The Importance of Secure Supply Chain Management

Larry Allen
Allen Federal Business Partners
July 2016

IMPORTANCE OF SSC IS GROWING

- All About Cyber Security
- Can Preclude You From Doing DOD Business
- Preclusions From DHS Business
- Other Agencies Getting On Board

SELECTED FEDERAL SECURITY REGS

- NIST Special Publication (SP) 800-37, the Guide for Applying the Risk Management Framework to Federal Information Systems
- SP 800-53 – Moderate Security Baseline Standards
- SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems (When You Store Federal Data)
- Executive Order 13556 – Controlled Unclassified Information (CUI)

TYPICAL ELEMENTS OF A SECURE SUPPLY CHAIN

- End-To-End Control or Quality Monitoring of Entire Manufacture and Shipping Process
- Extends to Component Parts
    - Where Were They Created & Assembled?
    - By Whom?
- How Were the Components/Final Products Shipped to You?
    - OEM, Authorized Distributor
- Shipped to the Government Site

DOD REQUIREMENTS – COVERED SYSTEMS

- National Defense or Other Covered System
- Can, Indeed, Contain Commercial Items
    - Specifically Covers FAR Part 12 (Commercial Item) Procurements
    - Protections Also Exist for Far 8 (Schedules) and 15 (Contract By Negotiation)
- Requires Contractors to Mitigate SSC Risk
- Full Definition in DFARS 239.73

MORE ON DOD SECURE SUPPLY CHAIN

- Sources May Be Excluded If DOD Deems There is A Supply Chain Risk
    - Applies to Subcontractors As Well
- Covered Elements Include: Quality, Configuration, & Security of Software, Firmware, Hardware, and Related Systems
- Companies That Knowingly Install Fraudulent Material Must Pay to Replace It – Likely Contract Termination

SSC NOT JUST A DOD REQUIREMENT

- GSA RFI May 9th
- Would Impact Schedules, Alliant, OASIS, and All Other GSA IDIQ'
- Intent: Authenticate Commercial Items Coming Into Government Market
- Retain GSA's Eligibility to Serve DOD Marketplace

KEY FACTORS

- No Recycled, Obsolete Parts
- TAA Compliance Must Be Assured
- Verify and confirm with original equipment manufacturer (OEM) if offering sold directly or through authorized distributor or reseller
- Validate OEM transactions by authorized resellers and distribution channels.
- NEXT STEP: Formulation of Formal Requirement

NASA SEWP & SSC

- NASA Concerned That Term “Authorized Re-Seller” Not Well-Defined
    - Seeking Information to Ensure That Contractors Are Authorized and Have a Secure Source for Products They Have on SEWP
- Looking at International “Open Group” ISO/IEC 20243, The Standard for An Open Technology Trusted Supplier
- Will Adhere to DOD Rules To Ensure DOD Business
- Active Participant in Federal/International SSC Organizations

WHAT ALL OF THIS MEANS TO YOU

- Don’t Assume Your Customer Knows About SSC Requirements in any Detail
- You Must Be Prepared To Educate the Customer
- Show How You Comply, Especially as a Comstor Partner
    - https://www.westconcomstor.com/global/en/capabilities/services/technical-services/supply_chain_services.html
    - https://www.youtube.com/watch?v=1zOSbYvM-60
- Tell Your Customer They Should Look For SSC Compliance From All Suppliers

For more information:

Contact the Comstor Federal Team at federalsales@comstor.com or at 800.955.9590

Larry Allen, Allen Federal Business Partners, lallen@allenfederal.com

Westcon Comstor

Delivering Results Together

powered by WestconGroup

Cloud Global Deployment Services

Security UCC Networking Data Center