
- DFARS 252.239-7018, Supply Chain Risk

Systems  
Owned/Operated  
by the Government

Systems  
Owned/Operated  
by the Contractor



# DFARS Clause 252.204-7012 (Dec 2019) - Requirements

## Requires the contractor/subcontractor 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. **Submit media/information** as requested to support damage assessment activities
5. **Flow down the clause in subcontracts** for operationally critical support, or for which subcontract performance will involve *covered defense information*

**If a contractor does not agree or is unable to comply with the terms of DFARS Clause 252.204-7012, then controlled unclassified information (CUI) shall not reside on the contractor's information system**



# Adequate Security to Safeguard 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 how the contractor shall protect covered defense information. The requirement to protect it is based in law, regulation, or Government wide policy.**



# NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

*Developed from FIPS 200 and NIST SP 800-53 guidance*



*Align with standard industry 'best practices' for Cybersecurity*

- ✓ Access Control
  - ✓ Awareness and Training
  - ✓ Audit and Accountability
  - ✓ Configuration Management
  - ✓ Identification and Authentication
  - ✓ Incident Response
    - ✓ Maintenance
    - ✓ Media Protection
    - ✓ Personnel Security
  - ✓ Physical Protection
  - ✓ Risk Assessment
  - ✓ Security Assessment
  - ✓ System and Communications Protection
- ✓ System and Information Integrity

*Tailored to eliminate uniquely Federal requirements*

**A System Security Plan (SSP) describes the security controls in place or planned for meeting the NIST 800-171 security requirements to safeguard DoD Information**



# Demonstrating Implementation of NIST SP 800-171

- **To document implementation companies should have a system security plan (SSP) in place and if required, an associated plan of action and milestones (POA&M):**
  - **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 (Plan of Action and Milestones)** 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



# DCMA DIB Cyber Assessments

- **USD(A&S) Policy Memoranda:**
  - 14 Nov 2019, *Assessing Contractor Implementation of Cybersecurity Requirements*
  - 5 Feb 2019, *Strategically Implementing Cybersecurity Contract Clauses*
  - 6 Nov 2018, *Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012*
  - 21 Sep 2017, *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*
- **FAR Clause 52.204-21** Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
- **DFARS Clause 252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)
- **NIST Special Publication 800-171**, *Protecting CUI in Nonfederal Systems and Organizations*
- **NIST Special Publication 800-171A**, *Assessing Security Requirements for Controlled Unclassified Information*



# DCMA DIB Cyber Assessments

- **The objective of the NIST SP 800-171 Compliance Assessment is to determine whether the contractor has implemented the NIST SP 800-171 security requirements**
- **Not intended as a value judgement about specific approaches to requirement implementation or an assessment of one solution compared to another**
  - Solutions that meet the requirements are acceptable
  - Scoring methodology is designed for an objective assessment of security requirements implemented and not yet implemented
- **Achievable scores range from 0 (no SSP) to 110 (all requirements met)**
- **Scores remain a matter of record until a subsequent assessment is performed**
  - Scores recorded in the DoD Supplier Performance Risk System (SPRS): <https://www.sprs.csd.disa.mil/>



# Cybersecurity Maturity Model Certification (CMMC)



- **OUSD(A&S) developed the CMMC framework in concert with DoD Stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research Development Centers (FFRDCs), and the Defense Industrial Base sector**
  - CMMC v1.0, January 30, 2020: <https://www.acq.osd.mil/cmmc/index.html>
  - The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust, but adds a verification component with respect to cybersecurity requirements
  - For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats
  - The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels
  - The plan is for certified independent 3rd party organizations to conduct audits and inform risk



# Cybersecurity Maturity Model Certification (CMMC)

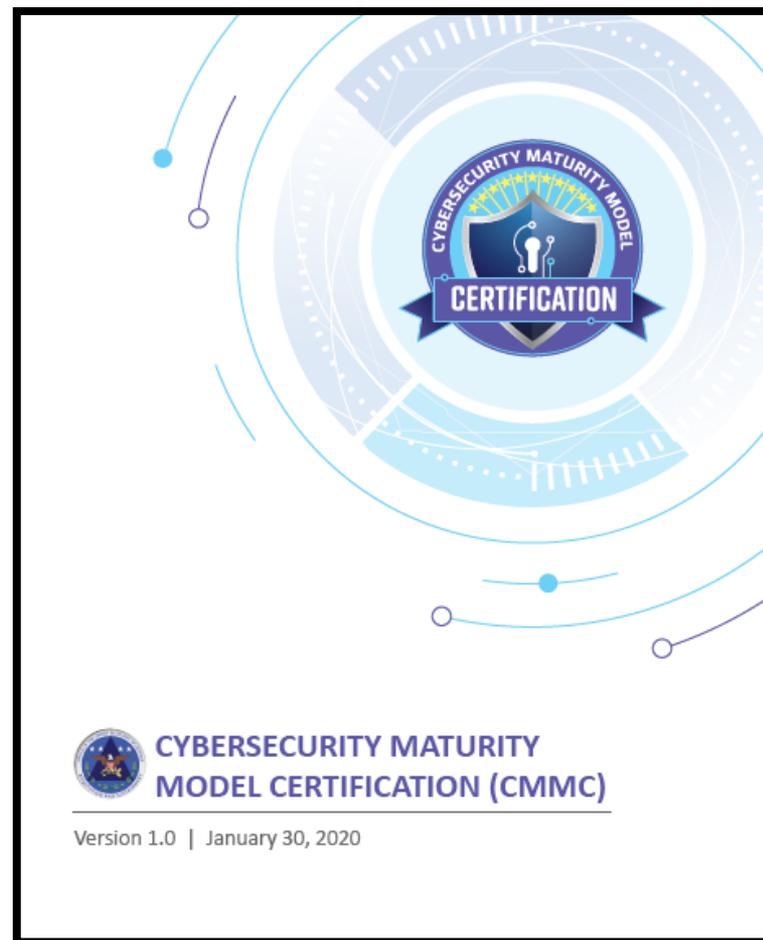


**CMMC is a DoD Certification process that measures a DIB sector company's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).**

**CMMC combines various cybersecurity standards and maps these best practices and processes to maturity levels, ranging from basic cyber hygiene to highly advanced practices.**

- **Level 5** | **Optimized Capabilities to Repel APTs**
- **Level 4** | **Substantial and Proactive**
- **Level 3** | **Good Cyber Hygiene**
- **Level 2** | **Intermediate Cyber Hygiene**
- **Level 1** | **Basic Cyber Hygiene**

**Cybersecurity must become a foundation of DoD Acquisition**





# CMMC Summary

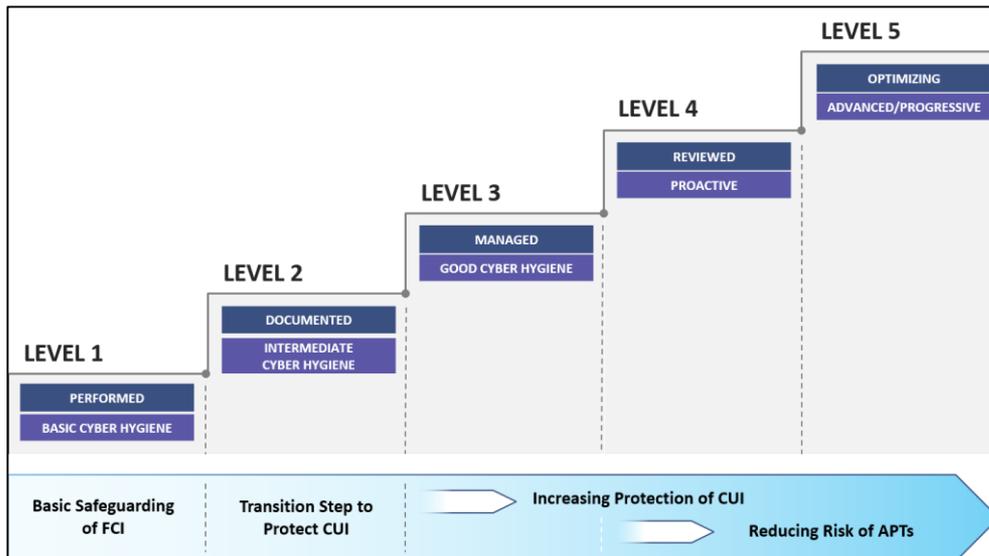


- **CMMC establishes cybersecurity as a foundation for future DoD acquisitions**
- **Levels align with the following focus:**

- Level 1: Basic safeguarding of Federal Contract Information (FCI)
- Level 2: Transition step to protect CUI
- Level 3: Protecting CUI
- Levels 4-5: Protecting CUI and reducing risk of Advanced Persistent Threats (APTs)

- **The CMMC model leverages multiple sources and references**

- Level 1 only addresses practices from FAR 52.204-21
- Level 3 includes all of the practices from NIST SP 800-171 Rev.1 as well as others
- Levels 4 and 5 incorporate a subset of the practices from draft NIST SP 800-171B plus others
- Additional sources, such as the UK Cyber Essentials and Australia Cyber Security Centre Essential Eight Maturity Model, were also considered and are referenced in the model





# What MDA is Doing to Enhance Cybersecurity

- **Ensuring Contractor Compliance of FAR clause 52.204-21 and DFARS clause 252.204-7012 to safeguard Controlled Unclassified Information (CUI) on non-federal systems**
- **Working with Industry Partners to promote cyber threat awareness through information sharing and collaboration**
- **Implementing the Information Management Control Plan (IMCP)**
  - *Addresses: Where is MDA CUI, and how is it protected?*
- **Executing joint MDA-DCMA DIB cyber assessment IAW NIST SP 800-171A**
- **Utilizing MDA Cyber Assistance Team (CAT)**
- **Piloting several efforts to assist with securing MDA CUI**
  - *Illuminating and providing visibility of CUI throughout the supply chain*
  - *Assisting partners in the development of SSPs and Plan of Action and Milestones*
- **Adding Cybersecurity provisions in the Source Selection process**
- **Adding evaluation of Cybersecurity operations into CPARS**
- **Adding Software Assurance in applicable MDA contracts**
- **Leading DoD pathfinder working to improve overall MDA cyber hygiene**



# MDA Information Management & Control Plan (IMCP)

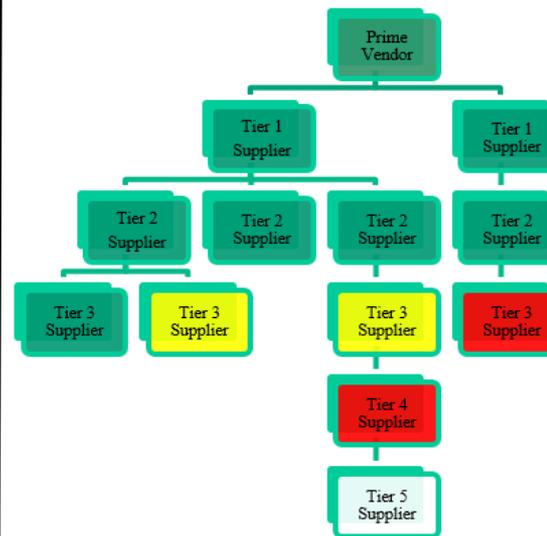
- Effective November 2019, MDA implemented the **IMCP** requirement for all new contracts as part of the statement of work or performance work statement
- The **IMCP** is a contract requirement that requires vendors to develop a plan and controls for information flow within their supply chain
- An acceptable IMCP is a **condition of contract award** and requires the Prime Contractor to:
  - Develop a plan to control the flow of CUI within the supply chain
  - Flow down IMCP to 1st tier subcontractors with requirement to continue to flow down to all tiers of the supply chain that utilize CUI
  - Demonstrate validation and enforcement of IMCP procedures by all members of the supply chain
- Requires Subcontractors to:
  - Submit Supplier Compliance Supplement directly to MDA and flow down that requirement to all subcontractors that utilize CUI
  - SSP and POA&M to Agency upon request
  - Follow IMCP procedures for flow of CUI within the supply chain



# MDA Information Management and Control Plan (IMCP)

- IMCP – Deliverable either at proposal submission or after contract award
- Requires vendor to:
  - Identify full supply chain where CUI is collected, developed, received, transmitted, used, or stored
  - Verify Flow down of DFARS 252.204-7012 to all applicable subcontractors
    - Implement practices to restrict unnecessary sharing and/or flow of CUI
  - Verify NIST SP 800-171 Compliance
  - Verify and monitor information safeguarding procedures throughout the supply chain
    - Provide system scans and monitoring reports
- Evaluate IMCP - Assess risk based upon DFARS 7012 implementation
- Vendors having high to moderate risk ratings, and/or failing to have DFARS 252.204-7012 included in their subcontract, will have priority for any voluntary CAT visits
- IMCP focuses on information flow and minimizing exposure of data while verifying proper cybersecurity controls
- Incorporate Cyber in CPARS annual evaluation for winner only following post protest period.

Example of Risk to MDA  
CUI down supply chain



L	<b>Low Risk</b>
<ul style="list-style-type: none"> <li>• CUI collected, developed, received, transmitted, used, or stored. DFARS 7012 included. <b>Meets</b> NIST SP 800-171 Rev 1 controls via SSP and POAM</li> </ul>	
M	<b>Medium Risk</b>
<ul style="list-style-type: none"> <li>• CUI collected, developed, received, transmitted, used, or stored. DFARS 7012 included, in the subcontract. Vendor is <b>NOT</b> in compliance with NIST SP 800-171 Rev 1</li> </ul>	
H	<b>High Risk</b>
<ul style="list-style-type: none"> <li>• CUI collected, developed, received, transmitted, used, or stored. DFARS 7012 is <b>NOT</b> included in the subcontract. Vendor is <b>NOT</b> in compliance with NIST SP 800-171 Rev 1</li> </ul>	
N	<b>Limited Risk</b>
<ul style="list-style-type: none"> <li>• No CUI collected, developed, received, transmitted, used, or stored. DFARS 7012 not required</li> </ul>	

IMCP answers the questions:  
Where is MDA data and how is it protected?



# MDA Cyber Assistance Teams (CAT)

- **MDA CAT Mission:**

- Improve DIB Cybersecurity posture through threat-based assessments of company networks, and creation of tailored mitigation strategies
- Strengthen MDS Technical Advantage by working with MDA DIB to protect critical MDA data and identify adversary tactics, techniques, procedures
- Share DoD Cyber threat information with MDA DIB partners, as applicable

- **MDA Cyber Assistance Teams:**

- Multi-discipline cyber team activity: closely resemble DoD Cyber Protect Teams “hunt team” operations; focused on unclassified DIB Partner commercial networks
- Threat-based assessments: comprehensively characterizes risk to MDA info on DIB vendor networks
- Comprised of subject matter experts: Cyber Hunt, Cyber Intelligence, Cybersecurity, Industrial Security, Counterintelligence and MDA program experts
- Company identification restricted by use of Nondisclosure Agreements, controlled ID numbers
- Voluntary MDA program founded on teamwork, non-attribution, and non-retribution policy



# Key Takeaways

- The threats facing DoD's unclassified information have dramatically increased as we share more information online, digitally store data, and increasingly rely on contractors for a variety of information, technology, and services
- DoD and MDA are focused on Cybersecurity and the Defense Industrial Base
- Missile Defense technical information is spread across the DIB in a highly complex supply chain
- The MDA IMCP reinforces DFARS 252.204-7012 and NIST SP 800-171 requirements in the implementation, controlling, and verification of security of Missile Defense Information
- NIST SP 800-171A is a tool for conducting efficient, effective, and cost-effective assessments of contractor systems and networks
- The MDA CAT is a voluntary program to assist the DIB in securing networks and systems
- The CMMC model measures cybersecurity maturity and is designed to provide DoD assurance that a DIB contractor can adequately protect CUI

**Cybersecurity has become a foundation of DoD Acquisition**

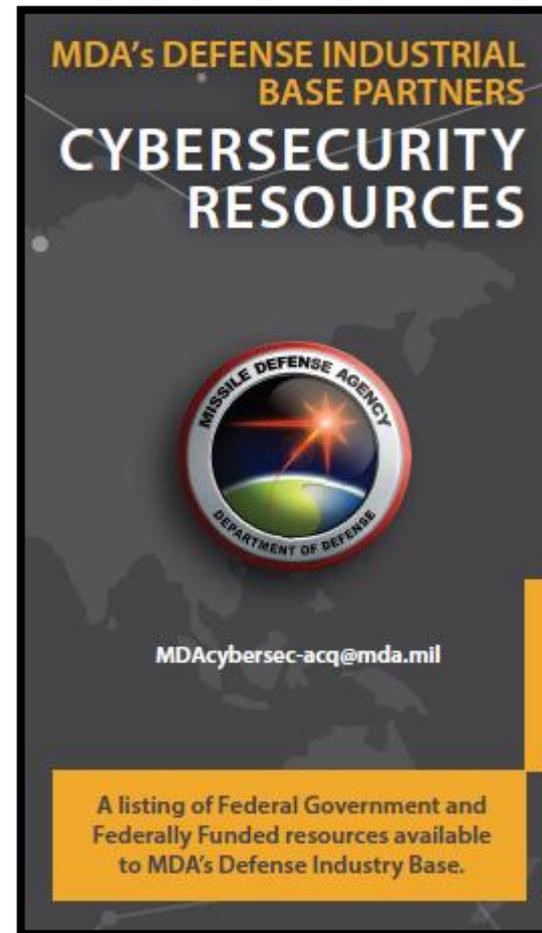


# MDA Cybersecurity Resources Brochure

Provides a listing of Federal Government and Federally Funded cybersecurity resources available to MDA's Defense Industrial Base partners

Topics include:

- Threat Indicator Resources
- DoD Cybersecurity Assessment and Policy
- NIST References
- DoD Cybersecurity Contract Requirements
- Cybersecurity Awareness and Outreach





# Resources

- **Cybersecurity Maturity Model Certification (CMMC)**  
(<https://www.acq.osd.mil/cmmc/index.html>)
- **DoDI 5200.48, Controlled Unclassified Information**  
(<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800>)
- **NIST SP 800-171, Revision 2**  
(<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>)
- **NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information**  
(<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf>)
- **DoD Cyber Exchange** (<https://public.cyber.mil/>)
- **DoD's Defense Industrial Base Cybersecurity program (DIB CS Program)**  
(<https://dibnet.dod.mil>)
- **MDA Cybersecurity Resources Brochure**  
([https://www.mda.mil//global/documents/pdf/cybersecurity\\_brochure.pdf](https://www.mda.mil//global/documents/pdf/cybersecurity_brochure.pdf))



# Resources

- **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
  - Published “Cybersecurity Self-Assessment Workbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements”, November 2017  
(<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>)



# Resources

- **Cybersecurity in DoD Acquisition Regulations** page at (<http://dodprocurementtoolbox.com/>) for **Related Regulations, Policy, Frequently Asked Questions, and Resources, June 26, 2017**
- **DPC Website** (<http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>) and ([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))
- **DoDI 5230.24, Distribution Statements on Technical Documents** ([www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf))



# Questions?

## MDA Strategic Cyber Council MDACyber

Headquarters MDA  
5700 18th Street, Building 245  
Fort Belvoir, VA 22448-5148

571.231.8496  
256.450.4477

[MDACybersec-acq@mda.mil](mailto:MDACybersec-acq@mda.mil)

DA/DE/IC

Address

Voicemail  
Office

MDAUNet



**571-231-8496**

**[MDACybersec-acq@mda.mil](mailto:MDACybersec-acq@mda.mil)**



**BACKUP**



# DoDI 5200.48, Controlled Unclassified Information (CUI)

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD
- Establishes the official DoD CUI Registry
- Defines CUI as information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls
- Cancels DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information,” February 24, 2012

March 6, 2020



DoD INSTRUCTION 5200.48  
CONTROLLED UNCLASSIFIED INFORMATION (CUI)

---

**Originating Component:** Office of the Under Secretary of Defense for Intelligence and Security  
**Effective:** March 6, 2020  
**Releasability:** Cleared for public release. Available on the Directives Division Website at <https://www.esd.whs.mil/DD/>.  
**Cancels:** DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information,” February 24, 2012, as amended  
**Approved by:** Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

---

**Purpose:** In accordance with the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.
- Establishes the official DoD CUI Registry.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800>



# Cyber Incident Reporting

- **When a cyber incident occurs, the contractor shall:**
  - Review contractor network(s) for evidence of compromise of covered defense information using contractor's available tools, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts
  - Identify covered defense information that may have been affected
  - If contract includes operationally critical support, determine if the incident affects the contractor's ability to provide operationally critical support
  - Rapidly report directly to DoD via <https://dibnet.dod.mil> (within 72 hours)
    - Subcontractors provide incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor)



**A DoD-approved medium assurance certificate is required to access the reporting module.**



# Strategies to Enhance Cybersecurity Measures Provided by DFARS

## Clause 252.204-7012 and 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



# Strategies to Enhance Cybersecurity Measures Provided by DFARS

## Clause 252.204-7012 and 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



# What is Controlled Unclassified Information (CUI)?

- **CUI is unclassified information that meets the standards for safeguarding and dissemination controls pursuant to laws, regulations, or government-wide policies under E.O. 13556**
  - CUI must be stored or handled in controlled environments that prevent or detect unauthorized access
- **The National Archives and Records Administration (NARA) CUI Registry is a primary source of information regarding CUI**
- **Reference: NIST SP 800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**

**CUI = Information that is sensitive but unclassified**