CYBERSECURITY FOR CONTRACTORS

Evan Wolff
Paul Rosen
Kate M. Growley (CIPP/US)
Today’s Curriculum

• Introduction to Cybersecurity
• Cyber Contracting Clauses and Provisions
• Information Sharing Arrangements
• Responding to Incidents
Introduction to Cybersecurity

• Overviewing the threat environment
  – Nation state actors
  – Economic espionage
  – Insider threats
    • Malicious and negligent
  – A word about ransomware
Introduction to Cybersecurity

- Key cybersecurity concepts
  - Goals: Confidentiality v. Integrity v. Availability
  - Methods: Administrative v. Technical v. Physical
  - Multi-stakeholder approach
    - This is not just an IT issue!
  - Managing up and down the supply chain
    - Security is all about the lowest common denominator.
Introduction to Cybersecurity

• Key cybersecurity standards
  – NIST = National Institute of Standards & Technology // SP = Special Publication
  – NIST SP 800-53 Rev. 4
    • Security standard for federal agency systems
    • Applicable when acting as an extension of your customer
  – NIST SP 800-171 Rev. 1
    • Security standard for contractor systems with federal information
    • Applicable when using your own systems to handle customer information
Cyber Contracting Clauses and Provisions

• Common cyber clauses
  – FAR 52.204-21 (JUN 2016), *Basic Safeguarding of Covered Contractor Information Systems*
  – Mandatory in all contracts
  – Requires protection of “Federal contract information” residing on their information systems
  – Requires protection via 17 controls pulled from NIST SP 800-171
Cyber Contracting Clauses and Provisions

• Common cyber clauses
  – DFARS 252.204-7012 (OCT 2016), Safeguarding of Covered Defense Information and Cyber Incident Reporting
    – Requires protection of “covered defense information”
    – Requires protection via all 110 controls in NIST SP 800-171
Cyber Contracting Clauses and Provisions

• Common cyber clauses
  – DFARS 252.204-7012 (OCT 2016), *Safeguarding of Covered Defense Information and Cyber Incident Reporting*
  – Also requires reporting of incidents affecting either “covered defense information” or “operationally critical support”
  – Also requires subcontractor flowdowns when applicable
Cyber Contracting Clauses and Provisions

- Common cyber clauses
  - Pending FAR clause focused on “controlled unclassified information”
  - Expected to largely mirror DFARS Safeguarding Clause
  - Expected to be proposed in the next few months
Cyber Contracting Clauses and Provisions

• Like DoD, many agencies have their own supplemental cyber clauses
  – Homeland Security → “HSAR”
  – State Department → “DSAR”

• And the customer can set a higher floor
  – Read your SOW/PWS!
  – But don’t be afraid to push back.
Information Sharing Arrangements

- Defense Industrial Base (DIB) Cybersecurity Information Sharing Program
- Information sharing & analysis centers (ISACs)
- Information sharing & analysis organizations (ISAOs)
Responding to Incidents

- Investigations
  - Internally led
  - Led by your customer (or their delegate)
- Notifications
  - Mandatory and voluntary
- Engaging with law enforcement
- Remediation and after-action reviews
QUESTIONS?

Evan Wolff  
ewolff@crowell.com  
(202) 624-2615

Paul Rosen  
prosen@crowell.com  
(213) 443-5577

Kate Growley  
kgrowley@crowell.com  
(202) 624-2698