What you need to know, why you need to care, and what you need to do
Security Environment - The Burning Platform

• Increasing frequency, sophistication of cyber attacks
  – Can result in business disruption
  – Can result in the loss of Confidentiality and/or Integrity and/or Availability of DoD data
• Loss of unclassified military technology and defense information can put at risk
  – National Security
  – US competitive technological advantage
  – US and allied warfighters
• DoD contractors and suppliers need to harden and make resilient unclassified systems
• New cyber frameworks and standards released
  – Tighter Security Controls
  – Increased Cyber incident reporting
“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
Regulatory Horizon

We have until Dec 31, 2017 to become fully DFARS compliant

DFARS 252.204-7012, Safeguarding Unclassified Controlled Technical Information (UCTI)
Nov 18, 2013  Selected controls NIST 800-53r4

Required in Defense contracts with UCTI to:

• Protect Unclassified (UCTI) Data
• Report Cyber Incidents
• Flow-down to Subcontractors

DFARS 252.204-7012, expanded to Covered Defense Information (CDI) interim effective Aug 26, 2015 109 controls NIST SP 800-171

Expanded to ALL Defense contracts (affecting over 13K companies)

FAR 52.204-21 BASIC SAFEGUARDING OF CONTRACTOR INFORMATION SYSTEMS REQUIREMENTS Effective June 16,2016 15 requirements (corresponding to 17 of the 109) NIST SP 800-171 Expanded to Federal Contract Information

DFARS Final Ruling issued Oct 21, 2016
- Does not apply to COTS
- Tied CDI to CUI Registry
- Subs required to notify next higher tier when requesting Deviations from NIST SP 800-171
- NIST SP 800-171r1 released Dec 20, 2016, 110 controls

Basic Safeguards Extended to ALL Federal contracts (affecting over 300K companies)

Anticipate additional FAR release
Leveraging Industrial Base/Supply Chain

Government leveraging industrial base/supply chain to enforce cyber controls on private networks

• What is the FAR?
• What is the DFARS?
FAR 52.204-21

BASIC SAFEGUARDING OF CONTRACTOR INFORMATION SYSTEMS REQUIREMENTS

• **Final FAR rule published May 16, 2016 effective June 15, 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
  – 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.
• Mandatory flowdown at all tiers
• Imposes 15 requirements that correlate to 17 NIST 800-171 security controls (limited subset)
• No incident reporting requirement
SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

• Must provide adequate security for covered contractor (internal) systems with Covered Defense Information
  – 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 approval
  – For contracts awarded through 9/30/17, submit a report NLT 30 days after contract award to DoD-CIO listing controls not fully implemented at time of award

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

   This is a self assessment/attestation
   (no certification authority exists and won’t be considered by the DoD)
SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

• In addition to 110 security controls, contractors and subcontractors must report cyber incidents on covered contractor information systems with CDI, or that affects 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

• Expands the definition of CDI, including items required on the CUI Registry
• 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
• Contracts signed after 9/30/17 do not require a 30 day notice submittal
What is CDI?

"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 [support of] 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 shifted to safeguarding of contractor systems rather than specific government information.
# Protect CDI

## NIST 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 & Comms Protection
- System and Information Integrity

<table>
<thead>
<tr>
<th>List Number</th>
<th>Control Family</th>
<th>NIST SP 800-171 CUI Security Requirement</th>
<th>NIST SP 800-53 Relevant Security Controls</th>
<th>NIST SP 800-171 Security Description</th>
<th>Company Status Ove</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access Control</td>
<td>3.1.1</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>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Access Control</td>
<td>3.1.2</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>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Access Control</td>
<td>3.1.3</td>
<td>AC-4</td>
<td>Control the flow of CUI in accordance with approved authorizations.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Access Control</td>
<td>3.1.4</td>
<td>AC-5</td>
<td>Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Access Control</td>
<td>3.1.5</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>
<td></td>
</tr>
</tbody>
</table>
Report Cyber Incidents

- “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
Flow-down to Subcontractors, Suppliers

- Contractor will include clause in solicitations, POs and Subcontracts
  - Include this clause in all POs 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 applicable to flow-down- (not verified by DoD)*

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

- Requires subcontractors subject to the clause to meet NIST 800-171:
  - DFARS obligation ends with flowing this clause to Subcontractor
  - Onus is on the Subcontractor to comply
  - Still in question: Contractor accountability to ensure supply base compliance
Engage your Business - What do you need to do?

• Start now (if you haven’t already)
• Read the FAR, DFARS and NIST SP 800-171r1
• Work across functions
  – IT, Info Security, Contracts, Supply Chain, (Engineering, Quality)
• Designate Business Point of Contact
  – Coordinate collection of existing practices, tools, standards
  – Map systems architecture and CDI data flow
  – Lead cross-org analysis of requirements, gaps in compliance, review of new standards
• Understand what CDI AND Federal Contract Information is associated with your contract and what systems it applies to
  – Evaluate “covered contractor information system” use, risk, and impact
    • Which unclassified systems, what data, and who’s managing it (various roles)
    • Integrate with Risk Management
  – Identify CDI and DFARS use cases, so that
    • Your new standards are compliant and support the business
    • Employees know their role(s) and responsibilities
Additional Resources

• https://ics-cert.us-cert.gov/Assessments
• http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
• http://www.codsia.org/
• The DoD Cyber Security Strategy
• KPMG Advisory Report “The five most common cyber security mistakes”
• SBA’s link for 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
• US Cert’s Page for Small and Medium Size businesses 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.
• FTC’s Start with Security: A Guide for Business
This guide developed by the Federal Trade Commission offers 10 practical lessons businesses can learn from the FTC's 50+ data security settlements. Visit https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business to download the guide, access videos, and more.
• www.NIST.gov/MEP/
• www.fbi.gov
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
Continued discussion, unresolved challenges

• COTS exemption (solicitation vs sub)
• Marking of CDI by the customer, or current lack thereof
• CUI registry (are business systems now back in scope?)
• FedRamp applicability for CSP’s (vs applicability of 800-171)
• POA&M for controls not in place by 12/31/17?
• Interpreting “in support of performance of the contract”
• Submittal of deviations/waivers to controls to next higher tier
• What to do with non-compliant suppliers
• DCMA/DCAA audit
• Advocacy plan
Why and how **YOU** are a target

**Why**
- Custodian of DoD data and your proprietary data used to make DoD products
- Threat actors targeting the supply chain (viewed as less secure than prime contractors)
  - *July 6, 2016, House Committee on Small Business Chairman, Steve Cabot, brought up the risk of cyber-threats on small businesses. Although foreign actors are a major threat, 71% of cyber-attacks happened to businesses with less than 100 employees.*

**How**
- Top 4 (based on insight into supply chain incidents)
  - Spear Phishing, Look to leverage:
    - current events (e.g., funny super bowl ads)
    - business/personal relevant topics (e.g., shipping receipt, industry newsletter)
    - organizational or “sender” trust (e.g., from “IT Dept.” or company executive)
  - Credential Harvesting
  - Unsecure perimeter Devices (e.g., running old OS, unpatched systems, etc.)
  - Social media
    - Facebook friend requests
    - LinkedIn
- Insider Threats
- APTs (Advanced Persistent Threats)
- Distributed Denial of Service
- Malware
- Password Attacks

Optional for Internal Training
Possible results of insufficient/inadequate cyber security practices to your products, services, supply chain?

• Product safety
• Product merchantability/degraded performance
• Intellectual Property Loss
• Operational disruption
• Ransom payments
• Insider Threats
• Personally Identifiable Information (PII) loss
• Financial Information Compromise
• Legal liability
• Inability to compete for future work
• Remediation Costs
• Reputation/Brand damage

Optional for Internal Training
CUI Registry

• [http://www.archives.gov/cui/registry/category-list.html](http://www.archives.gov/cui/registry/category-list.html)

• Administered by National Archives and Records Administration

• Controlled Technical Information
  – Marked with distribution statements B – F
  – Does not include “FOIA”able information
  – R&D Engineering data & drawings, specs, standards, process sheets, manuals, technical reports, tech orders, catalog-item ID, data sets, studies & Analysis, source code
## DFARS Subpart 204.73 and DFARS Clause 252.204-7012

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Published November 18, 2013</td>
<td>Published August 26, 2015</td>
</tr>
</tbody>
</table>
| • Applies to contracts and subcontracts/Requires safeguarding of company’s internal systems with unclassified controlled technical information | • Selected security controls in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations | • Removes requirement for COTS  
• Refines definition of CDI |
| • Applies to contracts and subcontracts/Requires safeguarding of company’s internal systems with covered defense information | • Security requirements in NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations | |
| • Security requirements in NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations | | |

[Source: aia-aerospace.org]
Protecting the DoD's Unclassified Information...

Information System Security Requirements

Contractor’s Internal System
- Security requirements from NIST SP 800-171/DFARS, Clause 252.204-7012 apply
- Federal Contract Information
- Covered Defense Information
- Controlled Unclassified Information (USG-wide)
- Covered Defense Information (includes Unclassified Controlled Technical Information)

Contractor System Operated on Behalf of the DoD
- Cloud Service Provider
  - When CSP is operated on behalf of the DoD, the DoD Cloud Computing SRG applies

DoD Information System
- Security requirements from CNSSI 1253, based on NIST SP 800-53, apply
- DoD Owned and/or Operated Information System
- Cloud Service Provider
  - When CSP is operated by the DoD, the DoD Cloud Computing SRG applies

Unclassified

aia-aerospace.org
<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>
</tbody>
</table>
Types of Unclassified Information Systems

- Contractor’s Internal Information System
- DoD Information System
  - DoD Owned and/or Operated Information System
  - Contractor System Operated on Behalf of the DoD

Types of Unclassified Information

- Covered Defense Information (to include Unclassified Controlled Technical Information)
  - August 26, 2015 and December 30, 2015, DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services (interim rule) (80 FR 51739 and 80 FR 81472)
- Controlled Unclassified Information (CUI)
- Federal Contract Information
  - May 16, 2016, FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems (81 FR 30439)