Ballistic Missile Defense System (BMDS)
Supply Chain Illumination

Naval Surface Warfare Center, Crane Division (NSWC Crane)

Microelectronics Integrity Meeting

Introduction

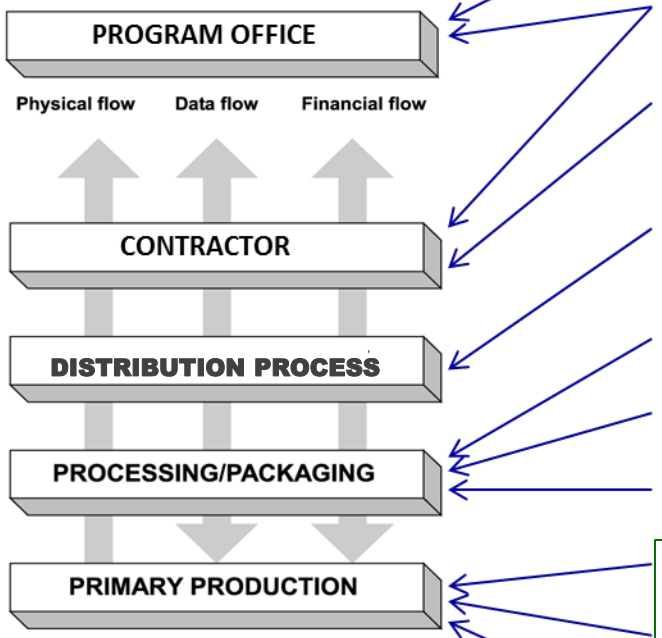
- **Missile Defense Agency is developing the Ballistic Missile Defense System (BMDS), an evolving, integrated, and interoperable system comprising multiple elements and components deployed world-wide that provides a capability to intercept ballistic missiles in all phases of their flight (i.e., boost, midcourse, and terminal) against all ranges of threats**
- **Our adversaries are attempting to influence the BMDS supply chain across the system life cycle, including design, manufacturing, development, and sustainment phases**
- **Supply Chain Risk Management (SCRM) is challenged with ensuring the integrity of microelectronics components with no trusted foundry and a COTS-intensive system**

MDA goal is preventing malicious microelectronic components from reaching the BMDS Warfighter

Generic Threats – Supply Chain Attacks

Coverage is for what part of the chain is infiltrated and what the malicious insertion accomplishes

Supply Chain



Attack Vectors

Clandestine changes to mission data

Infiltration of sites to insert back doors and malicious logic into some micro electronics (FPGAs and other devices)

Infiltration of company receiving department to add / substitute components with backdoors to allow remote penetration during operations, denial of service, etc.

Infiltration of transportation companies to intercept DoD component shipments (developmental or COTS) and substitute components that have malicious code inserted

Insertion of malicious software in the open source used for math libraries

Infiltration allowing malicious software implantation through 3rd party bundling

Establishment of shell company to insert counterfeit parts

Infiltration to manipulate the hardware or software baselines

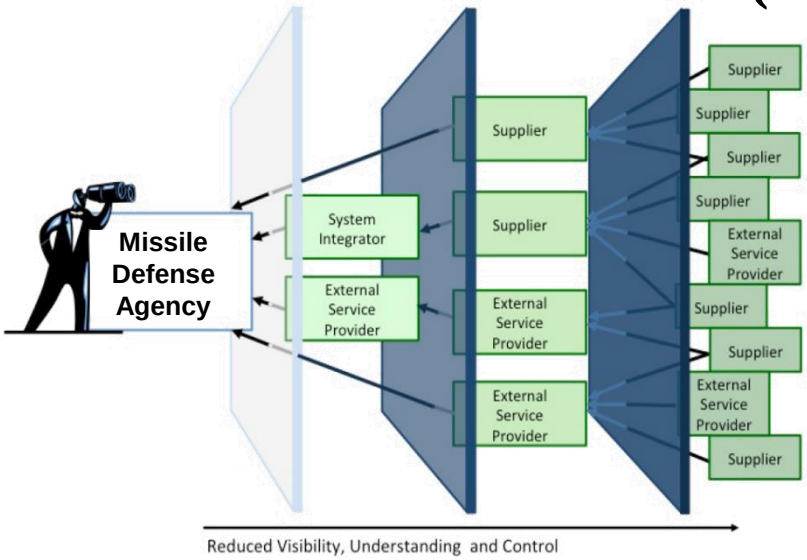
Infiltration of company software development to insert software which exfiltrates data

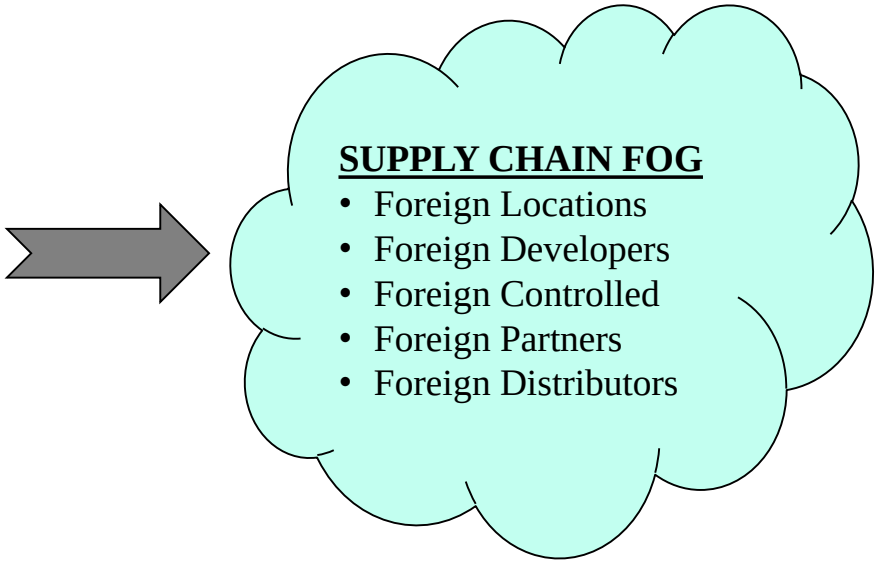
Infiltration to compromise the design/fabrication of hardware

Can have multiple levels: OEMs → subassembly suppliers → assembly suppliers → integrators

Increasingly Complex Supply Chain

Today's supply chains consist of a prime integrator and hundreds of global suppliers / developers providing custom and commercial-off-the-shelf (COTS) parts



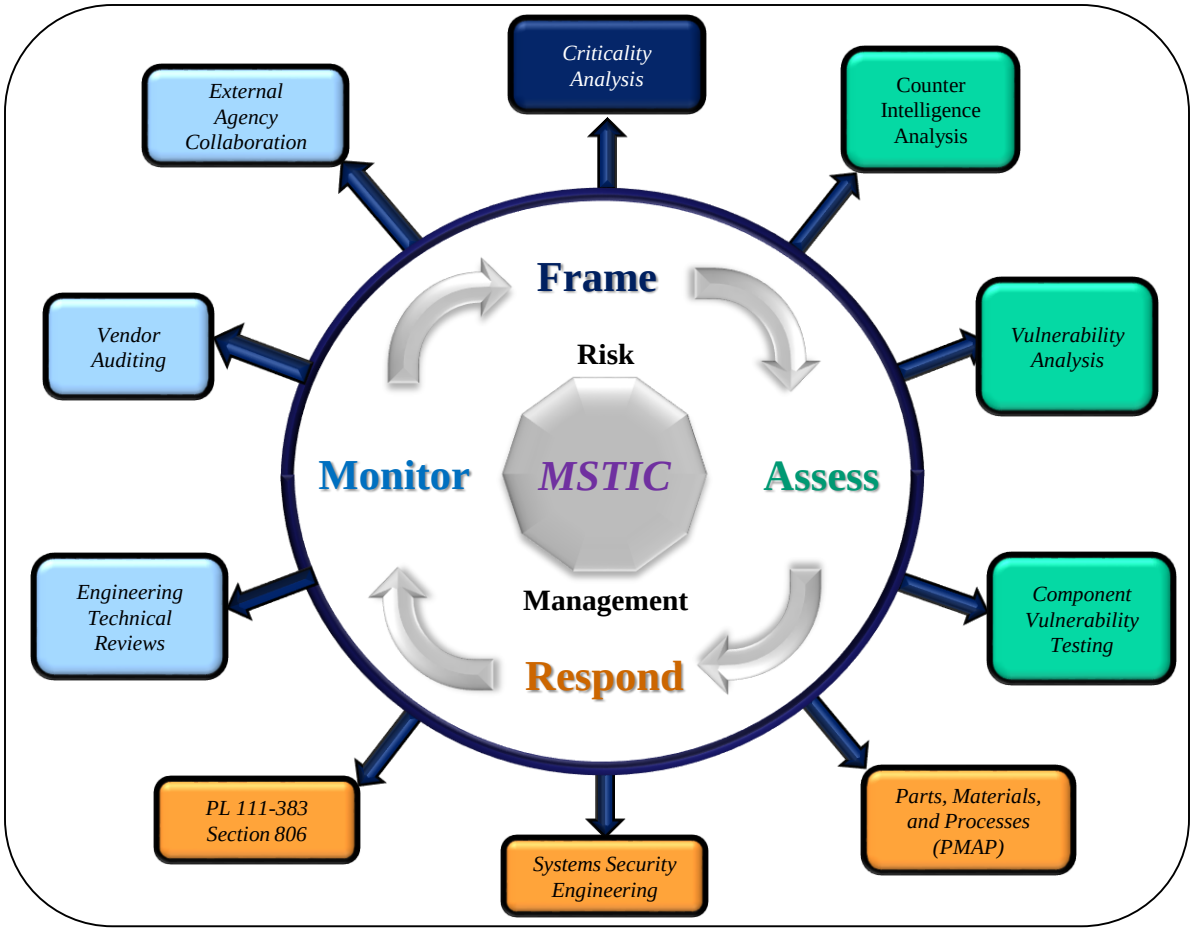


Government: *NIST Special Publication 800-161 , SCRM, April 2015*

- **Has a contractual relationship with only the prime contractor**
- **Has limited insight of the rest of the supply chain (perhaps only two or three levels down)**

Supply Chain Visibility Reduced at Lower Tiers

MDA Supply Chain Risk Management Strategy



- ***Frame*** **– Establish baseline criticality of the functions necessary to satisfy BMDS mission requirements**
- ***Assess*** **– Identify and assess the risk of critical logic-bearing components to mission success**
- ***Respond*** **– Develop mitigations for components providing the highest risk to mission fulfillment**
- ***Monitor*** **– Evaluate the risk of new components before introduction to the BMDS**

Identify, Assess, and Mitigate High-Risk Logic-bearing Components and Continuously Monitor System Changes to Minimize Cyber Supply Chain Risk During BMDS Evolutionary Acquisition

Summary

- **MDA strategy is to inject intelligence into the engineering process to proactively manage threats to microcircuit integrity during development and prevent malicious components from ever being introduced into BMDS elements**
  - **Supplier Management requirements ensure vendors procure components from trusted suppliers**
  - **MDA improving its capability to assess vendor threats to prevent counterfeit or malicious components from entering the production supply chain**
  - **Vendors need to be proactive in testing the integrity of microelectronics procured for the BMDS**

MDA goal is preventing malicious microelectronic components from reaching the BMDS Warfighter