Some examples of supply chain exploitation may include, but are not limited to, the introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to protected data, to alter data, to disrupt operations, to interrupt communication, reverse engineer, or otherwise cause disruption to the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of an equity.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

EXPLOITATION OF GLOBAL SUPPLY CHAIN

WHAT IS EXPLOITATION OF GLOBAL SUPPLY CHAIN?

Activities of foreign intelligence entities or other adversarial attempts aimed at compromising and or sabotaging the supply chain.

A supply chain consists of a network of suppliers, manufacturers, developers, warehouses, distribution centers, transportation vehicles, and wholesale or retail outlets. The supply chain may be global and also includes the designers, producers, shippers, and resellers that create, distribute or in any other way have the ability to influence the product.

Organizations should protect against supply chain threats to the affected information system, system component, or information system service by employing a standardized process to address supply chain risk as part of a comprehensive, defense-in-breadth information security strategy.

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

- Cyber operations
- Personal contact
- Phishing operations
- Academic and professional résumé submissions

WHO IS BEING TARGETED?

Any cleared contractor supplying or installing complete systems or components for DoD or other government agency's systems, equipment, facilities, or procurement programs.

- **Acquisition and procurement**: Personnel purchasing components to include microelectronics for use in the production or maintenance of U.S. Government systems, programs, or technology
- **Design, manufacturing, and assembly**: Personnel with access to manufacturing lines or supply chain of U.S. Government programs, projects, and systems
- **Technicians**: Personnel accessing U.S. Government equipment or systems conducting routine maintenance or incorporating new components in existing systems/equipment

WHY IS IT EFFECTIVE?

- Successful exploitation of supply chain would allow foreign agents, or personnel acting on their behalf, to manipulate components intended for DoD systems, degrading DoD capabilities and effectiveness during potential conflicts, or to gain access to sensitive information.
- Nonconforming components will not perform to specification and can include malicious logic intended to degrade or destroy DoD systems and could cause events ranging from injury, to loss of life, to compromise of national security.
- Nonconforming parts are often difficult to identify compared to authentic components.
- An actor with insider access could introduce malicious changes or substitutions with a nonconforming part during any phase, increasing the difficulty in identifying potential malfeasance.

During the design and manufacturing phases, an actor could perform a series of malicious changes, to include: Gate level changes, protocol changes, parameter modifications, wiring modifications, etc.

During the sustainment phase, limited sources for obsolescent components may lead to manufacturers receiving nonconforming parts via gray market suppliers.

HOW CAN YOU RECOGNIZE IT?

Exploitation of the global supply chain can occur at any phase during the process.

During design and manufacturing, personnel should use trusted and controlled distribution, delivery, and warehousing options.

During sustainment, personnel should also be aware of signs of tampering with shipping containers, and establish protocols to include the independent verification and validation of microelectronics, and in particular microelectronics obtained outside of authorized vendors (e.g., obsolete microelectronics).

>> Signs of a compromised supply chain may include any of the following:

- Exhibits functionality that was outside the original design
- A device, or multiple devices, from a lot, that exhibits a unique error or failure
- Employees violating security protocols for handling of components, or introducing non-compliant components
- Dealers offering rare or out of production components at low prices
- Dealers offering short lead times for large orders of components
- Shipping containers show signs of tampering

COUNTERMEASURES

>> To mitigate tampering with components at the cleared facility during assembly and production:

- Ensure security protocols are in place and adhered to for access to the facility, assembly and production lines, and networks
- Establish and maintain an effective insider threat program
- Train workforce to identify and promptly report suspicious activities

>> To mitigate the threat of counterfeit components:

- Use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods;
- Integrate acquisition offices with other offices including the information assurance and security offices;
- Ensure sub-contractor or off-site production facilities conduct effective supply chain risk management;
- Create incentives for suppliers who: implement required security safeguards, promote transparency into their organizational process and security practices, provide additional vetting of the processes and security practices of sub-suppliers, restrict purchases from specific suppliers, and provide contract language regarding the prohibition of uncompromised or counterfeit components;
- Always use independent verification and validation for obsolete microelectronics and vet external testing houses;
- Consider lifetime buys for components to avoid purchasing grey market nonconforming parts.

REPORTING

The introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to classified information, to alter data, disrupt operations, or to interrupt communications related to classified contracts or cleared constitutes a “suspicious contact,” and is reportable by cleared companies to DCSA (National Industrial Security Program Operating Manual 1-302b).

>> Examples of reportable activity include:

- Devices that exhibit functionality that was outside the original design
- A device, or multiple devices from a lot, that exhibits a unique error or failure
- Inadvertent or deliberate attempts to break a trusted chain of custody
- Introduction of counterfeit components into a U.S. Government system during production
- Unauthorized personnel of any nationality accessing restricted areas of a cleared facility involved in the production of components for DoD systems
- Efforts by any individual, regardless of nationality, to compromise a cleared employee involved in manufacturing, assembling, or maintaining DoD systems
- Successful exploitation of supply chain can have a catastrophic impact. It is vital that personnel promptly report suspected incidents to their facility security officer or DCSA representative.