Missile Defense Agency's Management of Supply Chain Risks

To: 9th NASA Supply Chain Quality Assurance Conference

Mr. John H. James, Jr.
Executive Director
Missile Defense Agency
October 23, 2018

Missile Defense Agency

Missile Defense Agency Mission

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









Missile Defense Capability Globally Deployed

Missile Defense Agency Priorities
- In Support Of The National Defense Strategy -

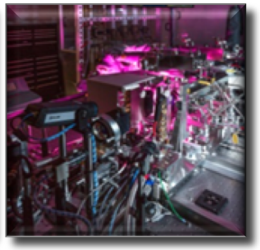
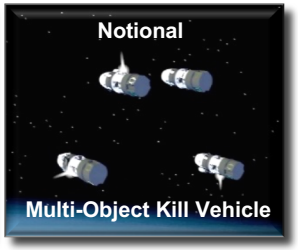
- Continue focus on increasing system reliability to build warfighter confidence



- Increase engagement capability and capacity

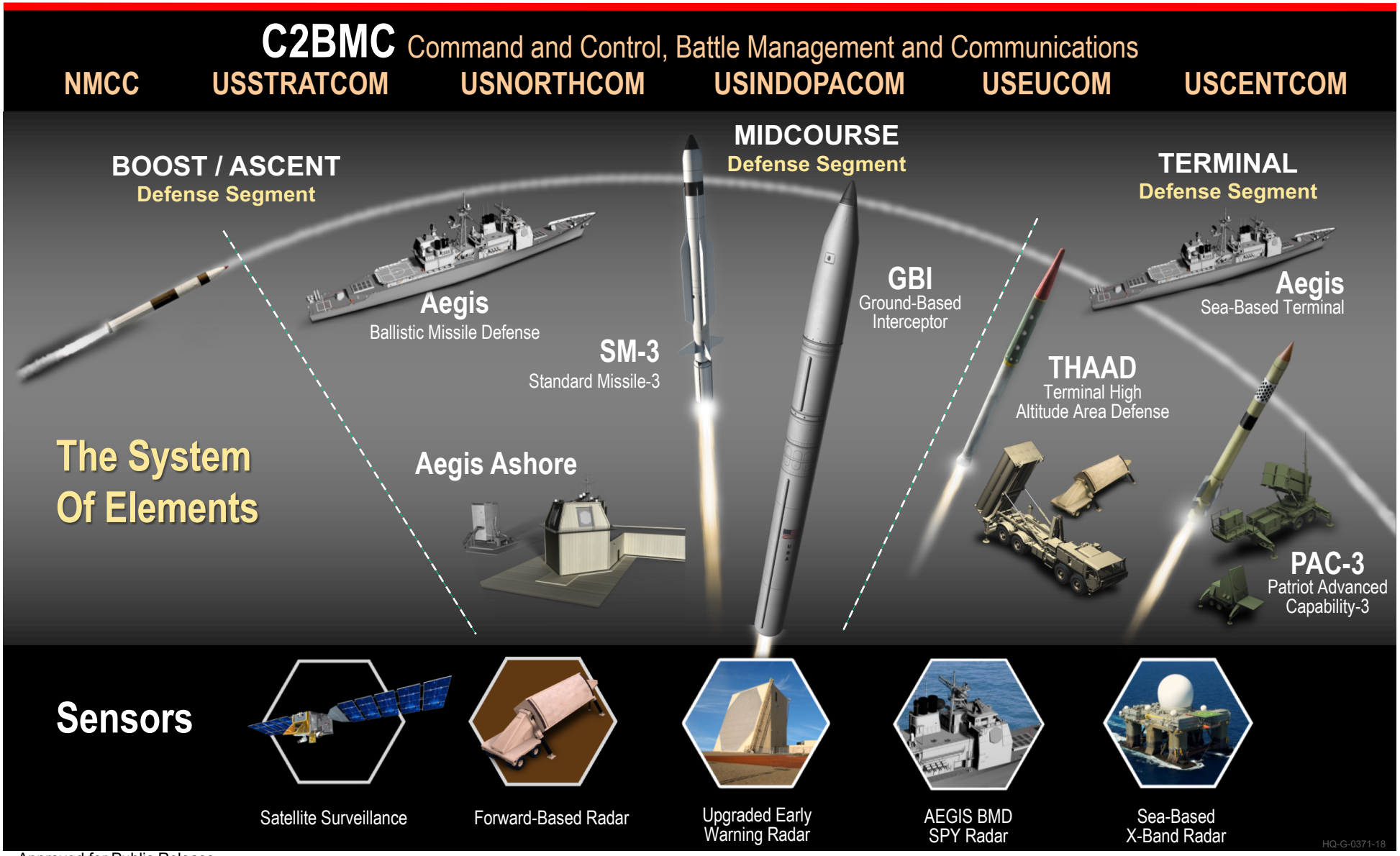



- Rapidly address the Advanced Threat

BMDS Meets Today's Threat but Requires Additional Capacity and Advanced Capability to Stay Ahead of the Evolving Threat

Today's Ballistic Missile Defense System



Missile Defense Agency Video

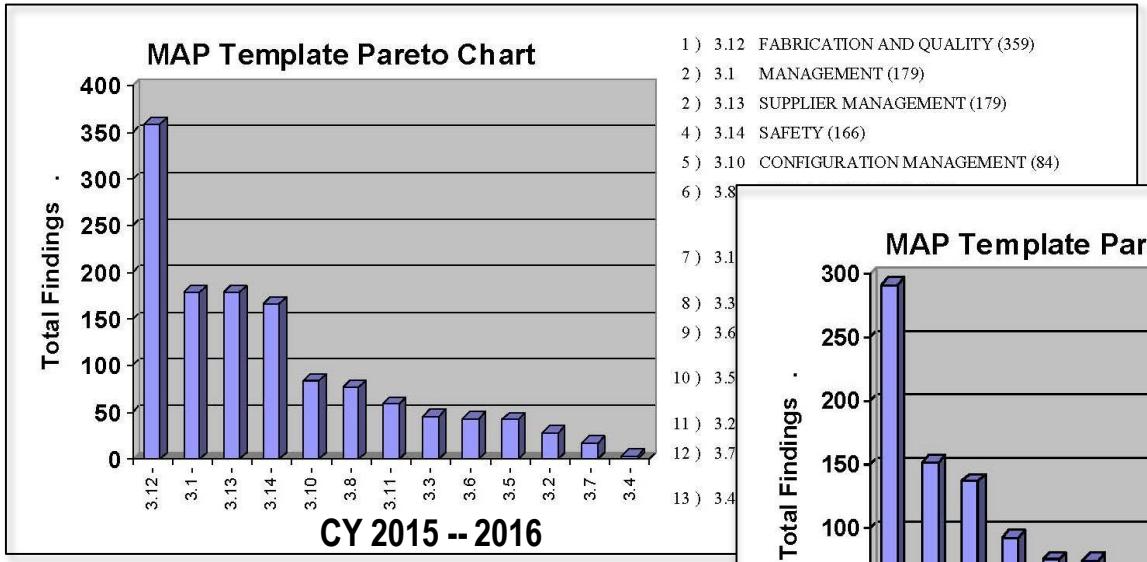
Advanced and Game Changing Technology for the Future

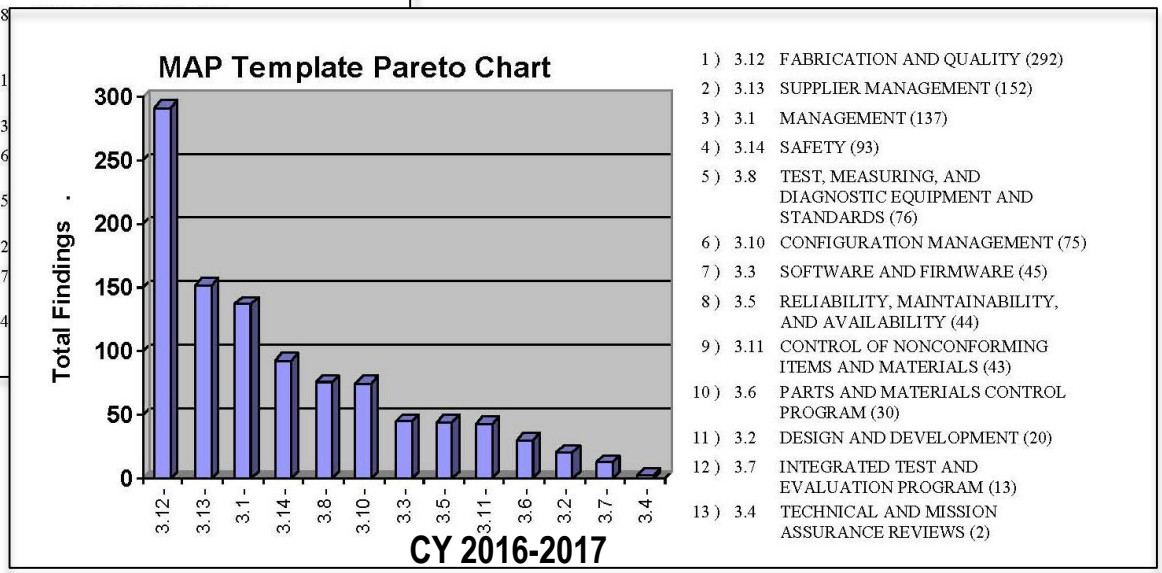
(2:30 mins / Sound)

MDA
Supplier Management

Why Supplier Management is Important to MDA

Technical Assessment metrics based using MDA Assurance Provisions (MAP) Rev B





"Supplier Management" has been typically one of the top three findings since MDA Technical Assessments began

MDA Supply Chain Communication

Key Ongoing Initiatives

- Supplier conferences by program
- Monthly quality metric reviews
- MDA/Industry Quality Forums
- Made for MDA Awareness Campaign to supply chain
- MDA Assurance Representatives (MAR) Regional Plan
- Joint MDA and DCMA Technical Assessments & Training
  - Assessing lower tier suppliers
  - MDA Assurance Provisions (MAP)
  - Parts, Materials & Processes Mission Assurance Plan (PMAP)
  - MAP, PMAP, and Technical Assessors Training

Initiatives in Development

- Add first time yield and test problem reports to defects per unit and escapes within quality metrics
- Increase attention to requirement compliance verification and supplier selection

MDA
Cybersecurity

Cybersecurity Best Practices Memo

DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
5700 18TH 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.

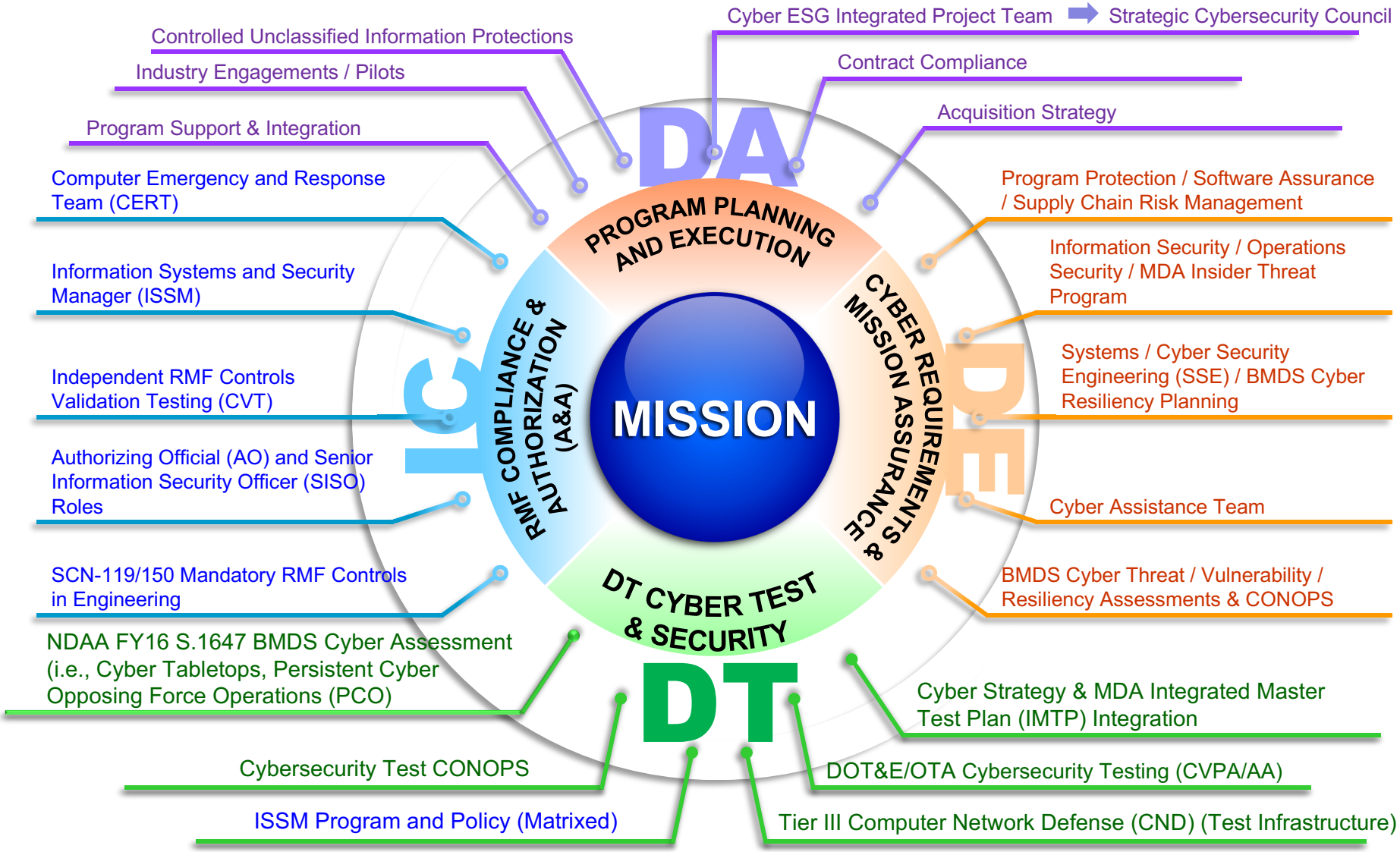
SAMUEL A. GREAVES 1/12/18
Lieutenant General, USAF
Director

Attachments:
As stated

2

"Although organizations are responsible for implementing all the controls, I am requesting your assistance in providing increased focus and vigilance when applying the subject of controls identified as "MDA Cybersecurity Best Practices"... These controls provide increased protection of MDA's BMDS information across the DIB."

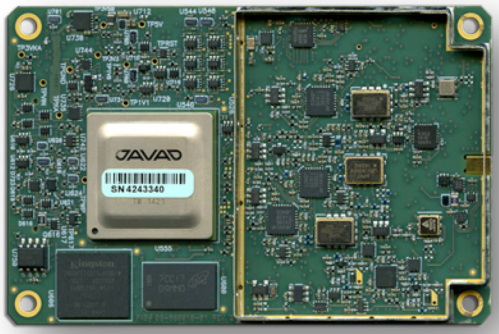
Cybersecurity: A Whole of MDA Effort



MDA
Commercial Off-The Self (COTS) Requirements

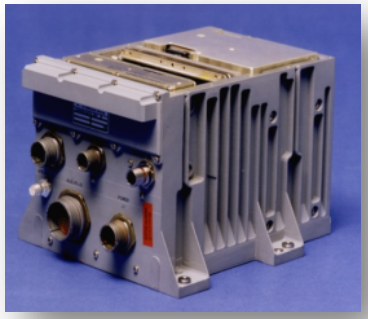
COTS Risk Management

- **Proposing additional/revised MDA guidance to address contractor requirements for COTS hardware**
  - **Add Bill-Of-Material (BOM)**
  - **Add Construction Analysis (CA) for components containing Electrical, Electronic, and Electromechanical (EEE) parts only**
  - **Add Disclosure of Process or Engineering Change Notification (PCN / ECN)**
  - **Change from Dialogue to COTS / Non-Development Items (NDI) Selection Checklist that provides a template for supplier surveillance**



Global Positioning System (GPS) Receiver

Inertial Measurement Unit (IMU)



Space Integrated GPS/ Inertial navigation unit (SIGI)

ISM-1000 Telemetry Data Encryption Unit

Case Study: Tin Whiskers

Tin Whiskers Risk Management

- **Background**
  - **Components with pure tin terminations are at risk for tin whisker growth**
  - **Whisker growth is unpredictable, but certain factors can increase the likelihood of formation:**
    - **Residual stresses within the tin plating**
    - **Coefficient of thermal expansion mismatches**
    - **Scratches or nicks**
    - **Bending or stretching**
    - **Intermetallic formation**
    - **Externally applied compressive stresses**

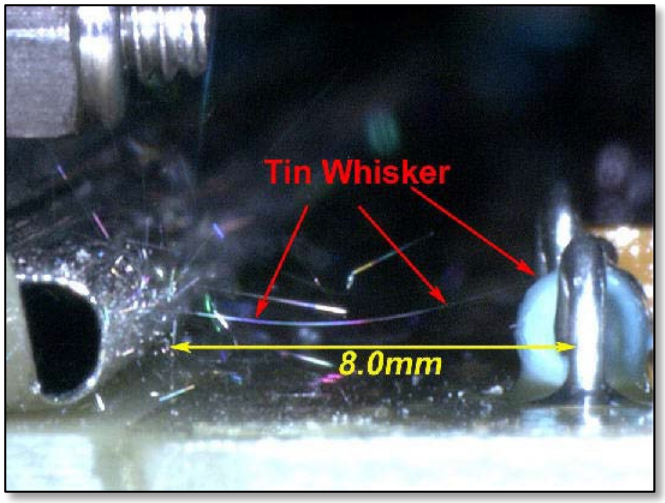


Photo Source: NASA Space Shuttle Program

- **Risks posed by the use of lead-free electronics and recommended mitigation practices are outlined in GEIA-STD-0005-1 and GEIA-STD-0005-2**
  - **Includes developing a lead-free control plan & proven mitigation practices**
- **In 2003, MDA issued a problem advisory discussing tin whisker risks and several follow-on advisories since the initial release**

Tin Whiskers Conclusion

- The use of pure tin finishes by commercial manufacturers impacts MDA
- Tin whisker growth is unpredictable
- Establish a lead-free control plan
  - Refer to GEIA-STD-0005-1 and GEIA-STD-0005-2
- Understand that the use of pure tin components without mitigation will decrease system reliability

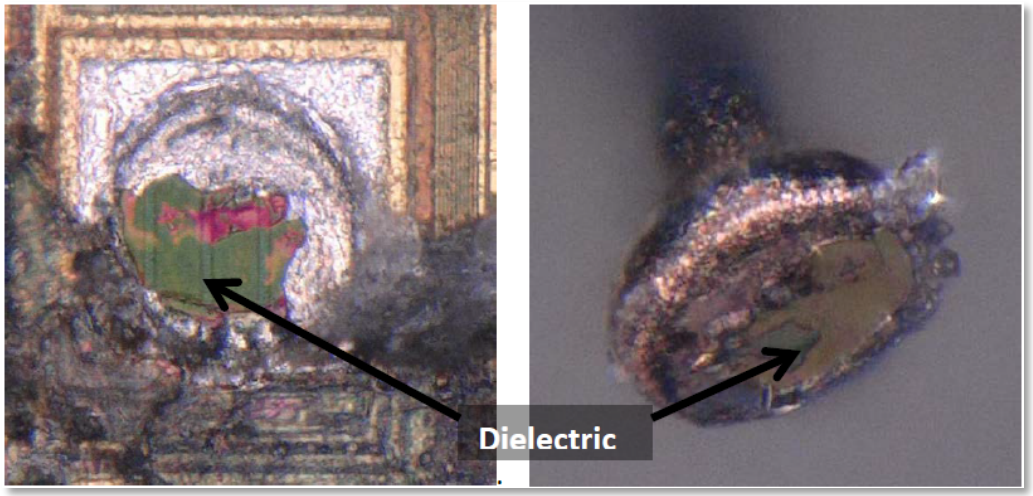
Case Study: Copper Wire Bond

Copper Wire Bond Risk Management

- The Department of Defense is continuing to identify and assess the risks associated with using copper bond wire parts in defense systems

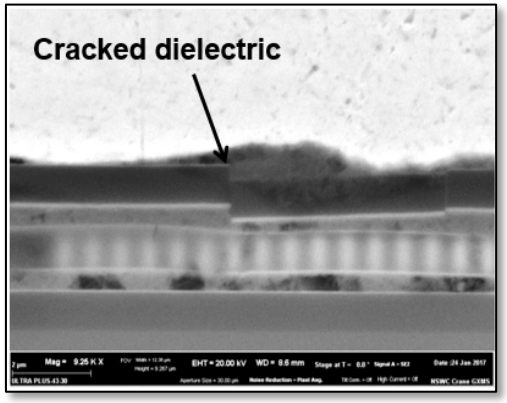
- Test and evaluation processes for PEMs must be updated to account for the differences between gold and copper bonding processes

- Destructive Physical Analysis (DPA) is an effective method for detecting manufacturing process indicators and defects



(e.g., Ball bond lift with cracked dielectric: Force to failure 1.3 grams)

- Screening processes should be in place to identify all use of plastic encapsulated microcircuits (PEM) with copper wire bonds in each system



Copper Wire Bond Conclusion

1. The technical risks of using copper bond wires are still under evaluation and a concern for defense applications
2. Copper bond wires are an emerging issue; updating requirements and assessing the risks should be a top priority industry wide
3. Screening processes need to be in place to properly identify any use of copper wire bond devices
4. DPA proved to be an expedient and statistically meaningful method for detecting/screening manufacturing process indicators, defects, and changes

Developing, Delivering, and Sustaining Ballistic Missile Defense

People, Processes, and Products

REAL WORLD DATA COLLECTION AND THREAT OBSERVATION

COLLABORATION WITH INTELLIGENCE COMMUNITY

THREAT ENGINEERING

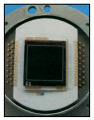
WARFIGHTER INVOLVEMENT IN PRIORITIES & CAPABILITIES

SERVICES

JROCM CAPABILITIES DOCUMENT FOR HOMELAND BMD

TECHNOLOGY DEVELOPMENT

Airborne Sensor



Focal Plane

Multi Object Kill Vehicle

Space-Based Kill Assessment

Directed Energy

PRODUCT DEVELOPMENT

Command & Control

GMD

Sensors

Aegis BMD

TESTING

THAAD

Aegis BMD

GMD

GMD Test

PRODUCTION

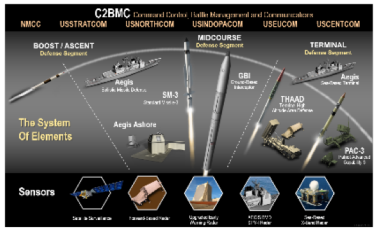
GMD

Aegis Ashore

THAAD

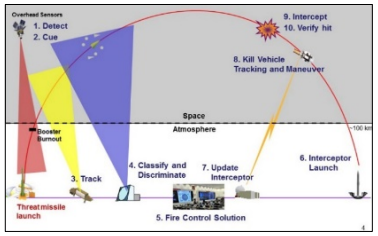
Standard Missile (SM-3) BLK IIA

DEPLOYED BALLISTIC MISSILE DEFENSE SYSTEM



OPERATIONS AND SUSTAINMENT

10 STEPS TO MISSILE INTERCEPT



CONGRESS
DEFENSE INDUSTRY
INTERNATIONAL PARTNERS
EXTERNAL INTEREST
PRESS / PUBLIC

SYSTEMS ENGINEERING PROCESS AND PRODUCTS

Plan	Define	BMDS System Design	Element Design & Build	Test & Verify	Assess	Deliver
• National Security Strategy • Warfighter Prioritized Capability List • Adversary Capability Document	• Capability Planning Specification • BMD System Description Document • Modeling & Simulation • Systems Requirements	• Adversary Data Package • BMD System Specification • M&S Simulation Conceptual Model	• BMD System Interface Control Document • Element Capability Specifications	• Integrated Master Test Plan • Integrated M&S Master Plan	• Integrated Master Assessment Plan • System Assessment Reports	• Technical Capability Declaration • Operational Capacity Baseline

Warfighter Request for Analysis and Request for Information

"The Engineering Process makes us special…because it's not only credible, it's repeatable, it's predictable and has stood the test of time." (Lt Gen Greaves – 27 Sep 2018)

Approved for Public Release 18-MDA-9814 (22 Oct 18)

As of October 16, 2018

Summary – MDA Priorities
- In Support of the National Defense Strategy -

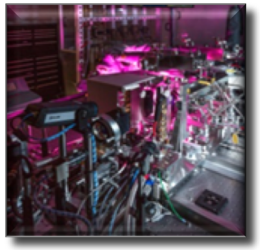
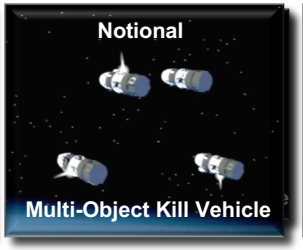
- Continue focus on increasing system reliability to build warfighter confidence



- Increase engagement capability and capacity




- Rapidly address the Advanced Threat

Management of Supply Chain Risks to Stay Ahead of the Evolving Threat


MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE