Global Supply Chain Risk Management



Roger Zakheim
Covington & Burling LLP

National Defense Industrial Association Summit

September 17, 2014

Supply Chain: Background

Scope of the Problem

- Supply chain issues have come to the forefront of USG policy attention in recent years
- Nowhere is this more important than the defense industrial base

Counterfeit Parts and the Supply Chain

"The Committee's investigation found the problem of counterfeit parts to be widespread in the defense supply chain. Looking at just part of the supply chain over a two year period . . . the investigation uncovered approximately 1,800 cases of suspect counterfeit electronic parts. The total number of individual suspect parts involved in those cases exceeded one million."

Senate Armed Services Committee Report, May, 2012.

Supply Chain: Notable Developments

The "Snowden Effect"

- Snowden made allegations that third parties can intercede with products and corrupt them
- Renewed focus on the integrity of products and systems
- Greater focus, in particular, on the risks in software-related products: third-parties can intercede with products and insert malware or otherwise corrupt them
- Exacerbated existing government concern over counterfeit parts

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- DFARS Final Rule Implementing Section 818 of the 2012 NDAA (as amended by 2013 NDAA) (May 6, 2014)
  - Applies to counterfeit and suspect electronic parts (but not all counterfeit items)
  - Clause applies to contractors subject to Cost Accounting Standard, OR their subcontractors, OR subcontracted-for commercial items.
  - Imposes reporting requirement to contracting officer or GIDEP
- Section 806 of 2011 NDAA (as amended by 2013 NDAA) / Interim Final Rule on Information Relating to Supply Chain Risk (Nov. 18, 2013)
  - Deals with IT procurements for DoD national security systems
  - DoD authority to exclude IT contractors or subcontractors based on a determination of supply chain risk

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- Under the DFARS final rule, covered contractors must "establish and maintain an acceptable counterfeit electronic part detection and avoidance system" which includes "risk-based policies and procedures" that, at a minimum, address:
  - (1) Training of Personnel with regard to counterfeit electronic parts.
  - (2) Inspection and Testing of Electronic Parts
  - (3) Processes to Abolish Counterfeit Parts Proliferation and Reporting and Quarantining Counterfeit Electronic Parts
  - (4) Processes for Maintaining Electronic Part Traceability
  - (5) Use of Suppliers who are the Original Manufacturer or Sources with the Express Written Authority of the Original Manufacturer
  - (6) Methodologies to Identify Suspect Counterfeit Parts

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- DFARS final rule "risk-based policies and procedures" (cont.):
  - (7) Design, Operation, and Maintenance of Systems to Detect and Avoid Counterfeit and Suspect Electronic Parts
  - (8) Flowdown of Counterfeit Detection and Avoidance Requirements to subcontractors.
  - (9) Processes for Keeping Continually Informed of Current Counterfeiting Information and Trends
  - (10) Processes for Screening the GIDEP Reports and Other Credible Sources of Counterfeiting Information
  - (11) Control of Obsolete Electronic Parts
- If a covered contractor fails to meet these requirements, its purchasing system may be disapproved and/or payments may be withheld for an inadequate business system.
  -

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- DFARS/DoD has NOT articulated how best to mitigate risk, leaving uncertainty about what an "acceptable counterfeit electronic part detection and avoidance system" actually requires.
  - The current regime amounts to strict liability for contractors, without much guidance
  - DoD may use Defense Contract Management Agency's Contract Purchasing System Review (CPSR) as a tool to review contractor detection and avoidance system
  - The Defense Contract Management Agency is developing a Counterfeit Detection and Avoidance System Checklist which may provide more guidance

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- The DFARS final rule on reporting counterfeit or nonconforming items may be expanded by the Federal Acquisition Regulatory Council to ALL federal government contractors.
  - FAR issued a proposed rule on June 10, 2014
  - Would require all contractors to report any suspect counterfeit products supplied to the Government to contracting officer within **30 days** of becoming aware of such products
  - Would require reporting of suspect counterfeit parts to Government-Industry Data Exchange (GIDEP) within **60 days** of awareness of such products

Supply Chain: The Legal Landscape

New Requirements for Government Contractors

- Section 309 of the Intelligence Authorization Act of 2012
  - Requires Intelligence Community agencies to conduct supply chain risk assessments for "mission-critical" products, materials, and services. Includes the authority to exclude IT contractors.
- "Wolf Amendment" – Section 215 of the Consolidated Appropriations Act of 2014
  - Prohibits DoJ, DoC, the NSF, and NASA from acquiring certain information systems (high or moderate-impact) without performing a supply chain risk assessment and reporting determination to Congress
  - Intended to focus on China, but drafted more broadly
  - One-year (appropriations act)

Objectives of Global Supply Chain Practices

- Security
  - Ensuring that design, development and testing addresses and anticipates threats (particularly relevant for software)
- Integrity
  - Making sure customers are able to verify the authenticity of components
  - Guaranteeing that the processes used to create and source components, as well as deliver components to customers addresses and anticipates threats
- Resiliency/ Continuity
  - Creating means to overcome unexpected threats and “shocks” to the system
- Quality Control
  - Monitoring and measuring the processes used to achieve goals

Conclusion

- Shifting Legal Landscape
  - Governments are mandating greater supply chain security for their contractors
  - Even private customers are asking for greater supply chain security
- More Demanding Compliance
  - Compliance is multilayered and must achieve the overlapping goals of security, integrity, resiliency and quality control.
- The Result: Increased Vendor Competition
  - Beyond any minimum requirements, supply chain security will be a competitive (dis)advantage,

Questions

Roger Zakheim
rzakheim@cov.com
(202) 662-5959