RESOURCES, INFORMATION AND REFERENCES

NIST RESOURCES

RE: FEDERAL ACQUISITION REGULATION (FAR)

**DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS)
AND PROCEDURES, GUIDANCE, AND INFORMATION (PGI)**

DoD PROCUREMENT TOOLBOX AND OTHER

DOD OFFICE OF SMALL BUSINESS PROGRAMS - CYBERSECURITY

ARTICLES, VIDEOS and OTHER INFORMATION

DEPARTMENT OF HOMELAND SECURITY: CYBER SECURITY EVALUATION TOOL

DEPARTMENT OF HOMELAND SECURITY: OTHER RESOURCES

NIST RESOURCES

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations:
NIST SP 800-171 Rev. 1 (December 2016, includes updates as of 06-07-2018; *updates listed at page ix-xv*)

Assessing Security Requirements for Controlled Unclassified Information:
NIST SP 800-171A (June 2018)

NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements:
NIST Handbook 162 (November 2017)

NIST Supplemental Materials:
CUI Plan of Action Template
CUI SSP Template (Per NIST: *"There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans."*)

NIST Publications and Computer Security Resource Center:
Federal Information Processing Standards (FIPS)
Special Publications (SP):
Computer Security
Cybersecurity practice guides
Information technology
Internal or Interagency Reports
Cybersecurity Framework Manufacturing Profile, NISTIR 8183
Small Business Information Security: The Fundamentals, NISTIR 7621 Rev. 1
Information Technology Laboratory (ITL) Bulletins

Mapping: Cybersecurity Framework v. 1.0 to SP 800-171 Rev. 1 (xls)

NIST ITL: Cryptographic Module Validation Program (with links to validated modules database)

NIST Cybersecurity Framework

RE: FEDERAL ACQUISITION REGULATION (FAR)

Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
52.204-21

Mapping: FAR 52.204-21(b)(1) to NIST SP 800-171

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) AND PROCEDURES, GUIDANCE, AND INFORMATION (PGI)

Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)
252.204-7012

Compliance with Safeguarding Covered Defense Information Controls (Oct 2016)
252.204-7008

Safeguarding Covered Defense Information and Cyber Incident Reporting *(Revised December 28, 2017)*
SUBPART 204.73

DFARS Procedures, Guidance, and Information PGI 204—Administrative Matters PGI 204.73—Safeguarding Covered Defense Information and Cyber Incident Reporting (Revised December 1, 2017)

DoD PROCUREMENT TOOLBOX AND OTHER

Cybersecurity FAQs – Implementation of DFARS (April 2, 2018)

"Recent" Items

Policy/Regulations

Other Resources

Note Regarding NIST Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Security Requirement 3.12.4, System Security Plan

While Revision 1 of the NIST SP 800-171 added the system security plan as an explicit requirement - the original version of the publication stated that the system security plan "is expected to be routinely satisfied by nonfederal organizations without specification…". Even without Revision 1 of the NIST SP 800-171 – the contractor may still document implementation of the security requirements with a system security plan.
Frequently Asked Questions (FAQs), dated January 27, 2017, regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 address this in FAQ 34 as follows: The "system security plan" is addressed in NIST 800-171 as "expected to be routinely satisfied by nonfederal organizations without specification" as part of an overall risk-based information security program (see footnote 16, page 6 and Table E-12, PL-2). The system security plan should be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate issues such as those listed in the question above, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities. Elements of the security plan may be included with the contractor's technical proposal (and may subsequently be incorporated as part of the contract).

(https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-11/Note%20Regarding%20NIST%20Special%20Publication%20800-171%20System%20Security%20Plan.pdf)

DARS

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

DoD Guidance - NIST SP 800-171 4-16-2018 (002)

DOD OFFICE OF SMALL BUSINESS PROGRAMS - CYBERSECURITY

Safeguarding Covered Defense Information – The Basics

DPAP Guidance for DoD Acquisition Personnel (Sept 19, 2017)

ARTICLES, VIDEOS and OTHER INFORMATION

Federal Risk And Authorization Management Program (FEDRAMP): Authorized products list

MDA Cybersecurity Best Practices

Northrop Grumman:

- Collected public resources on key controls
- Cyber Awareness Training

What Subcontractors Need To Know Part 1: Introduction to DFARS Cybersecurity Clause and CDI

What Subcontractors Need To Know Part 2: Applying NIST SP 800-171 Controls

What Subcontractors Need To Know Part 3: Incident Reporting and Flowdown Clause

DEPARTMENT OF HOMELAND SECURITY: CYBER SECURITY EVALUATION TOOL

CSET Video Tutorials (See 7.0 and 6.2 application playlists for most recent tutorials)

NCCIC ICS Cyber Security Evaluation Tool Fact Sheet

Downloading and Installing CSET - Instructions (the current version is 8.1)

Once installed, in CSET Preparation, under Mode Selection, choose "Advanced" - "Requirements Based Approach" and on the next screen under the Cybersecurity Standard Selection, choose "NIST Special Publication 800-171"*.

*Please note that the requirements included in CSET are based on the original SP 800-171, not Revision 1. You can customize the questions, or edit the documents you generate to include the additional requirement added at Revision 1, which is:

3.12.4 "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."

Additionally, NIST SP 800-171 at Revision 1 was updated as follows:

> "Unless otherwise specified by legislation, regulation, or governmentwide policy, the use of the term ***information system*** in this publication is replaced by the term ***system***. This change reflects a more broad-based, holistic definition of information systems that includes, for example: general purpose information systems; industrial and process control systems; cyber-physical systems; and individual devices that are part of the *Internet of Things*. As computing platforms and technologies are increasingly deployed ubiquitously worldwide and systems and components are connected through wired and wireless networks, the susceptibility of Controlled Unclassified Information to loss or compromise grows—as does the potential for adverse consequences resulting from such occurrences."

Further updates to Revision 1 are noted in the Errata at the beginning of the most current update.

In CSET assessment, use the "Comments" section to record descriptions of how a particular security requirement is currently being met (or not); use the "Discoveries" section to record your plan of action and milestones.

You can print a system security plan from CSET, which must be edited and customized to your organization. NIST has a simpler SSP template which could be combined with the requirement assessment results/comments details from CSET if you choose not to edit the detailed CSET template, which has more detail than is specified in the requirement at 3.12.4.

DEPARTMENT OF HOMELAND SECURITY: OTHER RESOURCES

Subscribe to US-CERT National Cyber Awareness System alerts

DHS' National Cybersecurity and Communications Integration Center (NCCIC) – National Cybersecurity Assessments and Technical Services (NCATS) team

NCATS provides the following assessment services at no cost to stakeholders in the defense industrial base and other critical infrastructure:

1. Cyber Hygiene: Vulnerability Scanning
2. Phishing Campaign Assessment (PCA)
3. Risk and Vulnerability Assessment (RVA)

Cyber Hygiene: Vulnerability Scanning helps secure your internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. DHS performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After we receive the required paperwork for Cyber Hygiene, our scans will start within 72 hours and you'll begin receiving reports within two weeks.

A **PCA** is a 6-week engagement that measures your team's propensity to click on email phishing lures, commonly used as a means to breach an organization's network. PCA results can be used to provide guidance for anti-phishing training and awareness.

An **RVA** allows you to select from a menu of network security services (network mapping; vulnerability scanning; penetration testing; and phishing, wireless, web application, OS security, and database security assessments). The actual assessment period differs by the type of services requested, but a typical RVA will take place over a two week period: one week external to your environment (testing from the Internet) and one week internal. These assessments are highly customizable to need. After we receive your completed RVA paperwork, you will be prioritized based on national mission needs, number of prior stakeholders in your sector, and other factors. DHS is also taking proactive steps and creating new services, such as remote penetration testing, to assist stakeholders with security relevant issues.

Testing availability is limited. For more information, please contact PolarisMEP, or email NCATS directly at NCATS_INFO@HQ.DHS.GOV

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

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