Supply Chain Management: Defense Considerations

Brian P. Gallagher
Senior Vice President, Operational Excellence
26 June, 2014
Over 50 Years Helping Customers Meet National Priorities

- $3.7 billion annual revenue
- Fortune World’s Most Admired Companies – 6th in IT Services
- Fortune 1000 Largest Companies in America
- 13th in Top 100 Federal Prime IT Contractors – Washington Technology
- Over 15,500 employees, some 70% with security clearances
- Consistently recognized as a top employer of veterans, who make up approximately 20% of our workforce
- Character-based culture of ethics, integrity, and operational excellence
- Headquartered in Arlington, VA
Serving National Priorities

Business Systems

Cyberspace

Geospatial

Integrated Security Solutions

Investigation and Litigation Support

C4ISR

Enterprise IT

Healthcare

Intelligence

Logistics and Material Readiness
Implications of Supply Chain

- Status of goods, services, and products must be transparent
- Traceability and authentication of any item’s Pedigree must be validated
- Behavior of products and services must be assured
- Transport and storage of items must be secure
How Hard Can That Be?

[https://buildsecurityin.us-cert.gov/swa/forums-and-working-groups/acquisition-and-outsourcing]
For Complex Supply Chains, It’s Really Hard!
Finding the Weakest Link

Supply Chain vulnerabilities provide easy access to systems that are critical to our Nation’s security.

Counterfeit parts lack quality and the performance required to perform difficult missions.

Adversaries look for weaknesses and infiltrate the supply chain with components that have “extra” capabilities.

Why is this important?

CACI
EVER VIGILANT
Implications of Failure

Complex systems developed by Defense Contractors support DoD, homeland security, law enforcement, border security, emergency response, and disaster relief missions in coordinated and controlled operational settings.

Failure of components or software to perform as intended place lives and missions at risk.

CACI
EVER VIGILANT
Implications of Failure

Complex systems help our Nation stay ahead of evolving threats, protect mission-critical systems, and ensure information confidentiality, integrity, and availability.

Supply chain failures and vulnerabilities have far reaching implications in supporting our Nation’s critical infrastructure.
Controls: Secure Supply Chain Management

ISO 28000/ ISO 27001/ CERT-RMM/ NI ST Cyber Security
Founded on Threat Management Delivering Supply Chain Resilience
Identification-Prevention-Detection-Response-Recovery

Security Controls
- InfoSec
- Supplier Management
- Compliance
- GPS Carrier Tracking
- Counterfeit ID Program
- Malware Detection
- Operations Security
- Incident Mgmt
- Access Control
- Asset Mgmt
- Environment Security
- Physical Security
- Hazmat Program
- HR Mgmt
- Training Program(s)
- Preparedness Testing

Supply Chain Management
Systems Manage all aspects of the Supply Chain
$, Tracking, Configuration, Inventory, Custodianship...

Threats/ Attacking Agents
- Counterfeit Parts
- Collusion
- Fraud
- Espionage
- Environment
- Nature
- Thief
- Piracy
- Spillage
- Terrorism
- Contamination
- Sabotage (Open Source Code)
- Viruses/ Malware
- Insider Threat

Connection/ Network

Development / Configuration
Transport

Storage

Configuration/ Integration
Transport

Procurement

Customer/ Consumer
Questions?