CYBERSECURITY’S ROLE IN THE EVOLUTION OF THE FOURTH PILLAR WITHIN FEDERAL ACQUISITIONS

Presented by CohnReznick’s: Bhavesh Vadhani, CISA, CRISC, CGEIT, PMP, Principal and Jeff Shapiro, CPA, Senior Manager

October 16 and 17, 2018
BEFORE WE BEGIN

This presentation has been prepared for information purposes and general guidance only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice.

No representation or warranty (express or implied) is made as to the accuracy or completeness of the information contained in this publication, and CohnReznick LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

This presentation and its content are the property of CohnReznick LLP and are protected by applicable copyright laws. Any unauthorized use of the information herein will be considered a violation of CohnReznick LLP’s intellectual property rights. Unless stated otherwise herein, no part of this presentation may be copied, distributed, or published, in whole or in part, without the prior written agreement of CohnReznick LLP.
AGENDA

• Update on the DoD “Deliver Uncompromised” Initiative
• Requirements under FAR 52.204-21 and DFARS 252.204-7012
• Information technology security and the impact on adequate accounting systems
• NIST best practices including the new NIST for small businesses
• Effective Cyber Risk Program
• Prime contractor’s responsibility and flow downs to sub-contractors
• Impact of new state privacy laws
• Questions and Answers
UPDATE ON THE DOD “DELIVER UNCOMPROMISED” INITIATIVE
GAO IS CONCERNED!

Source: GAO High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

September 2018
DOD DELIVER UNCOMPROMISED

• Study by MITRE, August 2018

• Holistic strategic approach to supply chain security within DoD

• Proposes security as the new fourth pillar within defense acquisition (cost, schedule and performance are the current three)

• Transform security from a cost center to a profit center

• “Products free of compromise represent more value than compromised products and have reduced total cost of ownership”
  – Think Healthcare.gov

• Reduce operational risk while applying positive incentives for companies to continuously examine and improve systems and practices
DOD DELIVER UNCOMPROMISED

Supply Chain risks exist across all phase of development.

Source: Center for Development of Security Excellence
DOD DELIVER UNCOMPROMISED – DELIVERED...?

MITRE report suggests:

• DOD work with industry to establish cyber/supply chain security standards/practices
  – NIST Revision 5 to SP 800-53
  – NIST Revision 2 to SP 800-37

• Security credentialing across all DOD Requiring Activities

• Careful scrutiny of System Security Plans (SSPs) during source selection (may involved being scored)
“Security is one of those measures that we need to hold people accountable for. And it shouldn’t be that being secure comes with a big bill. Like we wouldn’t pay extra for quality, we shouldn’t pay extra for security. We’re in a new world, and security is the standard, it’s the expectation, it’s not something that’s above and beyond what we’ve done before.”

- Deputy Secretary of Defense Patrick Shanahan
  September 19, 2018
GOVERNMENT CONTRACTORS – WHY SHOULD YOU CARE?

• Many instances the “Gateway” to government information and data - sensitive and non-sensitive
• Sometimes manage government agency systems, networks, programs, and data
• Varied and diverse industry based offerings
• Reputational risk
• Contractual obligations and risks
• Financial impact and penalties
• General business risks
• “Walk the Walk and Talk the Talk”
• Aftermath of data breaches could lead to cure notices, adverse past performance, fee reduction penalties, and possibly civil False Claims Act (FCA) implications, as well as reputational risk and responsibility issues which could lead to loss of awards.
CYBERSECURITY REGULATIONS
YOU NEED TO BE AWARE OF
SOME APPLICABLE REGULATIONS

• FAR 52.204-21 (Applies FAR 4.19 requirements)

• DFARS 252.204-7008 - Compliance with Safeguarding Covered Defense Information Controls

• DFARS 252.204-7012

• Federal Risk and Authorization Management Program (FedRAMP) - standardized approach to security for the cloud

• Federal Information Security Modernization Act of 2014 (FISMA)
FAR 52.204-21: BASIC SAFEGUARDING- COVERED CONTRACTOR INFORMATION SYSTEMS

• Imposes 15 “basic” security controls on “systems” holding Federal Contract Information (FCI) (not the information itself like DFARs);

• “Information not intended for public release, provided by or generated for the government under product or service contract”;

• Covers all Federal contractors since (i) it covers systems which “may” hold FCI & (ii) the safeguarding is “most basic” protection.

• Examples:
  – Limit controls to authorized users,
  – Verify controls on external connections,
  –Authenticate users, processes & devices before access,
  – Escort and monitor visitors,
  – Perform periodic scans of system and files, and
  – Update malicious code protections
  – [Note: No cyber incident reporting or audit requirements]
WHAT IF...?

• What if there was any inadvertent release of information that could be turned into not only an information security issue but also a violation of FAR 52.204.21 (and therefore be a breach of contract)?

• “Generally, as long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract” - 81 Federal Register 30444
DFARS 252.204-7012: NETWORK PENETRATION - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

- Covered Defense Information (CDI): Unclassified controlled technical information (UCTI) or Controller Unclassified Information (CUI) (i) marked or identified by USG as provided to contractor or (ii) collected, developed, stored, transmitted, processed, or used by contractor in contract performance;
- Excludes commercial-off-the-shelf (COTS) contracts (+ basic research);
- Contractor information systems must satisfy NIST SP 800-171
- Cyber incident reporting within 72 hours of discovery directly to DoD Cyber Crime Center (DC3) with DoD reporting code to prime contractor;
  - Acquire DoD approved medium assurance certificate to communicate with DC3 regarding the cyber incident
- Post Cyber Incident audit requirements;
- Flows down to lower tier subcontractors if CDI retains characteristics;
- If external Cloud Service Provided (CSP) to be used, the CSP must meet FedRAMP “moderate” security requirements + cyber incident reporting/audit requirements.
DFARS 252.204-7012: NETWORK PENETRATION - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

System Security Plan (SSP)
• Defines system boundaries
• Details security controls
• Described relationships or connections to other systems

Plan of Action and Milestones (POAM)
• Management tool for tracking the mitigation of cyber security program and system level findings/weaknesses
• Used to correct security deficiencies
• Used for reducing or eliminating vulnerabilities in organizational systems

Both may be needed for pre-award evaluation by DoD

POAM achievements may be monitored by DOD post-award
IT SECURITY IN COMPLIANT ACCOUNTING SYSTEMS

• DFARS 252.242-7006(c) Criteria 1 - “Sound internal control environment”

• Information Technology General Controls audit

• Non-compliances seen (some cause failure, some cause consideration for failure):
  – Accounting software on outdated server
  – Network/Software user access not reviewed frequently enough or improper assignments
  – Insufficient testing evidence of firewall protection (penetration testing)
  – Passwords not updated frequently enough
  – Change Management
  – Multi-Factor Authentication
  – Configuration Management
  – Privileged Account Access
WHAT’S ALLOWING SECURITY ISSUES TO PERSIST?

Generally weak security standards
• Up until recently - security was often an afterthought

Focus on Perimeter Security
• Relatively little monitoring detection and prevention at endpoints
• Ignoring where sensitive data actually resides

Security Awareness
• People are the weakest link of all
NIST 800-171 CONTROL FAMILIES
KNOW THE IT ENVIRONMENT

- Know the system(s) that support the services and contract
- Systems used to collect, develop, transmit, process, store, or use data for contract performance
- Develop a system boundary
- For cloud based applications, verify if the cloud solution is FedRAMP (Moderate) level accredited
WHAT WE HAVE SEEN: TOP WAYS HACKERS OBTAIN DATA

- Social Engineering
- Unpatched / legacy firewalls and operating systems
- Excessive Administrative rights on endpoints/servers
- Excessive access provided to normal business users
- Sensitive data not protected adequately
- Weak Credentials
- Insecure Password Storage (clear text)
- Outdated network and perimeter security
EFFECTIVE CYBER-RISK PROGRAM

- Strong Governance
  - Clearly defined governance structure
  - Roles and responsibilities
  - Policies and procedures
  - Holistic understanding of people, processes, and technologies
  - Periodic monitoring/health check

- Inventory of systems, environment including the data

- Regular internal and external vulnerability scans and penetration testing

- Security Incident Response and Reporting plan

- Adequate risk management program with effective risk response strategy

- Adoption and implementation of strong security controls
ROLES AND RESPONSIBILITIES

Board of Directors
- Oversee cyber strategy and monitor risks as part of the overall strategy and ERM

IT & Security
- Implement & Drive Conformance with cyber strategy

Business Units
- Provide Training & Education

Legal & Privacy
- Develop a good PR strategy and communication plan with regulators and external entities

Contracts
- Assure compliance with applicable cyber and privacy laws

Internal Audit
- Assure accountability and effective systems and controls

Finance
- Assure maximum efficiencies with limited dollars

Marketing & PR
- Ensure understanding of contract clauses
- Ensure third party (sub contractors) compliance
ROLES AND RESPONSIBILITIES

Board and C-Suite
- Know company's critical data assets and where they reside
- Understand key cyber threats including consideration of third party, subcontractor, and cloud exposure
- Include cyber risk in discussions of new and emerging business opportunities - major contracts; M&A activities; facilities expansions and IT initiatives
- Ask what mechanisms are in place to protect, detect, respond and recover from cyber incidents
- Agree on risk appetite, establish “tone at the top”, and understand monitoring activities

Contracts
- Understand and communicate requirements during procurement response cycle and on award
- Work with other business owners to understand and ensure compliance
- Consider subcontractor and third party requirements and compliance
ROLES AND RESPONSIBILITIES

Legal, Privacy, Compliance, and Security Officers
- Work with procurement and contracts to understand and support compliance efforts
- Update Board and management on existing and evolving legal and regulatory requirements including required reporting and disclosure to outside parties.
- Assess incident response program
- Advise on and develop appropriate external incident reporting

Finance
- On-going engagement with IT and other departments to assess and monitor exposure
- Manage costs (investment, allocation, etc.), and understand different disclosure requirements

Human Resources
- Contribute to development and assessment of training programs based on risk profiles
- Ensure on going training and communication
- Support tone at the top
ROLES AND RESPONSIBILITIES

Internal Audit
- Assist with risk identification and assessment
- Assess and report on management’s compliance with cyber risk program
- Support third party and subcontractor monitoring

IT
- Drive assessment and implementation of cyber risk program
- Stay current on emerging threats
- Provide open, ongoing reporting to executive management and board

Employees
- Attend training and understand responsibilities
- Comply with corporate policies and remain vigilant
- Communicate
**NIST CYBERSECURITY BEST PRACTICES SMB**

**Identify**
- Identify and control access to business information
- Conduct background checks
- Require individual user accounts
- Create policies and procedures for information security

**Protect**
- Limit employee access to data and information
- Install surge protectors and UPS
- Patch operating systems and applications
- Install and activate software and hardware firewalls on all business networks
- Secure wireless access points and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose old computers and media safely
- Train employees

**Detect**
- Install and update the following:
  - Anti-virus
  - Spyware
  - Malware
- Maintain and monitor logs

**Respond**
- Develop a plan for disasters and information security incidents

**Recover**
- Make full backups of important business data/information
- Make increment backups of important business data/information
- Consider cyber insurance
- Make improvements to processes/procedures/technologies
Focus on fundamentals first
PRIME CONTRACTOR’S RESPONSIBILITY AND FLOW DWONNS TO SUB-CONTRACTORS
PRIME CONTRACTOR RESPONSIBILITIES

• Pre-Award
  – As part of market research or maybe Teaming Agreement, bring up requirement for cybersecurity before teaming
  – RFP includes the FAR/DFARS or other relevant cybersecurity clauses

• At Award
  – Flow down FAR/DFARS/other relevant cybersecurity clauses
  – Consider having subs sign a Cybersecurity Self-Certification as a condition of award
PRIME CONTRACTOR RESPONSIBILITIES

• After Award
  – Talk about the extent of Cybersecurity which will be required at the kickoff meeting before work begins
  – Primes should be very clear in marking information as to whether it is covered or not covered content per the cybersecurity clauses during the course of the contract
  – For subs receiving very secure information, consider sending IT personnel to review the sub’s IT system and controls, if practicable

• Closeout
  – Ensure all covered information is treated according to the cybersecurity clause(s). Get a statement from the sub certifying to that effect.
HOW MUCH WILL THIS ALL COST?

It Depends
IMPACT OF NEW STATE PRIVACY LAWS
DATA BREACH NOTIFICATION AND PRIVACY LAWS

All 50 states currently have some form of data breach notification law in effect.

- California is the first state to pass a law related to Consumer Privacy
  - California Consumer Privacy Act (CCPA) passed in June 2018 applies to businesses that collect information from California residents and meet at least one of the following thresholds:
    1. have over $25 million in annual gross revenue; or
    2. buy, receive, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
    3. derive 50 percent or more of their revenue from the sale of consumers’ personal information

<table>
<thead>
<tr>
<th>States with Amendments or New Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama (SB 138)</td>
</tr>
<tr>
<td>Arizona (HB 2145)</td>
</tr>
<tr>
<td>Colorado (HB 1128)</td>
</tr>
<tr>
<td>Iowa (HF 2354)</td>
</tr>
<tr>
<td>Louisiana (Act no. 382)</td>
</tr>
<tr>
<td>Nebraska (LB 757)</td>
</tr>
<tr>
<td>Oregon (SB1551)</td>
</tr>
<tr>
<td>South Carolina (H4655)</td>
</tr>
<tr>
<td>South Dakota (SB No. 62)</td>
</tr>
<tr>
<td>Vermont (H. 764)</td>
</tr>
<tr>
<td>Virginia (HB 183)</td>
</tr>
</tbody>
</table>
QUESTIONS & ANSWERS
FOLLOW US ON TWITTER & VISIT US AT GOVCON360.COM
CONTACT

**Bhavesh Vadhani, CISA, CRISC, CGEIT, PMP**
Principal
Technology Risk and Compliance Leader, CohnReznick Advisory
Tysons, VA

📞 703-847-4418  📧 Bhavesh.Vadhani@cohnreznick.com

**Jeffrey L. Shapiro, CPA**
Senior Manager
Government Contracting Industry Practice
Tysons, VA

📞 703-286-1709  📧 Jeff.Shapiro@cohnreznick.com