Cisco Systems, Inc.

Counterfeit Electronic Part Detection and Avoidance System

Cisco deploys and maintains a comprehensive security capability across its global supply chain focusing on key threat areas including manipulation, espionage and disruption. We direct a multi-layered approach to the exposures arising from those threats such as:

- Taint
- Counterfeit, and
- Misuse of Intellectual Property.

Cisco's Counterfeit Electronic Part Detection Avoidance System includes efforts to protect against, detect when present, and continuously innovate to mitigate both counterfeit raw materials (*e.g.* electronic parts as defined in DFARS 252.246-7007 (a) (MAY 2014)), as well as counterfeit Cisco finished goods.

This security capability includes creation and deployment of:

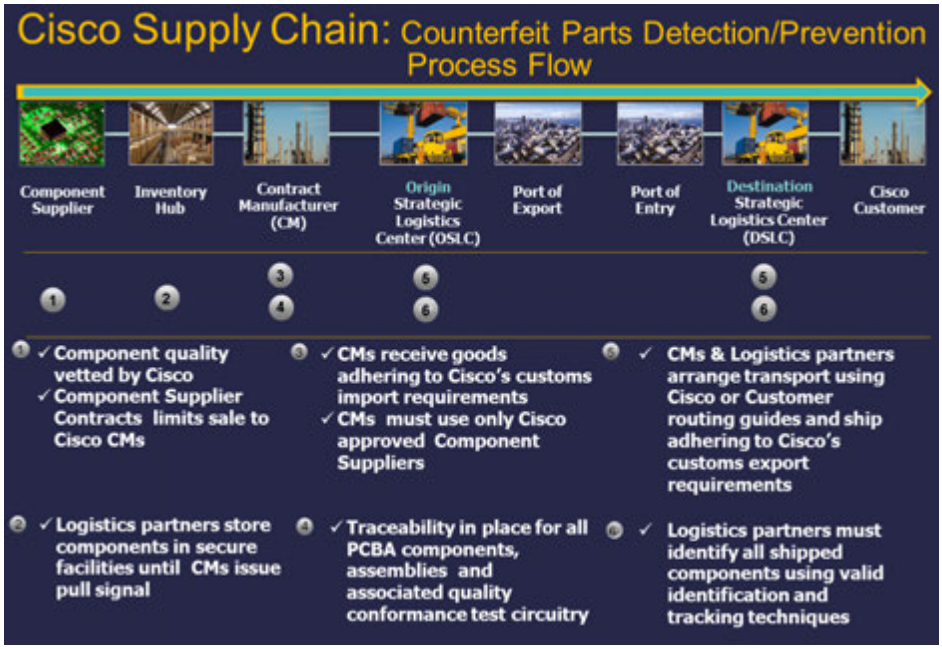
A. **Awareness Campaigns (Best Practice Training + Vulnerability/Counterfeit Trends)**
Awareness campaigns effected for Cisco employees and contractor employees, as well as suppliers. These campaigns address issues such as what constitutes Cisco Intellectual Property and the types of practices which could avoid insertion of counterfeit into the Cisco supply chain or the supply chains of our suppliers. This multi-tiered approach embraces members of the Cisco Supply Chain providing:
    - Electronic components
    - Printed Circuit Board Assemblies (PCBAs), and
    - Related software, firmware and security programming.

    The awareness campaign includes techniques such as:
    - Video training on intellectual property protection
    - Specific technical assistance and repair center team training regarding "indicia" of counterfeit – updated as trends change
    - Supplier Code of conduct training
    - Access control (both physical access and information access)
    - Scrap management
    - A covert test buy program designed to identify potential sources of counterfeit Information and Communications Technology, and
    - Coordination with government agencies to provide indicia of authenticity and identify counterfeit at borders before release into the commercial marketplace.

B. **Component and PCBA Inspection, Testing and Traceability**:

In addition, Cisco deploys a systematic approach to quality and authenticity which includes:

- Strict limitations on which suppliers are authorized to provide raw materials such as electronic components for any Cisco product or solution
- Contractual obligations with all suppliers which address authenticity/performance and acceptance criteria for all electronic parts, electronic assemblies and Cisco finished goods
- Mandates that manufacturers of Cisco products utilize ONLY raw materials from such approved suppliers of electronic components and more specifically, only those parts which have been tested and pre-qualified by Cisco
- Utilization of an electronic parts "hub" managed for Cisco leveraging security technology, physical security and logical security processes to minimize taint, counterfeit and misappropriation of Cisco Intellectual Property
- An overview of our process flow as shown below:



- Traceability via a link of such electronic parts through a proprietary in-circuit test process which correlates every component on every PCBA by:
    - Date code
    - Lot code
    - Manufacturers' Part Number (MPN)
    - Test process run
    - Test/quality results
    - Material content
    - Further traceability Insertion of immutable identity certificates (where applicable), and
    - Further traceability linking all electronic parts to a specific PCBA and each PCBA to a Cisco Finished Product ID via a system of labeling and serial number correlation.

C. **Secure Development and Deployment of Customized Cisco Anti-Counterfeit Technology**:

To further enhance the goal of electronic part avoidance and detection, Cisco leverages a suite of practices, technologies and third party accreditations. Among those are:

- Cisco's secure development lifecycle (addressing critical elements to avoid counterfeit code *e.g.* configuration management, version control, source code access protection, security-based release criteria)
- Open Source Software provenance and deployment oversight
- Proprietary anti-counterfeiting silicon technology
- Leveraging proprietary Secure Boot and Trust Hardware Anchor technology
- Accreditations/certifications such as US C-TPAT (and those that are sponsored OCONUS), FIPS, Common Criteria, IPv6, DCE, USG v6, and
- Continuous hardening of products based on counterfeit trends identified through our "Awareness Campaign" efforts identified above.

D. EOL and Scrap Processes:

Cisco deploys a comprehensive set of physical and logical security processes to ensure that excess, obsolete and end of life electronic parts are:

- Controlled and monitored by a select set of suppliers
- Collected, disassembled and destroyed in a fashion that minimizes re-utilization to create counterfeit, and
- Subject to reconciliation processes to avoid inadvertent loss or intentional removal.

E. Security Incident Communications and Alerts:

Cisco has a longstanding commitment to encourage the reporting of security vulnerability and suspected counterfeit products by customers, suppliers and channel/distribution partners. In addition to reviewing all publically reported vulnerabilities, a dedicated global team investigates and timely publishes security vulnerability alerts and fixes. See Cisco Security Advisory Center.

This comprehensive and layered approach comprises Cisco's Counterfeit Electronic Part Detection and Avoidance System. Moreover, Cisco leads and contributes to a number of International Standards focused on reducing counterfeit electronics parts across the ICT industry (*e.g.* ISO 27036; the Open Group Trusted Technology Partner Standard – ISO 20243).