SAME - Fort Bragg Post

System Security Requirements for Federal Contractors

Joseph Dickinson
Jackson Moore
David Hayden

EXPECT EXCELLENCE®
Agenda

• Safeguarding Clause (FAR 52.2013-13)
• DFARS Cybersecurity Clause (DFARS 252.204-7012)
• NIST SP 800-171
• Cyber Incidents - Reporting and Damage Assessment
• Developing a Culture of Security
FAR 52.204-21 - Basic Safeguarding

- Basic safeguarding measures
- 15 Basic Security Controls
- Applies to contractor systems that interface with “federal contract information”
  - “Federal contract information”:
    - Information provided by the Government
    - Information generated for the Government
    - But not otherwise publicly available information
- Include when contractor or subcontractor at any tier may have “Federal contract information” residing in or transiting through its information system. FAR 4.1903.
FAR 52.204-21 - Basic Safeguarding

• Covered contractor information system: information system owned/operated by contractor that processes, stores, or transmits Federal contract information. (FAR 52.20421(a))
FAR 52.204-21 - 15 Security Controls

1) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

2) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

3) Verify and control/limit connections to and use of external information systems.

4) Control information posted or processed on publicly accessible information systems.

5) Identify information system users, processes acting on behalf of users, or devices.
FAR 52.204-21 - 15 Security Controls

6) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

7) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

8) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

9) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

10) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
FAR 52.204-21 - 15 Security Controls

11) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

12) Identify, report, and correct information and information system flaws in a timely manner.

13) Provide protection from malicious code at appropriate locations within organizational information systems.

14) Update malicious code protection mechanisms when new releases are available.

15) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
DFARS 252.204-7012

- DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Required in all solicitations except COTS (DFARS 252.7304)
  - Mandatory to safeguard
  - Must be flowed down
- Originally published in 2013, mandatory 2018
- Applies to “covered contractor information system” but different definition from FAR: CCIS is unclassified system owned/operated by contractor that processes, stores, or transmits “covered defense information.”
DFARS 252.204-7012

- “Technical Information” - Technical data, software
- “Controlled Technical Information” - Technical Information with military or space application
- “Covered Defense Information” - Unclassified controlled technical information or other information on the CUI registry that requires safeguarding or dissemination controls and is EITHER:
  - Identified by DoD and provided to contractor; OR
  - Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor “in support of the contract”
NARA CUI Categories/Subcategories

- Agriculture
- Controlled Technical Information
- Critical Infrastructure (7)
- Emergency Management
- Export Control
- Financial (9)
- Geodetic Product Information
- Immigration (7)
- Information Systems Vulnerability
- Intelligence (6)
- International Agreements
- Law Enforcement (16)

- Legal (11)
- Natural and Cultural Resources (3)
- NATO
- Nuclear (6)
- Patent (3)
- Privacy (8)
- Procurement and Acquisition (2)
- Proprietary Business Information (5)
- SAFETY Act Information
- Statistical (3)
- Tax
- Transportation (2)
DFARS Compliance NIST 800-171

- NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Requires a system security plan:
  - Describe the system boundary
  - Operational Environment
  - Implementation of Requirements
  - Relationships/Connections to Other Systems.
  - Develop Plan of action regarding how requirements will be met and risks mitigated
- DoD Guidance: There is no one way to implement NIST 800-171 or for a contractor to assess its own compliance with those requirements
14 Categories for System Security Plan

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

- Review for evidence of compromise (identifying the affected computers, data, and accounts)
- Notify the DoD within 72 hours
- Preserve and protect images of affected information systems for 90 days
- Provide DoD with access to all information and equipment if DoD requests so it can conduct its own forensics
How Do Cyber Incidents Happen?

- **External Attacks**
  - Hacking the perimeter (SQL, XSS, FTP, WiFi...)
  - Phishing, Ransomware
  - Email spoofing, W-2 Spoofs

- **Internal Attacks**
  - Trusted business partners
  - Non-employee

- **Insider Attacks**
  - Disgruntled employees
  - Defecting employees

- **Mistakes**
  - Records disposal
  - Accidental Email
- Know your data - data map
- What information do you have?
- Know who you share data with?
- What is your incident response plan?
Sources of Risk

- Cloud?
- Data Flow?
- Vendor vetting and management
- Evaluate cloud vendor security measures

**Contract Provisions**
- Data protection and rights
- Legal Limitations - US? GDPR?
- Breach notice
- Risk allocation
- Increase/decrease legal/regulatory obligations
System Security Plan

- Culture? Demonstrated priority?
- Build Cybersecurity into Ethics and Compliance Program.
- Require employees to complete Cyber Security Awareness Training at least annually
- Make Cyber Security EVERYONE’s responsibility
- Cyber Insurance
Security Plan Common Themes

• Risk Assessments/Risk Analysis (Privacy Impact Assessment PIA)
• Designated Person of Responsibility
• Training of Employees
• Sanctions for Violations
• Regularly Updated Policies/Procedures
• Regular audits
• Incident Response Plan
• Access Management/Logging
• Document, Document, Document
Joseph Dickinson  
(919) 821-6782  
jdickinson@smithlaw.com

David Hayden  
(919) 821-6755  
dhayden@smithlaw.com

Jackson Moore  
(919) 821-6688  
jmoore@smithlaw.com

Smith Anderson Law Firm  
150 Fayetteville Street, Suite 2300  
Raleigh, North Carolina 27601
State Breach Notice Laws

- 48 States and the District of Columbia
- Must notify where unauthorized access to “personal information” has occurred or is likely to occur
- Outsourcing does not negate legal responsibility
- In addition: federal notification obligations
Response

- Counsel and forensic experts
- Regulatory and technical analysis
- Notification process
- Remediation efforts
- Regulator and consumer questions
Who Else is Responsible?

Pending: a Stricter North Carolina Bill?
Data Security Insurance?

- Hard copy documents?
- Regulatory actions and fines?
- Derivative claims?
Defending Claims After the Breach
State Law and Triggers for Notice

- **Some Primary Drivers**
  - Where the company conducts business
  - Where affected individuals reside

- **No common definition of “Breach”**
  - Incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. N.C. Gen. Stat. §75-61(14)

- **Proving the negative**
What’s the Cost?

- **Financial**
  - Incident Response
  - Lawsuits and Enforcement
  - Decreased Sales

- **Reputational**
  - Bad Publicity
  - Embarrassing Facts
  - Customer Attrition

- **Business Interruption**
  - Reduced Focus on Core Business
  - Restoration and Remediation
  - Loss of Key Business Members (CEO, CIO, CISO ...)

**EXPECT EXCELLENCE®**
Costs by Industry

Figure 5. Per capita cost by industry classification
*Historical data are not available for all years
Measured in US$