Supply Chain Symposium: Cyber Security Requirements: What All Prime Contractors and Subcontractors Must Know

C. Joël Van Over
Travis L. Mullaney

pillsbury

PUBLIC CONTRACTING INSTITUTE

What is Cyber?

- **“Cyber”** is a common prefix referring to various concepts surrounding the electronic storage and transmittal of information, including the following:
  - Cyberwarfare;
  - Cyberspace;
  - Cybersecurity;
  - Cyber espionage;
  - Cyber threat; and
  - Cyber attack.
- Cyber risks are unique because they change quickly and can be executed by almost anyone, from anywhere, and at any time

pillsbury

PUBLIC CONTRACTING INSTITUTE

WHY CYBERSECURITY MATTERS

- OPM Data Breaches
  - Two separate breaches compromised data of 22.1 million people
  - SF-86 Forms – everything from SSNs to fingerprints
- IRS Exploit
  - Access granted to tax forms of 330,000 people
- Whitehouse, Pentagon infiltrations

pillsbury

PUBLIC CONTRACTING INSTITUTE

WHY CYBERSECURITY MATTERS

- Insider Leaks
  - Chelsea Manning
  - Edward Snowden
- Other Notable Breaches
  - Sony Pictures Entertainment
  - Target
  - Home Depot
  - J.P. Morgan Chase
  - Ashley Madison
- Demonstrated hacks of everything from cars to rifles

pillsbury

PUBLIC CONTRACTING INSTITUTE

WHY CYBERSECURITY MATTERS

- Three Primary Sources of Cyber Threats
  - (1) Insiders and former disgruntled employees
  - (2) Loosely affiliated hackers / criminal networks
    - E.g., Anonymous
  - (3) Advanced Persistent Threat
    - Typically a foreign government, with the capability and intent to persistently and effectively target a specific entity

pillsbury

PUBLIC CONTRACTING INSTITUTE

WHY CYBERSECURITY MATTERS

- The cyber threat – whether internal or external – includes:
  - Unauthorized access to and/or distribution of confidential, sensitive information, and/or intellectual property
  - Potential liabilities to third parties and reputational damage:
    - Loss or disruption of intellectual property, R&D and company operations;
    - Embarrassing public revelation of sensitive internal communications; and
    - Exposure to class action suits, litigation threats from state Attorney Generals, regulatory fines, and other financial and reputational harms.

pillsbury

PUBLIC CONTRACTING INSTITUTE

WHY CYBERSECURITY MATTERS

- Cybersecurity Compliance Issues:
  - Understanding compliance requirements
  - Risk management: balancing risk of loss against resources req'd
  - Establishing and maintaining compliant systems
  - Recognizing/discovering cybersecurity incidents
  - Responding/reporting requirements
  - Supply chain compliance
  - Impacts of compliance failures
  - Public relations impacts

pillsbury

PUBLIC CONTRACTING INSTITUTE

Cybersecurity Compliance: Reactive v. Proactive

- Reactive:
  - Involve incident response team and investigate
  - Consult with counsel to assess contract and compliance obligations/conduct investigation
    - Cyber insurance coverage/obligations
    - State law breach reporting
  - Have system administrator/IT security expert maintain/preserve log of what occurred
    - Detection, preservation, and recovery efforts, response team
  - Assess lessons learned and materiality
    - Add breach impact to risk assessment for necessary protection
    - Implement corrective actions as needed to prevent recurrence

pillsbury

PUBLIC CONTRACTING INSTITUTE

Cybersecurity Compliance: Reactive v. Proactive

- Proactive:
  - Conduct compliance reviews of systems
    - Baseline against Framework, contract-specific requirements
    - "Check the box" versus risk-based threat assessment
  - Consider cyber insurance, understand exclusions (e.g., negligence)
  - Implement training programs for employees
  - Establish cyber incident response plan to prepare for a cyber attack
  - Identify a cross-functional team within company
    - IT, risk management, operations, legal and compliance
    - Management level support
  - Establish/update policies and procedures for new requirements
    - Update T's and C's to ensure protection from supply chain incidents

pillsbury

PUBLIC CONTRACTING INSTITUTE

GOALS OF THIS PRESENTATION

- Introduce recent federal cybersecurity developments
- Provide familiarity with requirements for compliance
- Identify opportunities for contractors in the cybersecurity space
- Forecast future developments

pillsbury

PUBLIC CONTRACTING INSTITUTE

Covered Topics

A. Cybersecurity Act of 2015

B. OMB Actions to Improve Cybersecurity

C. DoD Cybersecurity Regulations

D. Insider Threat Protections

E. FedRAMP

F. Opportunities for Contractors & Subcontractors

pillsbury

PUBLIC CONTRACTING INSTITUTE

A. Cybersecurity Act of 2015

- Consolidated Appropriations Act of 2015, Division N
  - Signed into law in December 2015
- Derived from draft Cybersecurity Information Sharing Act (CISA)
- Primary goal is to facilitate the exchange of information regarding cybersecurity threats between and among the federal government and the private sector

pillsbury

PUBLIC CONTRACTING INSTITUTE

A. Cybersecurity Act of 2015 (cont'd)

- DHS tasked with developing policies and procedures related to the receipt and sharing of cyber threat indicators and defense measures between the Federal Government and private entities
  - Goal is "real time" notification of cybersecurity threat information
- Cybersecurity Threat
  - "an action. . . on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."
- Cyber threat indicator
  - Information that its necessary to describe or identify a cybersecurity threat
  - E.g., security exploitations, vulnerabilities, malicious reconnaissance, etc.

pillsbury

PUBLIC CONTRACTING INSTITUTE

A. Cybersecurity Act of 2015 (cont'd)

- Protections for contractors engaging in sharing:
  - Government can't take adverse action against private entity based on information it receives
  - Private entities protected from liability for conducting activities in accordance with the act

pillsbury

PUBLIC CONTRACTING INSTITUTE

B. OMB Actions to Improve Cybersecurity

- OMB's Cybersecurity Strategy and Implementation Plan
- 5 Principal Objectives:
  1. Prioritized identification and protection of high value information and assets
     - Personal Identify Verification (PIV) credentials for employees and contractors with access to high value information
     - Current targets seek the implementation of 100% PIV for privileged users and 75% PIV for non-privileged users
  2. Timely identification of and rapid response to cyber incidents
  3. Rapid recovery from incidents when they occur and accelerated adoption of lessons learned

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB's Cybersecurity Strategy and Implementation Plan
- 5 Principal Objectives (cont'd):
  4. Recruitment and retention of the most highly-qualified cybersecurity workforce talent the federal government can bring to bear
  5. Efficient and effective acquisition and deployment of existing and emerging technology
     - Will require close partnerships with contractors to continue implementing cybersecurity solutions already underway and on the horizon
     - Significant opportunities for contractors to leverage experience

pillsbury

PUBLIC CONTRACTING INSTITUTE

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB guidance to improve cybersecurity protections in federal acquisitions
  - Published by Office of E-Government & Information Technology
  - Authority derives from:
    - Federal Information Security Modernization Act (FISMA)
      - OMB sets policies, DHS oversees compliance
    - OMB policy
    - National Institute of Standards and Technology (NIST) standards

Brief Aside Regarding NIST

- NIST standards contemplate “families” of security requirements
  - Access control
  - Awareness and training
  - Audit and accountability
  - Configuration management
  - Identification and authentication
  - Incident response
  - Maintenance
  - Media protection
  - Personnel Security
  - Physical protection
  - Risk assessment
  - Security assessment
  - Systems/communications protection
  - Systems/information integrity

pillsbury

PUBLIC CONTRACTING INSTITUTE

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB guidance to improve cybersecurity protections in federal acquisitions
- Key recommendations:
  - Security Controls
    - Baseline Standards:
      - For government systems: NIST SP 800-53
      - For contractor systems: NIST SP 800-171
      - Other NIST Standards may apply based upon the nature of the system (VPN, server security, etc.)
  - Cyber Incident Reporting
    - Contracts should specify to whom, what, when, and where cyber incidents should be reported

pillsbury

PUBLIC CONTRACTING INSTITUTE

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB guidance to improve cybersecurity protections in federal acquisitions
- Key recommendations (cont'd):
  - Information Systems Security Assessments
    - Agency impact assessment
    - Allowance for independent third-party verification of security assessment results
    - Contractors must provide access for audits related to information security incidents

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB guidance to improve cybersecurity protections in federal acquisitions
- Key recommendations (cont'd):
  - Information Security Continuous Monitoring
    - Agencies: DHS Continuous Diagnostics and Mitigation program (or at least meet M-14-03 requirements)
    - Contractors: Continuous monitoring in accordance with NIST SP 800-171

B. OMB Actions to Improve Cybersecurity (cont'd)

- OMB guidance to improve cybersecurity protections in federal acquisitions
- Key recommendations (cont'd):
  - Business Due Diligence
    - Utilization of GSA's business due diligence information shared service to evaluate risk information
    - Data collected from:
      - Voluntary contractor reporting
      - Public records
      - Publicly available data
      - Commercial subscription data

pillsbury

PUBLIC CONTRACTING INSTITUTE

C. DoD Cybersecurity Regulations

- DoD Interim Rule expanding DFARS provisions regarding Cybersecurity
- Cybersecurity Compliance and Incident Reporting
  - DFARS 252.204-7012
    - Mandates NIST 800-171 standards (or approved alternative) for safeguarding “covered defense information” on “covered contractor information systems”
    - 72-hour rapid reporting of cyber incidents
    - Required preservation of images of affected systems for 90 days
    - Mandatory flow-down to subcontractors

C. DoD Cybersecurity Regulations (cont'd)

- DoD Interim Rule expanding DFARS provisions regarding Cybersecurity
- Cybersecurity Compliance and Incident Reporting (cont'd)
  - DFARS 252.204-7009
    - Mandates conditions for handling and protecting information obtained from a third-party's reporting of a cyber incident and specifies potential penalties for the breach of these conditions
  - DFARS 252.204-7008
    - Mandates the procedures required for a contractor to justify and obtain DoD approval for alternative security measures that do not comply with NIST SP 800-171.

C. DoD Cybersecurity Regulations (cont'd)

- DoD Interim Rule expanding DFARS provisions regarding Cybersecurity
- Cloud Computing Services
  - DFARS subpart 239.76
    - Establishes DoD policy for the acquisition of cloud computing services
  - DFARS 252.239-7009
    - Requires offerors to check a box indicating whether it intends to use cloud computing services in the performance of the contract or a subcontract

C. DoD Cybersecurity Regulations (cont'd)

- DoD Interim Rule expanding DFARS provisions regarding Cybersecurity
- Cloud Computing Services (cont'd)
  - DFARS 252.239-7010
    - Must follow Cloud Computing Security Requirements Guide
    - Requires cyber incident reporting, preservation and cooperation in post-incident analysis
    - Mandatory flow-down to subcontractors, with no exceptions for small business or commercial items, if subcontract "may involve cloud services"

pillsbury

PUBLIC CONTRACTING INSTITUTE

C. DoD Cybersecurity Regulations (cont'd)

- DoD Cybersecurity Discipline Implementation Plan
  - Amended in Feb. 2016
- Four lines of effort:
  - Strong authentication – appropriate use of authentications / credentials
  - Device hardening – installing updates, ensuring proper settings / configurations
  - Reduce attack surface – eliminating unnecessary web connections
  - Alignment to cybersecurity / computer network defense service providers – agreements with accredited contractors

C. DoD Cybersecurity Regulations (cont'd)

- DoD Cybersecurity Discipline Implementation Plan (cont'd)
- DoD Cybersecurity Scorecard effort
  - Commanders and Supervisors report status with the requirements of the Implementation Plan via the Defense Readiness Reporting System
  - Scorecard effort allows SecDef to understand cybersecurity compliance at the strategic level by reporting metrics at the service tier

D. Insider Threat Protections

- Conforming Change No. 2 to National Industrial Security Program Operating Manual (NISPOM)
  - Sets the mandatory structural and process requirements for the protection of classified information to which properly cleared federal contractors and their employees have access in connection with classified contracts under the National Industrial Security Program (NISP)
  - Conforming Change No. 2 will outline insider threat requirements for cleared industry operating under the NISP

D. Insider Threat Protections (cont'd)

- Conforming Change No. 2 to National Industrial Security Program Operating Manual (NISPOM)
- Key elements:
  - Establishment of an insider threat program
  - Designation of an insider threat senior official who is cleared in connection with the facility clearance
  - Self-assessment of insider threat programs
  - Provision of training for insider threat program personnel and awareness of employees
  - Monitoring of network activity

D. Insider Threat Protections (cont'd)

- Conforming Change No. 2 to National Industrial Security Program Operating Manual (NISPOM)
- Potential contractor responsibilities:
  - 180 days to establish and implement insider threat program
  - Maintain records necessary to identify, analyze, and resolve insider threat matters
  - Active monitoring of network information systems
  - Handle access requests to insider threat information
  - Establish reporting guidelines

D. Insider Threat Protections (cont'd)

- Conforming Change No. 2 to National Industrial Security Program Operating Manual (NISPOM)
- Relevant information:
  - Counterintelligence and Security databases:
    - Personnel security files, polygraph records, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings
  - Information Assurance records:
    - Personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, etc.

pillsbury

PUBLIC CONTRACTING INSTITUTE

D. Insider Threat Protections (cont'd)

- Conforming Change No. 2 to National Industrial Security Program Operating Manual (NISPOM)
- Relevant information:
  - Human Resources data (cont'd):
    - Personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, etc.

pillsbury

PUBLIC CONTRACTING INSTITUTE

E. FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP)
- Government-wide program providing standardized approach to security assessment, authorization, and continuous monitoring for cloud products
- Developed through collaboration of General Services Administration (GSA), NIST, DHS, DoD, National Security Agency (NSA), OMB, the federal CIO Council and its working groups, and private industry groups

E. FedRAMP (cont'd)

- Advantages of gaining FedRAMP compliance
  - Mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels
    - Private cloud deployments intended for single organizations and implemented fully within federal facilities are the only exception
  - Clear standards for implementation
  - Certification of compliance through Authority to Operate (ATO)
  - Ability for multiple agencies to utilize cloud service providers (CSPs) after single authorization

pillsbury

PUBLIC CONTRACTING INSTITUTE

E. FedRAMP (cont'd)

- Apply directly or work with sponsoring agency
- FedRAMP Initiation Request
- Two ways for achieving authorization:
  - JAB Provisional Authorization (P-ATO)
  - Agency Authorization
- FIPS 199 worksheet – categorize data
- Develop System Security Plan

E. FedRAMP (cont'd)

- 3 step process for authorization of cloud system:
  - Step 1. Security Assessment
    - Must meet standardized requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations
    - Assessment conducted by Third Party Assessment Organizations (3PAOs)
    - 3PAO engaged directly by CSP
      - For JAB P-ATO, must use FedRAMP accredited 3PAO
      - For Agency Authorization, may use agency validated Independent Assessor
    - End product is Security Assessment Report, shared with contractor and agency

E. FedRAMP (cont'd)

- Apply directly or work with sponsoring agency
- 3 step process for authorization of cloud system (cont'd):
  - Step 2. Leveraging and Authorization
    - Federal agencies view security authorization packages in the FedRAMP repository and "leverage" the security authorization packages to grant a security authorization at their own agency
    - Agencies review Security Assessment Report and work with CSP to create Plan of Action and Milestones to address vulnerabilities
    - Decision to authorize formalized in ATO letter

E. FedRAMP (cont'd)

- 3 step process for authorization of cloud system (cont'd):
  - Step 3. Ongoing Assessment & Authorization
    - Post-authorization, ongoing assessment and authorization activities completed to maintain the security authorization
    - May also be conducted by 3PAOs / Independent Assessors
    - Three pillars:
      - Operational visibility
      - Change control process
      - Incident response

E. FedRAMP (cont'd)

- Opportunities for contractors as either CSPs or 3PAO / Independent Assessors
- To become an accredited FedRAMP 3PAO, must submit application materials demonstrating:
  - Technical competence in security assessment of cloud systems, and
  - Management requirements for organizations performing inspections
- The American Association for Laboratory Accreditation (A2LA) accredits FedRAMP 3PAOs with the FedRAMP PMO providing final approval.

E. FedRAMP (cont'd)

- Role of 3PAO / Independent Assessor is to:
  - Complete a Security Assessment Plan
  - Perform initial and period assessments of cloud system security controls
  - Conduct security tests and produce Secure Assessment Reports

E. FedRAMP (cont'd)

- Relation of FedRAMP to the new DOD cloud services regulations
  - FedRAMP compliance and authorization geared toward civilian agencies
  - Adoption of NIST 800-53 as versus NIST 800-171

pillsbury

PUBLIC CONTRACTING INSTITUTE

F. Opportunities for Contractors & Subcontractors

- Agencies are stepping up procurement of services related to cybersecurity assessment, protection, and monitoring
- Contractors that set up compliance systems now can potentially beat out non-compliant contractors for the same work

pillsbury

PUBLIC CONTRACTING INSTITUTE

Why is compliance and maintenance of system security so important?

- Risks to government contractors associated with a successful cyberattack include:
  - Suspension or termination of affected federal contracts
  - Risks to pending federal bids
  - Federal investigation into the cause of the cyberbreach and compliance with reasonable and contractual system security requirements
    - Investigation into whether detection of breach was timely and notice to government immediate
    - Cooperation will be evaluated
  - Congress may hold hearing, adverse press
  - Potential suspension or debarment

pillsbury

PUBLIC CONTRACTING INSTITUTE

Why is compliance and maintenance of system security so important? (cont'd)

- Examples:
  - U.S. Investigations Services (USIS)
    - Major government security clearance contractor
    - Lost significant business after breach
    - Parent company filed for bankruptcy
  - KeyPoint Government Solutions
    - Took over federal background checks after USIS was hacked
    - Attack on KeyPoint likely gave hackers the credentials needed to obtain access to OPM records
  - Both were investigated, many contracts were lost, jobs were lost at all levels, Congress held hearings, government agencies were also blamed, etc.

pillsbury

PUBLIC CONTRACTING INSTITUTE

Questions

C. Joël Van Over

Partner
Pillsbury Winthrop Shaw Pittman LLP
1650 Tysons Boulevard, 14th Floor
McLean, VA 22102-4856

703.770.7604
joel.vanover@pillsburylaw.com

Travis L. Mullaney

Associate
Pillsbury Winthrop Shaw Pittman LLP
1650 Tysons Boulevard, 14th Floor
McLean, VA 22102-4856

703.770.7751
travis.mullaney@pillsburylaw.com

pillsbury

PUBLIC CONTRACTING INSTITUTE