WHAT TO REPORT

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

EXAMPLES OF REPORTABLE ACTIVITIES

- Inadvertently or deliberately attempting to break a trusted chain of custody
- Introducing counterfeit components into a U.S. Government 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
- Devices exhibiting functionality outside the original design
- A device, or multiple devices from a lot, exhibiting a unique error or failure

REPORTING REQUIREMENTS

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

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

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

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

EXPLOITATION OF GLOBAL SUPPLY CHAINS

Defense Counterintelligence and Security Agency

WHAT IS EXPLOITATION OF GLOBAL SUPPLY CHAINS?

Exploitation of the global supply chain refers to foreign intelligence entitiy (FIE) attempts to compromise a supply chain.

A supply chain is a network of suppliers, manufacturers, developers, warehouses, distribution centers, transportation, outlets, and personnel. The supply chain may be global.

Organizations should protect against supply chain threats by employing a standardized process to address supply chain risk as part of a comprehensive information security strategy.

WHO IS BEING TARGETED?

- Design, Manufacturing, and Assembly Personnel
- Technicians
- Software Developers
- Stock Control Specialists

HOW ARE YOU BEING TARGETED?

Supply chain exploitation includes 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 disruption to design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an entity
- Intercept, disrupt, or delay shipping

METHODS OF OPERATION

Exploitation of Business Activity

Résumé Submission

Search and Seizure

METHODS OF CONTACT

Cyber Operations

Personal Contact

HOW CAN YOU RECOGNIZE IT?

- A device that exhibits functionality outside its original design
- 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
- A device or multiple devices from a lot exhibiting a unique error or failure
- Shipping containers showing signs of tampering

WHY IS IT EFFECTIVE?

- Successful exploitation of supply chain enables foreign agents to manipulate Department of Defense (DoD) system components, degrading capabilities and effectiveness or enabling 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 poor system interoperability, injury, loss of life, or compromise of national security
- Nonconforming parts are difficult to identify
- An actor with insider access could introduce malicious changes during any phase:

Design and manufacturing	An actor could perform a series of malicious changes, including: gate-level changes, protocol changes, parameter modifications, wiring modifications, etc.
Production and testing	An intentionally poorly manufactured part could cause the user to send the correct specifications back to the bad actor
Sustainment	Limited sources for obsolete components may lead to manufacturers receiving nonconforming parts via gray market suppliers.

COUNTERMEASURES

TO MITIGATE TAMPERING WITH COMPONENTS AT CLEARED FACILITIES:

Design and manufacturing	• Use trusted and controlled distribution, delivery, and warehousing options
Production and testing	• Comply with established security protocols for access to the facility, assembly and production lines, and networks • Establish and maintain an effective insider threat program • Identify and promptly report suspicious activities
Sustainment	• Check for signs of shipping container tampering • Establish protocols including independent verification and validation of microelectronics

TO MITIGATE THREAT OF COUNTERFEIT COMPONENTS:

- Vet 2-3 levels down the supply chain
- 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 organizational process and security practices, provide 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