CYBER ASSISTANCE TEAM OVERVIEW BRIEFING

By Mr. Kraig Kitchen-Henry
Director, Cyber Assistance Team
Missile Defense Agency
April 28, 2021
Agenda

• Introduction
• MDA CAT Operations
• MDA CAT Deployment Expectations
• Administrative Concerns
• Cyber Threat Overview
• Conclusion
Introduction

• MDA Cyber Assistance Team (CAT) Purpose:
  - Improve cybersecurity posture through threat-based reviews & creation of tailored mitigation strategies
  - Share unclassified & classified (as able) DoD cyber threat data with Missile Defense System (MDS) Defense Industrial Base (DIB) partners
  - Facilitate discovery & coordination of threat info, enabling protection of DoD DIB networks

• MDA CAT Background
  - Pilot Program started by MDA in 2016 to address the gap in protection of unclassified DIB networks
  - Goal is to highlight strengths, identify & remediate areas that need improvement
  - Company identification restricted by use of Nondisclosure Agreements, controlled ID numbers, etc.
  - Voluntary program relying on teamwork & non-attribution/non-retribution policy

• MDA CAT Process:
  - Identify Vulnerabilities
  - Prioritize effort by IT infrastructure complexity, MDA data criticality, cyber threat intelligence
  - Evaluate Threats
  - Research & characterize cyber threats, analyze threat reporting, tailored threat assessment
  - Assess Cyber Posture
  - Review security processes/mechanisms (policies, procedures, technical controls) & implementation
  - Report / Mitigate Risk
  - Comprehensive analysis with observations & findings, risks to MDA data & risk reduction recommendations
MDA CAT Operations

- **PROTECT UNCLASSIFIED MDA DATA**
  - **COLLABORATE**: Work collaboratively with DIB partner volunteers
  - **SHARE**: Success is driven by sharing information, expertise & security best practices
  - **FACILITATE**: Facilitate discovery & coordination of threat information, enabling protection of DoD DIB networks
  - **PROVIDE SMEs**: Support drawn from subject matter experts (SMEs) within MDA (e.g. Contracting, Counterintelligence, Intelligence)
  - **CYBER LIAISON**: Liaison with Defense Security Service (DSS), Federal Bureau of Investigation (FBI), Defense Cyber Crime Center (DC3) and others
What to Expect from MDA CAT

**Activity:**
- Smallest possible footprint & minimal disruption to operations
- On-site CAT activities are passive – team will not enter commands or alter existing configuration settings
- Team members may provide technical assistance to company personnel in order to generate or retrieve log information and metadata
- CAT members will work with DIB partners to address findings & observations
- Follow-up after DIB partner determines it has remediated findings
  - Will sample & observe remediation vs. full effort assistance visit

**Products:**
- Out-brief to DIB partner executive team upon completion of main effort
- MDA analysis and mitigation report
  - Findings summary report that includes detailed analysis & suggested mitigation or remediation strategies
  - Recommended Plan of Action & Milestones (POA&M)
  - Final mitigation report
Administrative Concerns

- MDA CAT services are offered at no cost
  - Any costs related to assisting CAT deployment & associated level of effort should be directed to the contracting officer
- Remediation costs will be borne by the DIB partner
- POA&M is a suggestion only, reflective of the voluntary nature of the program
- The MDA CAT routinely cooperates with FBI, DSS, and other agencies, as is relevant or necessary
- Any identified active network intrusion and/or activity will require prompt DIB partner notification of both law enforcement and the contracting officer
Cyber Threat Overview

• Missile Defense Cyber Threat Environment:
  - Missile defense information under constant threat by determined, increasingly capable cyber actors
  - Cyber actors actively pursuing missile defense information; exfiltration (theft) from DIB partners is extensive
  - Stolen missile defense information enables identification & exploitation of key technologies or deployment strategies
Conclusion

• The MDA CAT mission is to improve overall cybersecurity posture
  - Focus is on information exchange, recommendations, relationship building
  - No-cost, non-attributable, threat-based review of corporate network environment
• Small teams that analyze & assist
  - Provide findings & mitigation/remediation recommendations – No Grades
• Ultimate goal is to create a strong partnership with MDA’s Defense Industrial Base Partners in order to better protect your systems and networks and safeguard our Missile Defense Information

• How do you get involved?
  - Contact your Contracting Officer
  - Contact the CAT directly
    Director, Cyber Assistance Team: Mr. Kraig Kitchen-Henry
    Deputy Dir., Cyber Assistance Team: Mr. Thomas Wootton

Email: MDAcyberassistanceteam@mda.mil
Questions?