

# Cybersecurity in MDA

## Protecting DoD Controlled Unclassified Information

Ms. Diane Knight, Chief Executive Staff, MDA Director for Acquisition (DA)  
Dr. Mike Wojcik, DA Information Systems Security Manager (ISSM)





# What is Cybersecurity?



**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.

*Source: NSPD-54/HSPD-23*



# Ballistic Missile Defense System

## SENSORS

An effective layered defense incorporates a wide-range of sensors to detect and track threat missiles through all phases of their trajectory. Satellites and a family of land- and sea-based radars provide worldwide sensor coverage.



SATELLITE SURVEILLANCE



FORWARD-BASED RADAR



UPGRADED EARLY WARNING RADAR



AEGIS BMD SPY-1 RADAR



SEA-BASED X-BAND RADAR

## BOOST/ASCENT Defense Segment

Potential New Technologies



AEGIS Ballistic Missile Defense

SM-3 Standard Missile-3

## MIDCOURSE Defense Segment



EKV Exoatmospheric Kill Vehicle

GBI Ground-Based Interceptor

GMD Ground-Based Midcourse Defense

## TERMINAL Defense Segment



AEGIS Sea-Based Terminal

PAC-3 Patriot Advanced Capability-3

THAAD Terminal High Altitude Area Defense

## THE SYSTEM OF ELEMENTS

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

The Command and Control, Battle Management, and Communications (C2BMC) program is the hub of the Ballistic Missile Defense System (BMDS). It is a vital operational system that enables the U.S. President, Secretary of Defense and Combatant Commanders at strategic, regional and operational levels to systematically plan ballistic missile defense operations, to collectively see the battle develop, and to dynamically manage designated networked sensors and weapons systems to achieve global and regional mission objectives.

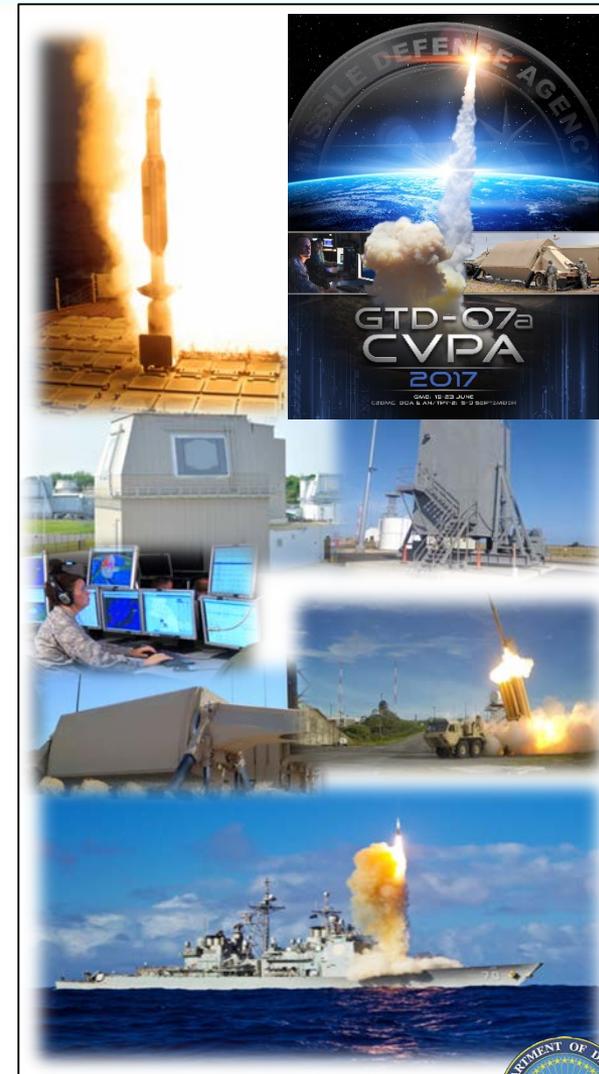
NMCC USSTRATCOM USNORTHCOM USPACOM USEUCOM USCENTCOM

Cybersecurity is Everyone's Responsibility



# Top MDA Cyber Focus Areas

- Identify cybersecurity vulnerabilities that exist on BMDS subsystems (i.e., platforms) and the manner in which they are connected and interoperate
  - Address the advanced threat at the BMDS & 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 BMDS tests
- Determining BMDS Mission Risk
  - Impact (i.e., consequence/severity) if threat actor were to exploit platform vulnerabilities with the intent to degrade the BMDS mission
  - Likelihood threat actor can gain access to a BMDS platform sufficient to execute an attack that impacts the BMDS mission





# 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

## Contractor's Internal System

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

**Federal Contract Information**

**Controlled Unclassified Information (USG-wide)**

**Covered Defense Information (includes Unclassified Controlled Technical Information)**

**Controlled Unclassified Information**

Internal Cloud  
NIST SP 800-171

External CSP  
Equivalent to FedRAMP Moderate

System Operated on Behalf of the DoD

**Controlled Unclassified Information**

Cloud Service Provider

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

## DoD Information System

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

Cloud Service Provider

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

DoD Owned and/or Operated Information System





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

	Nov 18, 2013 (Final Rule)	Aug 26, 2015 / Dec 30, 2015 (Interim Rules)	October 21, 2016 (Final Rule)
<b>Scope – What Information?</b>	<ul style="list-style-type: none"> <li>• <b>Unclassified Controlled Technical Information</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Covered Defense Information</b></li> <li>• <b>Operationally Critical Support</b></li> </ul>	<ul style="list-style-type: none"> <li>• Covered Defense Information (<b>revised definition</b>)</li> <li>• Oper Critical Support</li> </ul>
<b>Adequate Security – What Minimum Protections?</b>	<ul style="list-style-type: none"> <li>• Selected controls in <b>NIST SP 800-53</b>, Security and Privacy Controls for <b>Federal Information Systems</b> and Organizations</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Aug 2015 – NIST SP 800-171</b>, Protecting Controlled Unclassified Information on Nonfederal Information Systems &amp; Organizations</li> </ul>	<ul style="list-style-type: none"> <li>• NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems &amp; Organizations</li> </ul>
<b>When Req'd to Meet Minimum Protections?</b>	<ul style="list-style-type: none"> <li>• <b>Contract Award</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Dec 2015 – As soon as practical, but NLT Dec 31, 2017</b></li> </ul>	<ul style="list-style-type: none"> <li>• As soon as practical, but NLT Dec 31, 2017</li> </ul>
<b>Subcontractor/ Flowdown</b>	<ul style="list-style-type: none"> <li>• <b>Include the substance of the clause in <u>all</u> subcontracts</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Include in subcontracts for operationally critical support, or when involving covered information system</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Contractor to determine if information required for subcontractor performance retains its identity as CDI</b></li> </ul>





# 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 Information Systems and Organizations, as soon as practical, but not later than December 31, 2017**

**\*\*\***

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





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

- **Developed for use on contractor and other nonfederal information systems to protect CUI (Revision 1 published December 2016)**
  - Replaces use of selected security controls from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- **Enables contractors to comply using systems and practices likely already in place**
  - Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.
- **Provides standardized/uniform set of requirements for all CUI security needs**
  - Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers)
  - Allows contractor to implement alternative, but equally effective, security measures to satisfy CUI security requirements







# Demonstrating Implementation of NIST SP 800-171

To document implementation of NIST SP 800-171 Rev 1, 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





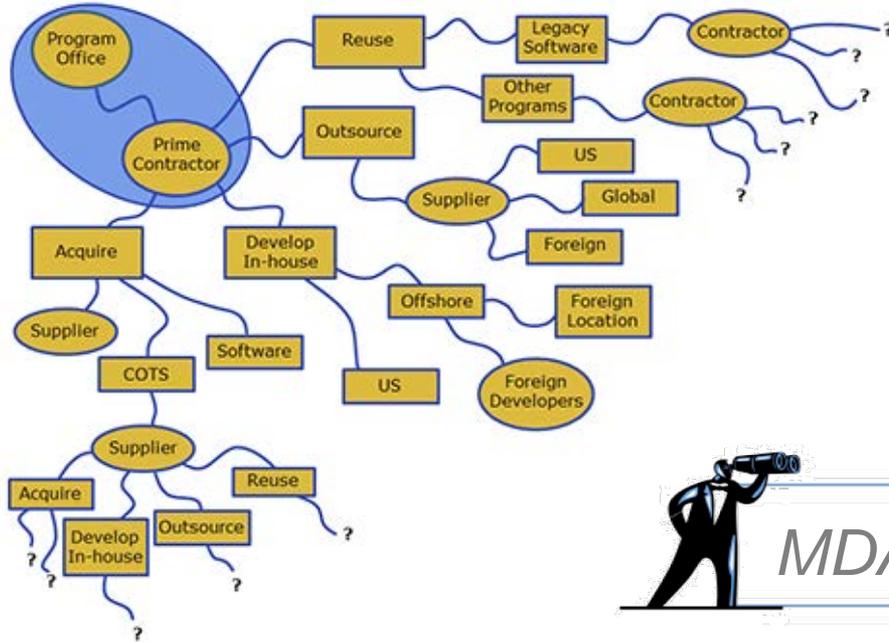
# Contractor Compliance — Implementation of DFARS Clause 252.204-7012

- **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 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**
- **If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract**

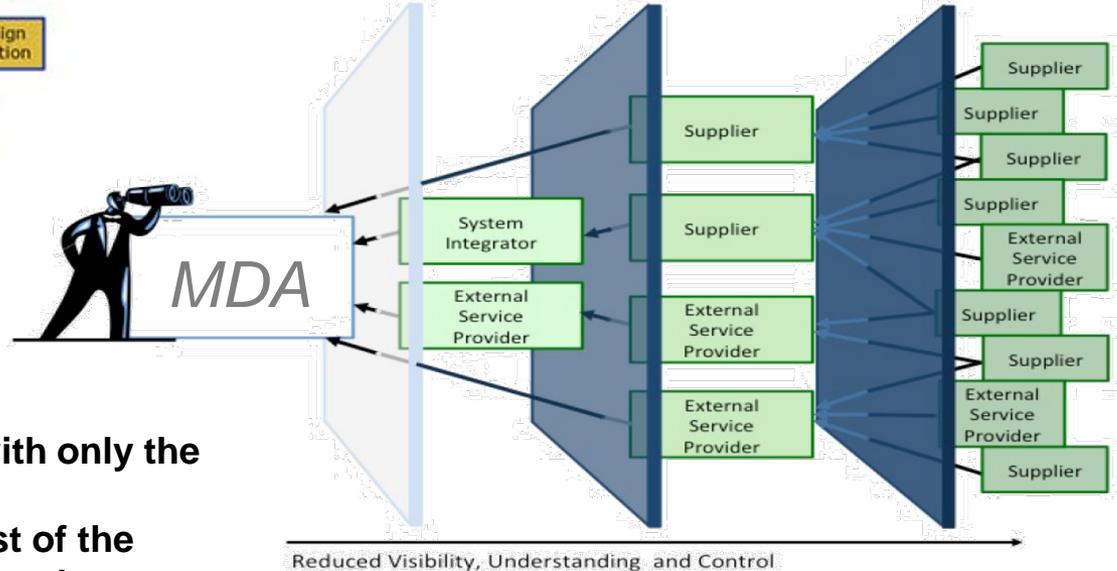




# Increasingly Complex Supply Chain



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



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





# 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 its 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.**





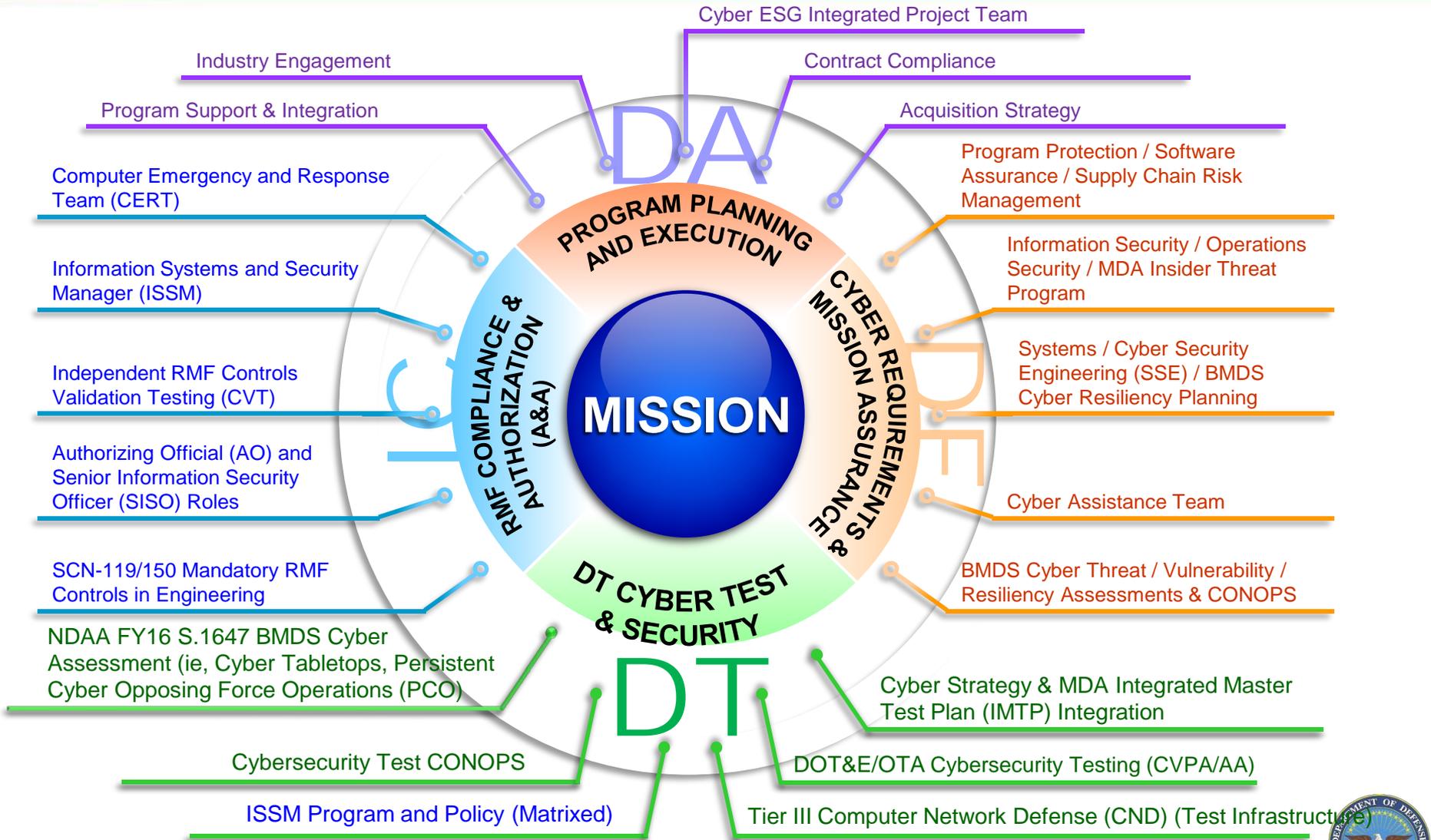
# What MDA Is Also Doing to Support Cyber

- **Cyber Executive Steering Group** addressing policy, organization, workforce & industry implementation
- **Strategic Cyber Council** working with MDA and Industry
- **Cyber Assistance Teams (CAT)**
- **Special Contract Provisions in PWS, SOW, SOO**
  - **DRAFT Information Management and Control Plan (IMCP)**
- **Source Selection provisions for Cyber**
- **CPARS evaluation of Cyber operations, DFARS 252.204-7012 compliance and cyber incident reporting**
- **Incentives for Cyber compliance**
- **New guidance on software development/assurance**





# MDA Cyber Roles and Responsibilities





# MDA Cybersecurity Best Practices Memo



DEPARTMENT OF DEFENSE  
MISSILE DEFENSE AGENCY  
5700 18<sup>TH</sup> STREET  
FORT BELVOIR, VA 22060-5573

DA

JAN 12 2018

MEMORANDUM FOR ALL MDA PRIME CONTRACTORS THROUGH THE COGNIZANT CONTRACTING OFFICERS

SUBJECT: MDA Cybersecurity Best Practices

The Missile Defense Agency (MDA) relies on its industry partners to help execute our mission, which requires the sharing and protection of sensitive data. MDA data is targeted and at risk for compromise across multiple domains, with significant cybersecurity vulnerabilities existing in the Defense Industrial Base (DIB). I am soliciting the continued commitment and assistance of all MDA DIB stakeholders to prevent adversary exfiltration of Ballistic Missile Defense System (BMDS) information from your systems and from systems throughout all levels of your sub-tier contractors and suppliers.

Effective October 21, 2016, revised DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," clarified the definition of Covered Defense Information (CDI) and required compliance with security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 rev.1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Covered Defense Information is defined in DFARS clause 252.227-7013, "Rights in Technical Data-Noncommercial items," Controlled Unclassified Information (CUI) and Department of Defense Manual (DoDM) 5200.01 Vol 4, "Controlled Unclassified Information." To safeguard CDI, contractors and subcontractors are required to implement NIST SP 800-171 rev.1 by December 31, 2017.

Based on feedback received from our industry partners, practices observed in the DIB, and lessons learned from MDA supply chain vulnerability assessments, we have identified a list of frequently recurring NIST 800-171 rev. 1 control shortfalls that you should consider as you take steps to improve cyber hygiene. We have aligned these frequently recurring shortfalls to identified threat vectors within the DIB (spear phishing, credential harvesting, and unsecure perimeter infrastructure). Although organizations are responsible for implementing all the controls outlined in NIST 800-171 rev. 1, I am requesting your assistance in providing increased focus and vigilance when applying the subset of controls, identified as 'MDA Cybersecurity Best Practices', in Attachment 1. These controls provide increased protection of MDA's BMDS information across the DIB.

Additional government resources are available to industry for improving your cybersecurity hygiene are provided in Attachment 2. These sites provide relevant and actionable cybersecurity information.

Our adversaries are engaged today, around the clock, working to infiltrate our networks. Cybersecurity is a team effort and a 24/7 activity that requires steadfast commitment from all stakeholders. It is imperative we continue to improve our cybersecurity protections.

My cybersecurity points of contact are Lieutenant Colonel Todd Cook, Chief, Network Warfare Division, Todd.Cook@mda.mil or 719-721-9997 and Mr. Tony Mesenbrink, MDA Senior Information Security Officer, Anthony.Mesenbrink@mda.mil or 719-721-8157. Please address your comments or questions regarding this subject matter to them.

SAMUEL A. GREAVES 1/12/18  
Lieutenant General, USAF  
Director

Attachments:  
As stated

Identified Threats in the DIB			
Spear Phishing	Credential Harvesting	Unsecure perimeter infrastructure	
Possible Mitigation Solutions			Effectiveness level based on implementation
Email filter			1 - High
Category None Blocking with proxy (web content filter)			1 - High
Elimination of desktop administrators			1 - High
Two-/Multi-factor authentication for remote access			1 - High
Identified Threats in the DIB			
Whole disc	Spear Phishing	Credential Harvesting	Unsecure perimeter infrastructure
Possible Mitigation Solutions			
Secure Distribution statements	1		
Sharing o	- New markings for Controlled Unclassified Information (CUI)		
practices	- Mandate Distribution Statements on CDRLs AND "Work Products" (non-deliverables)		
Mandatory Government & Contractor Training	1		
- FOUO/CUI Marking & Safeguarding			
- Cybersecurity Awareness			
- Distribution Statement Markings			
Supply Chain Operational Security Practices	1		
- Restrict Information Flow-Down (Manufacturing need-to-know)			
Improve Cyber intelligence sharing between Government & industry	1		





# MDA Information Management & Control Plan

- **The Information Management and Control Plan (IMCP) focuses on information flow and minimizing exposure of data while verifying proper cybersecurity controls**
- **Requires contractors to:**
  - **Identify full supply chain where Controlled Unclassified Information (CUI) is collected, developed, received, transmitted, used, or stored**
  - **Verify flow down of DFARS 252.204-7012 (DFARS 7012) to all applicable subcontractors**
  - **Verify NIST Special Publication (SP) 800-171 Rev.1 compliance**
  - **Provide System Security Plan (SSP) and POA&M when requested**
  - **Implement information safeguarding practices to restrict unnecessary sharing of CUI**
  - **Verify and monitor information safeguarding procedures throughout the supply chain**





# Assessing the State of a Contractor's Internal Information System in a Procurement Action

- **DoD Guidance for Reviewing System Security Plans – Developed to:**
  - Facilitate the consistent review of System Security Plans and Plans of Action, and the impact that NIST SP 800-171 Rev 1 Security Requirements “not yet implemented” have on an information system
  - Assist in prioritizing the implementation of security requirements not yet implemented
  - Address the method(s) to implement the security requirements
  - When applicable, provides clarifying information for security requirements that are frequently misunderstood.
- **NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information (*in Final Draft with expected May publication*)**





# 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**

**Ref: DFARS 252.204-7012 (c) - (g)**





# 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**





# Key Takeaways

- MDA has a highly complex supply chain with technical information about the Ballistic Missile Defense System (BMDS) spread across the Defense Industrial Base (DIB)
- DFARS 252.204-7012 requirements for Cybersecurity and Cyber incident reporting are mandatory for MDA contractors in the BMDS supply chain and any information systems or unclassified networks processing BMDS Information
- MDA Information Management Control Plan (IMCP) reinforces DFARS 252.204-7012 and NIST 800-171 requirements implementation, controlling information, minimizing data exposure, verifying proper cybersecurity controls
- NIST SP 800-171 Rev 1 (20Feb18) provides minimum baseline requirements for protecting DIB information systems with DoD information
- NIST SP 800-171A (Draft) is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements
- The DoD / DIB Cybersecurity (CS) program is a voluntary threat information sharing program to supplement DIB capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems.





# Resources

- **Cybersecurity in DoD Acquisition Regulations** page at <https://dodprocurementtoolbox.com/> for Related Regulations, Policy, Frequently Asked Questions, and Resources
- **DPAP Website** <https://www.acq.osd.mil/dpap/dars/dfarspgi/> for DFARs, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- **Cybersecurity Evaluation Tool (CSET)** - Download at <https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET> or request physical copy of software at [cset@dhs.gov](mailto:cset@dhs.gov) — Select “Advanced Mode” to display option to select NIST 800-171\*
- **NIST Manufacturing Extension Partnership** at <https://www.nist.gov/mep>
- **The Procurement Technical Assistance Program (PTAP)** at <http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx>
- **NIST MEP Handbook Cybersecurity Handbook (HB-162) (20 Nov 2017)**, the Handbook provides a step-by-step guide to assessing a small manufacturer's information systems, at <https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security>

\* Includes Revision 1 and all updates up to 20 Feb 2018





# Ballistic Missile Defense System

## SENSORS

An effective layered defense incorporates a wide-range of sensors to detect and track threat missiles through all phases of their trajectory. Satellites and a family of land- and sea-based radars provide worldwide sensor coverage.



SATELLITE SURVEILLANCE



FORWARD-BASED RADAR



UPGRADED EARLY WARNING RADAR



AEGIS BMD SPY-1 RADAR



SEA-BASED X-BAND RADAR

## BOOST/ASCENT Defense Segment

Potential New Technologies



AEGIS Ballistic Missile Defense

SM-3 Standard Missile-3

## MIDCOURSE Defense Segment



EKV Exoatmospheric Kill Vehicle

GBI Ground-Based Interceptor

GMD Ground-Based Midcourse Defense

## TERMINAL Defense Segment



AEGIS Sea-Based Terminal

PAC-3 Patriot Advanced Capability-3

THAAD Terminal High Altitude Area Defense

## THE SYSTEM OF ELEMENTS

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

The Command and Control, Battle Management, and Communications (C2BMC) program is the hub of the Ballistic Missile Defense System (BMDS). It is a vital operational system that enables the U.S. President, Secretary of Defense and Combatant Commanders at strategic, regional and operational levels to systematically plan ballistic missile defense operations, to collectively see the battle develop, and to dynamically manage designated networked sensors and weapons systems to achieve global and regional mission objectives.

NMCC USSTRATCOM USNORTHCOM USPACOM USEUCOM USCENTCOM

# Cybersecurity is Everyone's Responsibility





# 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

