additional sub-supplier vetting, restrict purchases from specific suppliers, and provide contract language that prohibits compromised or counterfeit components

- Always use independent verification and validation for obsolete microelectronics and to vet external testing houses
- Consider lifetime buys for components; avoid purchasing gray market, nonconforming parts
- Validate vendor with DOD customers/other authorized resources prior to purchase

REPORTING

A "suspicious contact" occurs when someone attempts to introduce counterfeit or malicious products or materials into the supply chain.

Examples of Reportable Activities:

- Devices exhibiting functionality outside the original design
- A device, or multiple devices from a lot, exhibiting a unique error or failure
- Inadvertently or deliberately attempting to break a trusted chain of custody
- Introducing counterfeit components into a USG system during production
- Unauthorized personnel, of any nationality, attempting to access restricted areas of a cleared facility involved in producing components for DOD systems
- Any individual, regardless of nationality, attempting to compromise a cleared employee involved in manufacturing, assembling, or maintaining DOD systems

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires the reporting of suspicious contacts, behaviors, and activities.

If you suspect you or your company has been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence threats and mitigating risks. Reporting allows us to share and address risks together.

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

EXPLOITATION OF GLOBAL SUPPLY CHAINS

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

WHAT IS EXPLOITATION OF GLOBAL SUPPLY CHAIN?

Exploitation of the global supply chain refers to foreign intelligence entities' and other adversaries' attempts to compromise a supply chain. This may include the introduction of counterfeit or malicious products into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

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

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

Some examples of supply chain exploitation may include, but are not limited to, introducing counterfeit or malicious products or materials into the supply chain to:

- Gain unauthorized access to protected data
- Alter data
- Disrupt operations
- Interrupt communication
- Reverse engineer
- Cause any disruption to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an entity
- Intercept, disrupt, or delay shipping
- **Design, Manufacturing, and Assembly**: Personnel that access manufacturing lines or U.S. Government (USG) supply chain programs, projects, and systems
- **Technicians**: Personnel that access USG equipment or systems to conduct routine maintenance or incorporate new components into existing systems/equipment
- **Software Developers**: Personnel providing code to support both classified and unclassified networks and technology
- **Stock Control Specialists**: Personnel that inventory and control the flow of equipment and material (physical or virtual) in and out of a facility

WHY IS IT EFFECTIVE?

- Successful exploitation of supply chain enables foreign agents, or personnel acting on their behalf, to manipulate Department of Defense (DOD) system components, degrading DOD capabilities and effectiveness during potential conflicts, or to gain access to controlled unclassified information (CUI)
- Counterfeit components will not perform to specification and can include malicious logic intended to degrade or destroy DOD systems and cause events ranging from poor system interoperability, to injury and 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 difficulty to identify 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

During the production/testing phase, a part that was intentionally manufactured poorly due to lack of information could cause the user to send the correct specifications back to the bad actor

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 check for signs of tampering with shipping containers. Personnel also should establish protocols to include independent verification and validation of microelectronics, particularly microelectronics obtained outside of authorized vendors (e.g., obsolete microelectronics)

SIGNS OF A COMPROMISED SUPPLY CHAIN:

- A device that exhibits functionality outside of its original design
- A device or multiple devices from a lot exhibiting a unique error or failure
- Employees violating security protocols for handling components or introducing non-compliant components
- Dealers offering rare or obsolete components at low prices
- Dealers offering short lead times for large component orders
- Shipping containers showing signs of tampering

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

- Cyber operations
- Personal contact
- Joint ventures
- Academic and professional résumé submissions
- Tampering

COUNTERMEASURES

To Mitigate Tampering with Components at the Cleared Facility During Assembly/Production:

- Ensure compliance with established security protocols 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 Threat of Counterfeit Components:

- Due Diligence Reporting: Use available resources to look 2-3 levels down the supply chain to vet your downstream suppliers
- Use available all-source intelligence analysis to plan acquisition strategies/tools/methods
- Integrate acquisition offices with other departments, including information assurance and security offices
- Ensure subcontractor/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