MDA / Defense Industrial Base Effort: Data and the Supply Chain

Panel Discussion: NDIA Cyber DFARS Summit

7 December 2016

Approved for Public Release
16-MDA-8927 (22 November 16)

Cyber Defense in the Defense Industrial Base (DIB)

- PROBLEM: MDA Data is at risk in the DIB

  - Most MDA Industry Partners store/transmit Covered Defense Information - sensitive/technical data, for example:
    - ➢ System design specifications
    - ➢ Network / Software Architectures
    - ➢ Drawings of systems, equipment, facilities
    - ➢ Test Information including plans, analysis, outcomes

  - MDA Primes and their subs/suppliers have varying levels of cybersecurity defenses

  - MDA DIB partnership: Lockheed, Boeing, Northrop, Raytheon
    - ➢ DFARS 252.204-7012 Implementation (NIST 800-171)
    - ➢ Compliance Date: 31 December 2017

IPT formed to address DFARS compliance

Cooperative Efforts

2 Key Questions:

Where is MDA data?
How is MDA data being protected?

- **MDA Data Call** – effort to proactively identify cyber protections
- **Quick Wins –** technical/non-technical measures to address most frequent adversary threats*
  - MDA and industry primes collaborated on solutions
  - MDA Director Memo (recommendation)
- **Deep Dive Study** – understand how covered defense information is flowing from the prime contractor to varying levels of subcontractors and how the information is being protected by the subcontractors

*Identified Threats in the DIB		
Spear Phishing	**Credential Harvesting**	**Unsecure perimeter infrastructure**

Technical	**Email Filter**	**Web Content Filter**	**2 factor authentication for web facing applications**	**Removal of desktop administrator**	**End of life operating systems**
Non-Technical	**Mandatory Marking**	**Supply Chain OPSEC Practices**	**Mandatory Government and Contractor Training**	**Cyber Intel Sharing between MDA/Industry**	**Incident Response Plan**

Improve the overall cybersecurity posture both in MDA and the DIB

MDA Data Call (Revised)

Process

- Each of the four prime contractors surveyed all their tier 1 and 2 suppliers across 32 contracts vice 450 MDA contracts (initial data call)
  - 1st tier
    - 258 suppliers total
  - 2nd tier
    - 158 suppliers total

Results

Possible Mitigation Solutions	Results
Email filter	🟡🟢
Category None Blocking with proxy (web content filter)	🟡🟢
Two-/Multi-factor authentication for remote access, sysadmins, Outlook Web Access (OWA) on internet facing devices	🟡🔴
End of life (EOL) operating systems for internet connected systems	🟡🟢
Data Classification / Labeling (New)	🟡🔴

Key:

🟢 **Generally good conformance**

🟡 **Area of concern – work to be done**

🔴 **Major concern area - priority**

Quick Wins: Technical Focus Items

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
End of life operating systems for internet connected systems	1 – High
Whole disk encryption for remote laptops	2 – Medium
Data encryption at rest	2 – Medium
Transport Layer Security	2 – Medium
Secure Dropbox	2 – Medium
Sharing of hardening practices / Configuration Control practices	2 – Medium

Quick Wins: Non-Technical Focus Items

Identified Threats in the DIB		
Spear Phishing	Credential Harvesting	Unsecure perimeter infrastructure

Possible Mitigation Solutions
Distribution statements - New markings for Controlled Unclassified Information (CUI) - Mandate Distribution Statements on CDRLs AND “Work Products” (non-deliverables)
Mandatory Government & Contractor Training - FOUO/CUI Marking & Safeguarding - Cybersecurity Awareness - Distribution Statement Markings
Supply Chain Operational Security Practices - Restrict Information Flow-Down (Manufacturing need-to-know)
Improve Cyber intelligence sharing between Government & industry

“Deep Dive” Study

Process

- CDI data sets selected for three major programs
- The goal was to trace data from the prime to the end supplier tier
- Suppliers surveyed about quick wins and other data protections in place

Results

- In most cases secure email and secure portal were the preferred methods for data transfer
  - ➢ In a few cases all work was performed and data retained on site
- Compensatory measures support compliance with SP 800-171
- Data “adequately” protected at the Prime and their Tier 1 … Tier 2 and beyond have *mixed* capabilities
- Lack of contractual relationship between ‘Prime’ and below creates possible constraints

Comments / Questions