BakerHostetler

Updates in Government Contracting: Cybersecurity and Country-of-Origin

W. Barron A. Avery

February 5, 2019

BakerHostetler

Information Security in Government Contracts

Cybersecurity in Government Contracting – New Standards

BakerHostetler

- New Global Standard
  - FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
  - Applicable to all federal contractors
- New Military Contract Standard
  - DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Applicable to all defense contractors

BakerHostetler

Cybersecurity in Government Contracting—Common Concepts

- Key Concepts in FAR/DFARS Clauses:
  - "Information"
  - "Information System"
  - "Covered Information"
  - "Covered Contractor Information System"
- Technical Definitions Differ, but Core Concepts are Similar

BakerHostetler

Cybersecurity in Government Contracting – The FAR Clause (FAR 52.204-21)

- Basic Safeguarding Standards for (Almost) All Contractors
  - Includes 15 performance-based security safeguards that contractors must implement to protect their covered information systems.
  - "Common Sense" Safeguards
    - Limiting System Access
    - Sanitizing/Destroying Media
    - Limiting Physical Access
    - Escorting Visitors
    - Monitoring, Controlling Communications
- FAR Clause Does Not Override Specific Security Requirements
- Flowdown Requirement – Subcontractors!

BakerHostetler

Cybersecurity in Government Contracting – The DFARS Clause (DFARS 252.204-7012)

- Detailed Safeguarding Standards for Military Contractors
  - Contractors must provide "adequate security," which includes implementation of NIST SP 800-171
  - Contractors must report cyber incidents to the government
  - System Security Plan must be prepared
- National Institute of Standards and Technology (NIST) SP 800-171
  - 100+ Performance Based Metrics
    - Limiting System Access
    - Training organizational personnel
    - Maintaining system audit records
    - Performing regular risk assessments
- Deadline for Compliance: December 31, 2017

BakerHostetler

Cybersecurity in Government Contracting – Practical Considerations and Conclusion

- Compliance Risk Is Higher
  - Higher Profile
  - Increased Investigations
    - Investigations in First Instance
    - Investigations Increased Scope
- Self-Assessments Are Key
- Consider Variance Requests
- Take Incident Reporting Seriously

BakerHostetler

Supply Chain Developments in Government Contracting

Introduction

- Federal Government Has Placed Increasing Emphasis on Information Security in Recent Years
  - FAR 52.204-21
  - DFARS 252.204-7012
- Emphasis Shifting from Network Security to Supply Chain Risks
  - DFARS 252.246-7007 (Counterfeit Electronic Parts)
  - Supplier Blacklists

Russia & China

- Kaspersky Lab
  - 2018 National Defense Authorization Act
  - Interim Rule Published on June 15, 2018
- Huawei, ZTE
  - 2019 National Defense Authorization Act
  - Rulemaking Pending

“Do Not Buy” List

- Internal List Developed by Department of Defense to Identify Compromised Vendors
- First Reported in Summer 2018; No Current Plans to Make Public

Questions?

W. Barron A. Avery
Partner

Baker Hostetler LLP
202.861.1705
wavery@bakerlaw.com

BakerHostetler

Atlanta
Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Philadelphia
Seattle
Washington, DC

www.bakerlaw.com