Northrop Grumman Corporation Supplier Cyber Regulatory Awareness

Cyber FAR & DFARS Requirements

Feb 14, 2017

POC: Sue Vrzak
NGC Global Supply Chain Director of Compliance
cybersupplychain@ngc.com
Security Environment

• Increasing frequency, sophistication of cyber attacks
  – Can result in business disruption
  – Can result in the loss of Confidentiality and/or Integrity or Availability of data including your own, ours or governments.

• Loss of unclassified military technology and defense information can be put at risk
  – National security
  – Competitive technological advantage
  – US and allied warfighters

• DoD contractors and suppliers need to harden and make resilient unclassified systems

• New mandatory cyber regulations requiring:
  – Tighter security controls
  – Increased cyber incident reporting
Not Theoretical

“OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought” The Washington Post

600 million Samsung Galaxy phones were discovered to have a major security flaw is more than a bit unsettling. According to the cyber-security firm NowSecure, the Samsung flaw originated with one of its software suppliers.


In its publication, “Gazing into the Cyber Security Future: 20 Predictions for 2015,” FireEye analysts predicted that cyber risks through the supply chain would only increase. Its advice to business:.. require suppliers to show evidence of good security controls...


“Target cyber breach hits 40 million payment cards at holiday peak” - Reuters
Potential Cyber Security Supply Chain Risks
Government is leveraging industrial base/supply chain to protect data by applying cyber controls on supply base networks at all tiers

- What is the FAR? USG Acquisition Statutory Requirements

- What is the DFARS? US Department of Defense Supplemental Requirements

- What is NIST SP 800-171? National Institute of Standards and Technology Special Publication
Regulatory Horizon

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>DFARS 252.204-7012, Safeguarding Unclassified Controlled Technical Information (UCTI) Nov 2013</td>
</tr>
<tr>
<td>2014</td>
<td>DFARS 252.204-7012, expanded to Covered Defense Information (CDI) &amp; new controls interim effective Aug 2015</td>
</tr>
<tr>
<td>2015</td>
<td>FAR 52.204-21 BASIC SAFEGUARDING OF CONTRACTOR INFORMATION SYSTEMS REQUIREMENTS Effective June 2016 15 requirements (corresponding to 17 of the 109) NIST SP 800-171 Applies to Federal Contract Information</td>
</tr>
<tr>
<td>2016</td>
<td>DFARS Final Ruling issued Oct 2016</td>
</tr>
<tr>
<td>2017</td>
<td>NIST SP 800-171r1 released Dec 2016</td>
</tr>
</tbody>
</table>

We have adequate controls now Full compliance by Dec 31, 2017

Required in Defense contracts with UCTI to:

- Protect Unclassified (UCTI) Data
- Report Cyber Incidents
- Flow-down to Subcontractors
**FAR 52.204-21 Basic Safeguarding Of Contractor Information Systems Reqs.**

- **Final FAR rule published 2016 effective June 2016**
- Applies to all federal contracts and subcontracts at any tier (except those for COTS products) and requires basic safeguarding of contractor systems that contain *Federal Contract Information*
  - Very broad definition likely to cover many companies.
  - Information, not intended for public release, provided by or generated for the Government, but not public information or transactional information, such as that necessary to process payments.
    - No implementation period, compliance required upon award
- Mandatory flow-down at all tiers
- Imposes 15 requirements that correlate to 17 NIST 800-171 security controls (limited subset)
- No incident reporting requirement
DFARS Clause 252.204-7012 Safeguarding CDI and Cyber Incident Reporting

- Original interim rule released August 2015, updated interim rule in December 2015 & final rule issued October 21, 2016

- Applies to all DoD contracts/subcontracts (except if solicitation is solely for COTS) and requires enhanced safeguarding of covered contractor information systems that contain Covered Defense Information (CDI)

- Mandatory flow down of clause in all subcontracts at all tiers for operationally critical support or for which subcontract performance will involve a covered system with CDI

- Applies to cloud computing; If the Cloud Service Provider (CSP) is a subcontractor, then clause 7012 would flow down, otherwise, CSP with CDI complies with requirements in paragraphs (c) through (g) of the clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment. (FAQ page 26, Q57)
• Must provide adequate security for covered internal systems with Covered Defense Information (CDI)
  – At a minimum must comply with all NIST 800-171 security controls as soon as practical but not later than December 31, 2017
  – Ability to submit “alternative yet equally effective” controls or that specific controls are not applicable to the DoD for CIO approval

• Significant expansion of security controls and scope of covered information from 2013 rule

• No certification authority is recognized by DoD as of Feb 2017
In addition to security controls, contractors and subcontractors must report cyber incidents on covered contractor information systems with CDI, or that affect the contractor’s ability to perform operationally critical support under a contract:

- Upon discovery must conduct a review for evidence of compromise
- Rapidly report within 72 hours directly to DoD via specified online portal
- Must provide DoD-assigned incident report number to prime/higher tiered subcontractor
- Must preserve and protect images of known affected images and systems for 90 days
- Must provide DoD access to additional information or equipment necessary to conduct forensics analysis
- Must submit any malicious software uncovered to DC3, not the Contracting Officer
Key Changes in October 2016 Final Rule

- COTS exemption (does not extend to commercial items)
- Clarifies the definition of “operationally critical support”
- Contemplates that primes and higher tiered subcontractors may consult with contracting officer for guidance as to whether the clause needs to be flowed down
- Subs are required to notify higher tiered subcontractor or prime of requests for alternative but equally effective solutions
- Incident report ID Numbers must be provided to next higher tier subcontractor or prime
- Expands the definition of CDI, including items required on the CUI Registry
"Covered Defense Information" (CDI) is unclassified information that:

- Covered contractor information system” means an [unclassified] information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—

- (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in the performance of the contract; or

- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

Note: Rules Focus on protecting systems with CDI not just the specific information.
Protect CDI
NIST SP 800-171 Security Control Families

- Access Control
- Awareness & Training
- Audit & Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

<table>
<thead>
<tr>
<th>Control Number</th>
<th>Control Family</th>
<th>NIST SP 800-171</th>
<th>CUI Security Requirement</th>
<th>NIST SP 800-53 Relevant Security Controls</th>
<th>NIST SP 800-171 Security Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access Control</td>
<td>3.1.1</td>
<td></td>
<td>AC-2, AC-3, AC-17</td>
<td>Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</td>
</tr>
<tr>
<td>2</td>
<td>Access Control</td>
<td>3.1.2</td>
<td></td>
<td>AC-2, AC-3, AC-17</td>
<td>Limit information system access to the types of transactions and functions that authorized users are permitted to execute.</td>
</tr>
<tr>
<td>3</td>
<td>Access Control</td>
<td>3.1.3</td>
<td></td>
<td>AC-4</td>
<td>Control the flow of CUI in accordance with approved authorizations.</td>
</tr>
<tr>
<td>4</td>
<td>Access Control</td>
<td>3.1.4</td>
<td></td>
<td>AC-5</td>
<td>Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</td>
</tr>
<tr>
<td>5</td>
<td>Access Control</td>
<td>3.1.5</td>
<td></td>
<td>AC-6, AC-6(1), AC-6(5)</td>
<td>Employ the principle of least privilege, including for specific security functions and privileged accounts.</td>
</tr>
</tbody>
</table>
DFARS 252.204-7012 Safeguarding CDI & Cyber Incident Reporting

• “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on a Covered Contractor information system and/or the CDI residing on that system (this requirement is currently in effect).

• Contractor shall rapidly report (i.e., within 72 hours of discovery):
  — Directly to DoD at http://dibnet.dod.mil, AND
  — Provide incident number to Prime Contractor or next higher-tier Subcontractor
  — Must obtain & install medium level assurance cert before you have an event so you can report per the rule

• In addition, Contractor shall:
  — Conduct a review for evidence of compromise
  — Submit any related malicious software
  — Preserve and protect images of all known affected information systems
  — Upon request, provide:
    • access to conduct a forensic analysis
    • all of the related damage assessment information gathered
• NGC will include mandatory flow-down clause in solicitations, POs and Subcontracts supporting all DFARS-applicable contracts
  — Clause is ‘self-deleting’ if subcontractor/supplier’s system does not meet the definition of “covered contractor information system”
  — COTS Suppliers are exempted from Oct. 2016 final rule- at solicitation, not flow-down

• Specifically applies to subcontractors who
  — Provide “operationally critical support”, and/or whose
  — Work involves “covered contractor information systems”

• All subcontractors currently must:
  — Provide adequate security,
  — Report any NIST 800-171 gaps to the DoD CIO within 30 days of award, and
  — Sign up to DIBNet to facilitate reporting.
  — Full compliance to NIST Standard by December 31, 2017
What do you need to do?
Engage your Business

- **Start now** (if you haven’t already)
- **Read the FAR, DFARS and NIST SP 800-171 (Rev 1)**
- **Complete assessment** (NGC Suppliers should use EXOSTAR)
- **Register with DIBNet:** [http://dibnet.dod.mil](http://dibnet.dod.mil)
- **Work across functions**
  - IT, Info Security, Contracts, Supply Chain, *(Engineering, Quality)*
- **Designate Business Point of Contact**
  - Coordinate collection of existing practices, tools, standards
  - Lead cross-org analysis of requirements, gaps in compliance, review of new standards
Primary Resources & Links
Copy these links to your browser.

• FAR: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/Far/52_000.htm#P891_130989

• DFARS: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012


• CUI Registry: http://www.archives.gov/cui/registry/category-list.html


• DoD CIA 30 Day Notice: osd.dibcsia@mail.mil
Additional Cyber Resources

- Industrial control Systems Cyber Emergency Response Team (ICS-CERT): [https://ics-cert.us-cert.gov/Assessments](https://ics-cert.us-cert.gov/Assessments)
- SBA’s link for Cybersecurity [https://www.sba.gov/managing-business/cybersecurity](https://www.sba.gov/managing-business/cybersecurity)
- DHS’ Stop Think Connect cyber resource page for small businesses [https://www.dhs.gov/publication/stopthinkconnect-small-business-resources](https://www.dhs.gov/publication/stopthinkconnect-small-business-resources)
- US Cert’s Page for Small and Medium Size businesses [https://www.us-cert.gov/ccubedvp/smb](https://www.us-cert.gov/ccubedvp/smb)
- Federal Communications Commission (FCC), in collaboration with other government agencies and industry leaders, created the Small Biz Cyber Planner - an easy-to-use, free online tool that will help you create a customized planning guide to protect your business from cybersecurity threats. Learn more at [www.fcc.gov/cyberplanner](http://www.fcc.gov/cyberplanner).
- Federal Bureau of Investigation: [www.fbi.gov](http://www.fbi.gov)
- EXOSTAR: [https://www.exostar.com/](https://www.exostar.com/)
Acronyms

• CDI – Covered Defense Information
• FCI - Federal Contract Information
• NIST – National Institute of Standards and Technology
• FAR – Federal Acquisition Regulations
• DFARS – Defense Federal Acquisition Regulation Supplement
• POA&M – Plan of Action and Milestones
The Value of Performance.

Northrop Grumman

Back-up from here
<table>
<thead>
<tr>
<th>Date</th>
<th>Summary</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 30, 2015</td>
<td>Extends compliance to all NIST SP 800-171 Standards to Dec 31, 2017</td>
<td><a href="http://federalregister.gov/a/2015-32869">http://federalregister.gov/a/2015-32869</a></td>
</tr>
<tr>
<td>NARA Final CUI Ruling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>