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.

Sam Greaves

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

Attachments:
As stated

Cybersecurity Best Practices: Recommended Measures to Improve Cybersecurity Hygiene

Technical Focus Items		
Identified Threats in the DIB		
Spear Phishing	Credential Harvesting	Unsecure Perimeter Infrastructure
Measures	NIST SP 800-171 Rev.1 Control #	Impact level
Audit/Control - Administrator Privilege	3.1.5	1 – High
Limit logon attempts and lock after periods of inactivity	3.1.8 / 3.1.10	1 – High
Disable unlimited remote access	3.1.12 / 3.1.13	1 – High
Deploy network access control	3.1.20	1 – High
Remove stale/unused IT end of life systems	3.4.1 / 3.7.1	1 – High
Prohibit “Gray Market” IT procurements (EBay)	3.4.4	1 – High
Enable Two-/Multi-factor authentication	3.5.3	1 – High
Enforce a minimum password complexity	3.5.7	1 – High
Control use of removable media on system components	3.8.4 / 3.8.7	1 – High
Conduct system risk assessment and remediate	3.11.1	1 – High
Deploy Email filter	3.13.1	1 – High
Configure Category “None” blocking (web content filter)	3.13.1	1 – High
Harden Perimeter Networks	3.13.1 / 3.13.6	1 – High
Identify / report system flaws	3.14.1 / 3.14.3	1 – High
Deploy Security / Patching	3.14.4	1 – High

Non-Technical Focus Items		
Identified Threats in the DIB		
Spear Phishing	Credential Harvesting	Unsecure Perimeter Infrastructure
Measures/Controls		
Distribution statements • Develop Controlled Unclassified Information (CUI) marking instruction (***3.1.22***) • Mandate Distribution Statements on CDRLs and program documents (non-deliverables) (***3.1.22***)		
Mandatory Government & Contractor Training • FOUO/CUI Marking & Safeguarding (***3.1.22***) • Cybersecurity Awareness (***3.2.2***) • Distribution Statement Markings (***3.1.22***)		
Supply Chain Operational Security (OPSEC) Practices • Restrict Information Flow-Down (Manufacturing need-to-know) (***3.1.3***) • Limit information listed on commodity Purchase Orders (***3.1.3***)		
Improve Cyber Intelligence Sharing between MDA & Industry • Known supplier issues (***3.11.3***)		
Information System Procurement • All network hardware should be cybersecurity approved – Prior to emplacement on production network (***3.4.4***)		

Cybersecurity Resources

- United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov
- DoD Defense Industrial Base Cybersecurity program (DIB CS program) https://dibnet.dod.mil
- DoD Office of Small Business Programs http://business.defense.gov/
- FBI InfraGard https://www.infragard.org
- DHS Cybersecurity Information Sharing and Collaboration Program (CISCP) https://www.dhs.gov/ciscp
- DHS Enhanced Cybersecurity Services (ECS) https://www.dhs.gov/enhanced-cybersecurity-services
- Defense Security Information Exchange (DSIE) https://www.dsie.org/

Policy Resources

- DoD Procurement Toolbox, Cybersecurity Policy, Regulations, Frequently Asked Questions (FAQs) http://dodprocurementtoolbox.com/
- DPAP Website/DARS/DFARS and PGI http://www.acq.osd.mil/dpap/dars/dfarspgi/current/
  - DFARS Subpart 204.73 and PGI 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - SUBPART 239.76 and PGI 239.76-.Cloud Computing
  - 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
  - 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
  - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
  - 252.239-7009 Representation of Use of Cloud Computing
  - 252.239-7010 Cloud Computing Services
- National Institute of Standards and Technology SP 800-171
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
  - National Institute of Standards and Technology – Cybersecurity https://www.nist.gov/topics/cybersecurity
  - Cloud Computing Security Requirements Guide https://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf