Supply Chain Security for Government Contractors

Addie R. Cliffe, Partner, Crowell & Moring LLP

Kate M. Growley, Partner, Crowell & Moring LLP

Overview

- Introduction to supply chain security risk management
- Current regulatory landscape
- What’s on the horizon?
- Risk mitigation best practices

Privileged & Confidential / Attorney-Client Communication / Attorney Work Product

What is supply chain security?

Supply Chain Security & Risks Defined

- FY2018: $4.1 trillion in federal government outlays funding broad array of programs and operations, including in areas of national security, national defense, and public health and safety
- “Supply chain risk management (SCRM) bridges expertise from acquisition, information management, logistics, intelligence, counterintelligence, security, and cyber to share threat assessments, vulnerabilities, and mitigation information.”
  - - ODNI, National Counterintelligence and Security Center

Supply Chain Security & Risks Defined

Key Risks

- The National Institute of Standards and Technology (NIST) has published guidance on supply chain risks and management.
- Key Risks include:
  - Third party service providers or vendors with physical or virtual access to information systems
  - Poor information security practices by lower-tier suppliers
  - Compromised software or hardware purchased from suppliers
  - Software security vulnerabilities
  - Counterfeit hardware or hardware with embedded malware
  - Third party data storage or data aggregators

Supply Chain Security & Risks Defined

- Includes both cyber risks and physical risks
- Other related areas of concern:
  - Physical security of facilities
  - Foreign ownership and influence of suppliers
  - Insider threats

Forces Driving Supply Chain Security to the Forefront

Deliver Uncompromised

- The threat is real
- Deliver uncompromised” grew out of concerns that contractors were delivering compromised capabilities to the DoD
    - Focus on cyber and supply chain security
    - Four primary attack vectors: (i) supply chain (software, hardware, services), (ii) cyber-physical (cyber systems with real-time operating deadlines including weapons systems and industrial control systems), (iii) cyber-IT (informational technology), and (iv) human domain (witting or unwitting; foreign intelligence service or insider)

Forces Driving Supply Chain Security to the Forefront

Deliver Uncompromised

- August 2018 MITRE Report: 15 recommendations on how USG and private sector can address growing threats, e.g.,
  - Recommending security as a fourth pillar in defense acquisition decisions (in addition to cost, schedule and performance), i.e., could go to evaluation decision
  - Educating senior leaders and improving coordination to take on supply chain threats
  - Recommending changes to contracting, monitoring, and program protection
  - Calling for a long-term commitment to incentivizing private sector participation
  - Institute industry-standard IT practices in all software developments
- DoD “deliver uncompromised” pilot program (FY 2018 NDAA, Section 1696)
  - Pilot program established June 1, 2019
  - Onus on contractors to deliver uncompromised products/services

Forces Driving Supply Chain Security to the Forefront

Given these concerns, there have been major developments / increased efforts to mitigate cybersecurity & supply chain risks

- Statutory and regulatory product and company-based exclusions
  - e.g., Kaspersky Lab, ZTE, Huawei bans
- Agency-specific internal supply chain & cyber restrictions
  - DHS supply chain cyber initiative
  - DoD prohibitions against procuring from National Security Systems Restricted List

KASPERSKY lab HUAWEI ZTE

The Future State of Supply Chain Security

- Security as the foundational element upon which the traditional 3 pillars of government procurement are built.

- In the short term, a failure to respond to the challenges will expose contractors to the financial consequences of noncompliance, as well as increased risk of exposure to liability under intersecting regimes.

- Ultimately, contractors must find a way to shift from managing the evolving landscape of compliance to pursuing competitive advantage.

Regulatory Landscape

Cybersecurity

Introduction to DFARS 252.204-7012

- DFARS 252.204-7012 (OCT 2016), Safeguarding of Covered Defense Information and Cyber Incident Reporting
  - Incorporated into all DoD contracts to protect sensitive DoD information
    - Formally referred to as covered defense information or “CDI”
  - Under the Clause, contractors must meet three primary requirements:

    (1) protect CDI residing on contractors’ networks,

    (2) rapidly report cyber incidents affecting CDI, and

    (3) flowdown these obligations to subcontractors handling CDI on the contractors’ behalves.
  - Mandatory in all DoD contracts and solicitations except exclusively off-the-shelf (COTS) items
    - Self-deleting where no CDI involved

Cybersecurity

-7012 Flowdown Requirements

- Contractors must flow down the Clause without alteration to subs whose performance requires CDI.
  - Usually requires proactive dialogue to determine what CDI may be necessary
- Contractors must also require subs to:
  1. Notify when submitting NIST SP 800-171 variance requests to DoD CIO
  2. Provide DoD incident report number upon cyber incident occurrence.
- Contractors may also negotiate separate terms into their subcontracts, e.g., access to full cyber incident reports.
- Contractors may <u>not provide CDI</u> to a subcontractor who has <u>not accepted the flowdown</u> or where there is reasonable evidence that sub is <u>not meeting the flowdown requirements</u>.

Cybersecurity

Cloud Service Provider (CSP) Requirements

- Separate requirements exist for external Cloud Service Providers that handle CDI:
  - CSPs must meet security requirements equivalent to Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline
  - Contractors must also require CSPs to:
    1. Comply with cyber incident reporting requirements
    2. Send malicious software to DoD Cyber Crime Center (DC3)
    3. Preserve and protect images of affected systems for 90 days
    4. Provide DoD access to information necessary for forensic analysis and damage assessment

Cybersecurity

Defense Contract Management Agency (DCMA)

- Authorities under Contractor Purchasing System Reviews (CPSRs) permit DCMA to:
  - Review contracts to determine if:
    - The Clause was appropriately flowed down to subcontractors;
    - CDI was properly marked for subcontractors (or proper instructions were provided);
    - The contractor can demonstrate how they determined subcontractors have a Covered Contractor Information System that can handle CDI, to include an adequate SSP;
    - CDI was adequately protected when transferring to subcontractors; and
    - DoD incident report numbers received from subcontractors are recorded.

Cybersecurity

Cybersecurity Maturity Model Certification (CMMC)

- CMMC, Version 1.0 sets forth the cybersecurity requirements to which all contractors must soon be certified to participate in the Department's supply chain.
- Third-party assessors ("3PAOs") will issue CMMC level-based certificates to contractors under the CMMC to certify contractor compliance with DoD cybersecurity requirements.
- Incorporates core themes from other cyber frameworks such as NIST 800 Series, NIST Cybersecurity Framework, ISO 27001, and CIS Critical Security Controls.
- CMMC breaks down cybersecurity standards into 5 levels, where each CMMC level is cumulative, meaning that the higher levels include all practices and processes for the levels below.
- The framework categorizes the practices into 17 domains, which are largely based off of the 14 control families of NIST SP 800-171, Rev. 1.
- Meeting the specified CMMC level will be a "go/no-go" condition to bidding on the contract.
- CMMC levels will begin to appear in RFIs in June 2020 and in RFPs by September 2020.

Foreign Sourcing and Ownership Restrictions

- FAR 52.204-23: prohibition on contracting for hardware, software, and services developed or provided by Kaspersky Lab
- FAR 52.204-24 and -25: prohibition on procurement of any equipment, system or service that uses covered telecommunications equipment or services from certain Chinese companies (including Huawei and ZTE)
- DFARS 252.204-7018: prohibition on procurement of telecommunications equipment, systems, or services from certain Chinese and Russian companies for critical technology for nuclear or homeland defense missions
- DFARS 252.225-7051: prohibition on procurement of satellite services from China, North Korea, Russia, or state sponsor of terrorism or related entities
- DFARS 252.225-7018: restriction on the acquisition of certain magnets and tungsten from China, Russia, and Iran

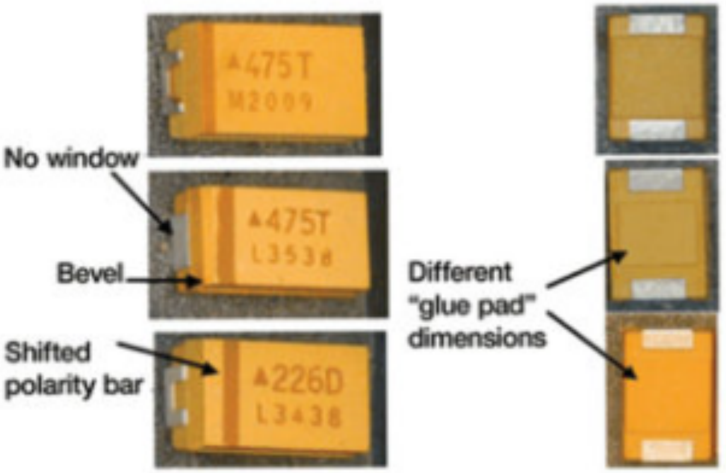
Foreign Sourcing and Ownership Restrictions

- FY18 NDAA Section 1069: requires DoD to assess and develop a plan and recommendations to improve interagency vetting of foreign investments that could affect national security, including reliance on foreign suppliers for materials essential to national defense.
- FY19 Section 1654: requires DoD to create a prioritized list of countries of concern related to cybersecurity based on government's hostility, intelligence activity, criminal activity, and willingness and ability to disrupt U.S. Government supply chain.
- FY19 Section 1655: establishes disclosure obligation and prohibitions where there is risk of foreign government influence over providers of IT products and services
- FY20 Section 224: DoD to develop microelectronics products and services Trusted Supply Chain and Operational Security Standards
- FY20 Secton 847: requires DoD to evaluate foreign ownership, control, and influence (FOCI) for contractors and subcontractors with contract over $5M by requiring disclosure of certain FOCI information and incorporation of FOCI evaluation into responsibility determinations (commercial items exempt).

Counterfeit and Nonconforming Parts

Screening and Reporting

- **FAR 52.246-26**: requires screening for and reporting counterfeit or suspect counterfeit parts and any critical or major nonconformances
- **DFARS 252.246-7007 and -7008**: avoidance and detection of counterfeit parts for electronic parts and components



Other Requirements and New Initiatives

- FAR 52.203-13: contractors required to report credible evidence of wrongdoing by suppliers, distributors, vendors, and provide training for agents and subcontractors "as appropriate"
- DFARS 239.73: allows DoD, for procurements for national security system or an item of IT that is purchased for inclusion in a national security system to exclude a source that: (1) fails to meet qualification standards for reducing supply chain risk; (2) fails to achieve an acceptable rating under supply chain risk evaluation factor; or (3) withhold consent for a subcontract.
  - DoD can limit disclosure of information relating to the basis for exclusion
  - If agency limits disclosure of information, action is not subject to bid protest review.

Other Requirements and New Initiatives

- Numerous NDAA provisions:
  - FY18 Section 807: requires DoD to establish a process for enhancing scrutiny of acquisition decisions to integrate supply chain risk management into overall acquisition decision cycle (including training for acquisition work force and coordinating with other U.S. agencies and international partners)
  - FY20 (Senate version)
    - Section 831: requires DoD to streamline and digitize the approach to identifying and mitigating supply chain risk across acquisition process
    - Section 10306: requires Director of National Intelligence to establish a Supply Chain and Counterintelligence Risk Management Task Force

Industrial Security

- Per DCSA guidance, cleared contractors being targeted for exploitation of global supply chain; requires cleared contractors to:
  - Recognize signs of compromised supply chain
  - Take countermeasures to mitigate supply chain security
  - Report to DCSA; *e.g.*,
    - Device exhibiting functionality outside of original design or exhibiting unique error
    - Attempts to break trusted chain of custody
- FY18 NDAA Section 1696: Requires DoD to establish a pilot program (prior to June 1, 2019) for information sharing with cleared DoD contractors for purpose of ensuring security and integrity of supply chain in programs related to nuclear weapons; nuclear command, control, and communications; continuity of government; ballistic missile defense; other command and control systems; and space systems.

Intersections with Existing Liability Regimes

- The flurry of supply chain security driven requirements is creating a host of new opportunities for the creation of FCA exposure
    - *E.g.*, New contract terms that must be flowed to suppliers, new restrictions on suppliers, new certification requirements
- Gaps and other growing pains to be expected
    - *E.g.,* Department of Defense Inspector General (DODIG) audit finding inconsistent implementation of NIST SP 800-171 and DFARS 252.204-7012
- Where potential gaps in security and/or contract compliance are identified, a new class of potential relators awaits, including those connected to third party suppliers
- Early example: *United States ex rel Glenn, et al v. Cisco Systems Inc*.

Intersections with Existing Liability Regimes

- Mandatory Disclosure Rule
  - Per FAR 52.203-13, contractors are required to report "credible evidence" of false claims and other wrongdoing by its suppliers, distributors, vendors; and provide training for agents and subcontractors "as appropriate"
  - Must be considered as supply chain is engaged to meet the challenges of security
  - Availability as a pro-active risk management tool
- Suspension & Debarment
- Lost Business
  - Agencies already incorporating cybersecurity into contracts and solicitations as technical evaluation factors and go/no-go criteria

Cases

- GAO and COFC have found that agencies have wide discretion in evaluating supply chain security risks
- ***Iron Bow Tech., LLC v. United States*, 136 Fed. Cl. 519 (2018)**
  - Iron Bow excluded from competitive range due to concerns with influence of Chinese government over U.S. supplier of printers
  - Court found agency appropriately documented risks and agency had wide discretion to exclude companies based on these risks given the criteria in the RFQ

What’s next?

Cyber Requirements on the Horizon

Pending Impacts to Supply Chain

- There are several pending cybersecurity requirements and regulations that, when enacted, will have new implications for supply chain management including:
  - NIST SP 800-171B (“Bravo”)
  - FAR Rule on Controlled Unclassified Information (”CUI”)

Cyber Requirements on the Horizon

NIST SP 800-171B ("Bravo")

- Currently in draft form
- Designed to protect CUI from advanced persistent threats (APTs)
- Will apply only to contractors handling CUI that the government determines is part of a "critical program" or is a "high value asset"
- Currently includes 33 "enhanced" controls, reflecting core principles of penetration resistance, damage-limiting operations, and resiliency
- Specific controls include those related to segregation/segmentation; hunt teams; AI-enabled monitoring tools; IoT security; and supply chain security
- Comments are currently being reviewed

Cyber Requirements on the Horizon

NIST SP 800-171B ("Bravo") Supply Chain Security Controls

- Two separate controls increase supply chain responsibilities for government contractors. The controls require contractors to:

  1) Assess and monitor supply chain risks associated with organizational systems; and
  2) Develop a plan for managing those supply chain risks.

- The Enhanced Requirements highlight the types of supply chain events that the government is focusing on that can impact information residing on contractor systems including:
  - use of defective components;
  - insertion of counterfeits;
  - malicious development practices; and
  - insertion of malicious code.

Pending Cyber Requirements

FAR CUI Clause

- Expected to mirror DFARS Safeguarding Clause and expand requirements to all civilian contracts
  - Resulting in similar flowdown requirements and broader supply chain impact
  - Greater prime contractor responsibilities possible due to DoD's increased reliance on prime contractor oversight
  - Latest timeline projects April 2020 publication
- Agency oversight will include 3 tiers, based on the sensitivity and/or volume of CUI handled by the contractor:
  - **Self-certification** through the contracting process.
  - Self-certification, plus supporting **documentation**, such as SSPs, POAMs, CUI training records, corporate safeguarding policies and procedures, etc.
  - Self-certification and documentation, plus **validation** through either a customer or third-party assessment.
- DFARS Safeguarding Clause revision anticipated after FAR CUI Rule implementation.

Pending Cyber Requirements

Reactions to Cyber Unknowns

- Will CMMC implementation replace flowdown requirements?
  - Certification by a DoD-accredited assessor provides a certain level of trust. As a result, a prime or higher-tier subcontractor may only have to maintain suppliers' certificates.
  - However, the risk lies in the chance that individual contract requirements may exceed current cybersecurity regulations.
- What other diligence will be necessary on the part of prime and higher-tier subcontractors?
- Will different CMMC levels be required of various contractors and suppliers within the same contract?
- The uncertainties within these pending regulatory regimes will require operational agility of contractors throughout the supply chain.

Supply Chain Liabilities

Foreseeable Risks

- Cybersecurity continues to be an increased liability in supply chain management

- Cyber requirements and associated penalties for noncompliance and/or breaches are appearing in contract solicitations
  - E.g., if something happens to the customers' data, then the contractor is financially responsible
  - Contracts are including defined financial consequences

- DCMA's recent inclusion of DFARS Safeguarding Clause compliance in the CPSR Guidebook poses financial liabilities to prime and higher-tiered contractors
  - Financial consequences to CPSR audit failure
  - Large part of CPSR audits is now cybersecurity supply chain management

COVID-19 and Supply Chain Security

COVID-19 Supply Chain Security Considerations

- Requires holistic approach with input from legal, HR, IT, communications, and senior leadership
- Increased teleworking and remote access may strain company's resources and connectivity options – requires evaluation of existing IT infrastructure to determine whether the systems can manage the increased demand and identification of additional/new resources
- Review regulatory and contractual requirements to determine what work can be performed remotely and put in place guardrails for electronic and physical data
- Threat actors may attempt to leverage the disruption. Companies should be on heightened alert for malicious actors (e.g., increase in phishing attacks)

COVID-19 Contractor Toolkit

- Create a disaster preparedness plan
  - Plan in advance for potential impacts
  - Outreach to government customers to address contractor operations as part of agency-specific emergency preparedness plans
- Prepare for performance interruptions
  - Supplies sourced from countries affected by the virus may be delayed or cancelled
  - Suppliers may close offices, which may affect contract performance
  - Consider contract clauses re excusable delays, suspension or work or stop work, changes
- Prepare for labor and employment impacts

Best Practices and Meeting the Challenges of Supply Chain Security Risk Mitigation

Best Practices—Dynamic, Risk-Based Approach

- **Gather** – collect data and information about critical suppliers' cyber hygiene and compliance
  - Requires adherence to enterprise-wide definitions (e.g., critical suppliers, covered sensitive information)
  - Use tools to collect and protect data from suppliers (e.g., Exostar)
  - Requires education of suppliers (to address reluctance to share information)

Best Practices—Dynamic, Risk-Based Approach

- **Analyze** – analyze data and information provided by critical suppliers to identify risks and vulnerabilities
    - Develop infrastructure (human and technical) to support efficient and enterprise-wide analysis of information gathered
- **Act** – Consider and implement actions to mitigate risks
    - Clear compliant suppliers
    - Consider termination of suppliers that are out of compliance
    - Assist critical suppliers in coming into compliance (training, site visits, etc.)
    - Document risk mitigation and compliance plans
    - Audit and re-assess

Meeting the Challenges of Supply Chain Security

Draft NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management*

- Proposes 8 distinct practices that organizations may use to enhance their Cybersecurity Supply Chain Risk Management (C-SCRM)
- Provides corresponding recommendations that are scalable based upon an organization's size.
- Each key practice includes a number of recommendations, which synthesize how these practices can be implemented from a people, process, and technology perspective.

1. **Integrate C-SCRM across the organization.**
2. **Establish a formal program.**
3. **Know and manage your critical suppliers.**
4. **Understand your supply chain.**
5. **Closely collaborate with your key suppliers.**
6. **Include key suppliers in resilience and improvement activities.**
7. **Assess and monitor throughout supplier relationship.**
8. **Plan for the full lifecycle.**

Meeting the Challenges of Supply Chain Security

Creative Solutions for Cyber -7012 Supply Chain Compliance

- Contractors are often faced with the quandary of needing to share CDI with suppliers that are either incapable of receiving CDI or are a high-risk vulnerability
- When faced with non-compliant or high-risk suppliers creative solutions are sometimes needed:
  - Determine whether the supplier must have CDI in order to perform
  - Utilize a third-party cloud service provider to help the supplier meet cyber compliance gaps
  - Give supplier access to prime or higher-tier subcontractor's network
  - Provide hard copies of the CDI with secure, controlled access
  - Training – sometimes an inexperienced supplier simply needs training to understand the means necessary to implement the controls and attain compliance
    - However there is a degree of risk associated in training a supplier and they are still non-compliant

Meeting the Challenges of Supply Chain Security

Best Practices -- Cybersecurity

1. Understand the regulations. Don’t be afraid to educate and politely push back.
2. Understand your data. This will likely require proactive discussions with your customers, subs, and business teams.
3. Understand your customer. Know what unique requirements they may have (e.g., Navy enhanced requirements, etc.) and open a dialogue discussing what CDI is expected ASAP.
4. Understand the risks. DoD has been emphasizing the benefits of risk-based approaches, especially for supply chain security.
5. Don’t forget about vendors. Company-wide suppliers and service providers also need to protect the CDI they can access.

Meeting the Challenges of Supply Chain Security

Best Practices -- Cybersecurity

6. Document more than less. Written policies and procedures can be a first line of defense against individual actions. Documentation is the first thing DCMA will review. Maintain updated copies of compliance certificates, etc.
7. Have a playbook so you know how you will respond to issues of non-compliance. Know your response before you inquire with your suppliers.
8. Train. Train personnel that interact with suppliers, so if they observe an indication of noncompliance or concern, they will know when and how to escalate the issue.
9. Audit yourself. Know your strengths and weaknesses before the government or other contractors tell you.
10. Track your costs. Compliance is allowable!
11. Keep legal in the loop. Legal drivers carry the protections of privilege.

Meeting the Challenges of Supply Chain Security

Best Practices – Compliance and Competitiveness

1. Incorporate supply chain security into overall compliance program
    1. Requires coordination among legal, contracts management, IT, procurement, global trade, and others
    2. Ensure sufficient resources to continually assess and address evolving threats and requirements
    3. Vet suppliers, service providers and products and include strong contractual requirements and penalties for non-compliance
2. Prepare for supply chain security evaluation criteria: be prepared to articulate how supply chain security is a competitive advantage
3. Look for opportunities to partner with Government (information sharing, involvement in rulemaking and other industry outreach)

Questions?