Huntington
Ingalls
Industries

Supplier Information Session

Safeguarding Covered Defense Information and Cyber Incident Reporting, DFARS 252.204-7012

September 6, 2017

Christopher Page
Senior Staff Counsel

Andrew Pilant
Senior Counsel

DFARS Cybersecurity Rule

- Current Rule
- Covered Contractor Information Systems
- NIST Standards
- Reporting Requirements
- Compliance with the Rule
- Cyber Security Evaluation Tool (CSET)
- Expected Future Regulatory Changes

The content discussed in this presentation is provided for informational purposes only and does not constitute legal advice or counsel. For legal advice or counsel related to issues discussed herein, please consult your attorney.

Current Rule – DFARS 252.204-7012

Effective in prime contracts issued after October 2016

- Must comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171
- Deadline to meet NIST SP 800-171 is December 31, 2017
- Must report areas of non-compliance to DoD CIO
  - *DoD CIO must approve exceptions and alternative measures*
- Cyber incidents must be reported within 72 Hours to both:
  - DoD at http://dibnet.dod.mil
  - Prime Contractor (or your next higher tier contractor)
- *Required Inclusion in all DoD Contracts*
- *Mandatory Flowdown to all Subcontractor Tiers*

Covered Contractor Information Systems

- Unclassified systems owned or operated by, or for, a contractor and that <u>processes</u>, <u>stores</u> or <u>transmits</u>:

- "*<u>Covered Defense Information,</u>*" which includes:
  - **Technical Information marked with a DoD Distribution Statement**
  - **Export Controlled Information**; or
  - Any other information that requires safeguarding or dissemination controls, and is (a) marked or otherwise identified in the contract and provided by the Govt, or (b) developed, received, transmitted, used, stored, etc. by the Contractor in support of the contract.

"Covered Information Systems" is <u>Broad</u> Concept

NIST Standards

NIST SP 800-171

- Covers a variety of factors:
  - Access control
  - Awareness and Training
  - Audit and Accountability
  - Configuration Management
  - Identification and Authentication
  - Incident Response
  - Maintenance
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk and Security Assessments
  - System and Communication Protection
  - System and Information Integrity

Over 100 Items Included in the Standards

Reporting Requirements

Two Important Requirements of the DFARS rule:

1. Report to DoD CIO within 30 days of contract award from HII:
   - YES or NO: In compliance with NIST Standards
   - If NO: must report areas of non-compliance to DoD CIO

2. Report Cyber Incidents within 72 Hours to ***BOTH*** DoD (through http://dibnet.dod.mil/) and HII SCM POC
   - Must first acquire a DoD-approved medium assurance certificate from http://iase.disa.mil/pki/eca/Pages/index.aspx.

The Reporting Requirements are in effect upon award of a contract with the clause (i.e., the December 2017 deadline for NIST Compliance DOES NOT change the reporting requirements)

Reporting Requirements are in Effect Now

DoD Investigation of Reported Incidents

If and when a cyber incident is reported to DoD, DoD has the right to investigate the incident.

- Contractors are obligated to preserve and protect images of affected information systems for at least 90 days
- DoD may conduct forensic analysis of such systems
- If DoD elects to conduct a damage assessment, it may request damage assessment information gathered by the contractor, and seek access to information and equipment necessary to conduct forensic analysis

DoD Damage Assessment Requirements are in Effect Now

Compliance with DFARS 252.204-7012

Deadline: December 31, 2017 (No extension expected).

- "Implementation" means having a System Security Plan (**SSP)** and a Plan of Action and Milestones (**POAM)** that accurately reflect the status of a contractor's compliance with NIST controls, even if the SSP & POAM extend beyond the December deadline.
- DoD is permitted to accept a contractor-proposed "alternative but equally effective" control.
- Look for NIST SP 800-171A to be issued within the next year, which will include assessment procedures to help companies determine whether they are in compliance.

Certification Form for HII Bid and Proposal Activities

- Form provided to any Seller/Offeror expected to receive CDI from HII in support of HII bid and proposal activities
  - You agree to notify the DoD CIO and HII within 30 days of Order award of an Order from HII of any security requirements specified by NIST SP 800-171 not yet implemented at the time of Order award
  - You agree to notify HII in writing when submitting any request to the DoD CIO or Contracting Officer to vary from a NIST SP 800-171 security requirement

- Each Seller/Offeror certifies that:
  - Your information system has security in place that complies with the security requirements of the NIST SP 800-171, **OR**
  - You are in the process of and will complete implementation of adequate security as soon as practical, but not later than December 31, 2017
  - If you are not selected as a subcontractor, you will dispose/destroy any CDI it received from HII.

Cyber Security Evaluation Tool (CSET)

- Free application developed by DHS's Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) to help evaluate systems against NIST SP 800-171 standards.

- Download at: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Expected Future Regulatory Changes

- Corresponding FAR rule (FAR Case 2017-016)
- NIST SP 800-171A
- Updates to resources
  - Network Penetration Reporting and Contracting for Cloud Services FAQs
    - http://dodprocurementtoolbox.com/faqs/cybersecurity/frequently-asked-questions-faqs-dated-jan-27-2017-implementation-of-dfars-case-2013
  - PGI 204.73
    - http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/PGI204_73.htm
  - Guidance to Stakeholders for Implementing DFA
    - http://www.acq.osd.mil/se/docs/DFARS-guide.pdf
  - DoDI 8582.01
    - http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858201p.pdf

No major changes expected, but look for updated resources & guidelines

Questions?

Huntington
Ingalls
Industries

Hard Stuff Done Right ™