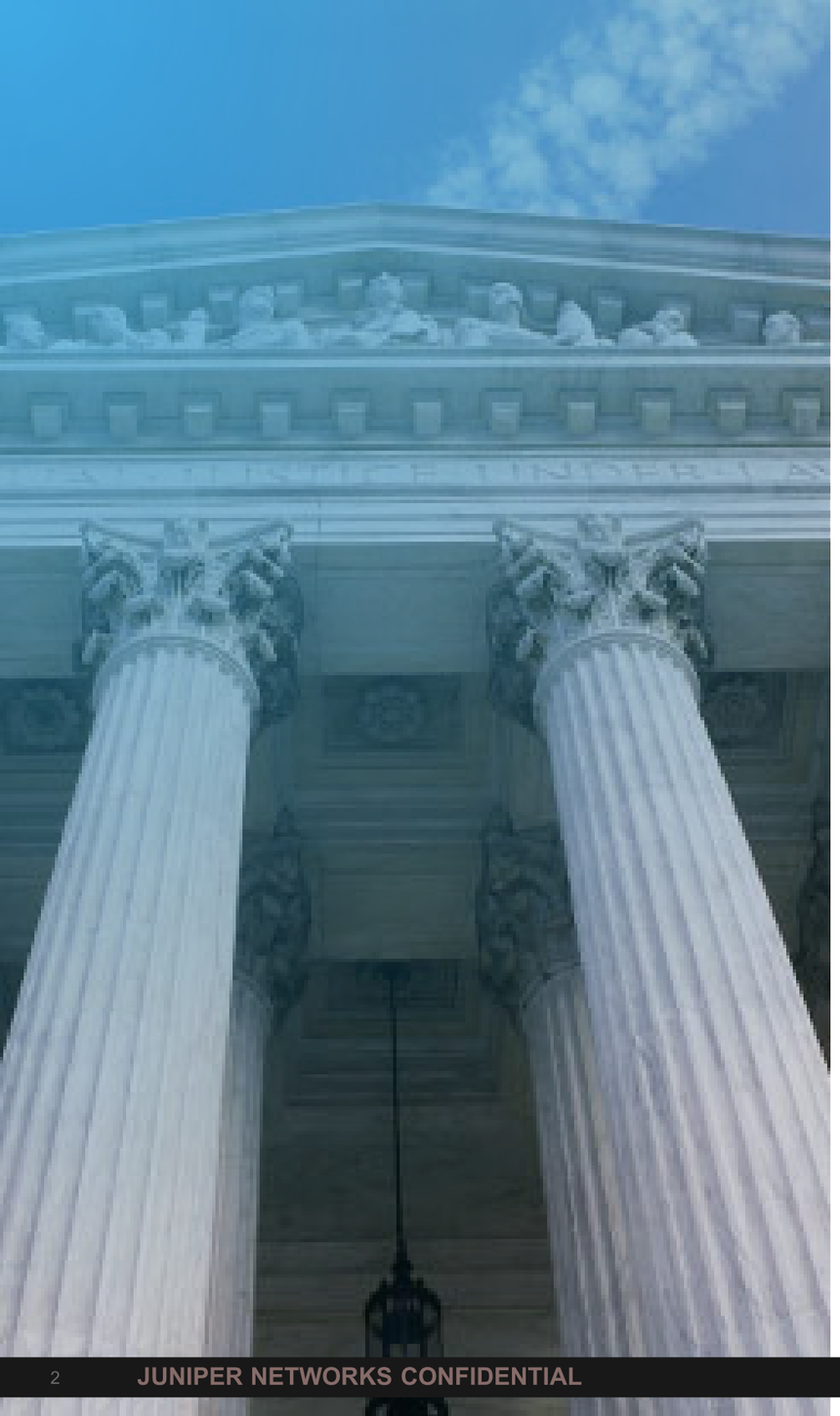
Juniper Networks Supply Chain Risk Management

Danielle M. Zeedick, Ed.D., CISM, CBCP | Sr. Manager, EHS&S, FSO—ISSO--CSSO

Prepared for SSCA

December 2017



Juniper Networks

- Long-term, trusted supplier to the US Department of Defense, Department of Homeland Security, and the US Intelligence community.
- Publicly Traded, US Headquartered Company
- Top Secret Facility Clearance

Supply Chain Risk Management Overview

- Introduction
- Definition of Supply Chain Integrity
- Process Driven Approach
- Technology
- Third Party Assessments and Certifications
- Secure Development Lifecycle
- Customer Responsibilities
- Questions

Introduction

- Supply Chain Risk Management has been a long term emphasis at Juniper Networks
- Driven by Juniper Networks Brand Integrity and TL9000 certified Quality Management Programs
- Informed by NIST IR 7622, National Supply Chain Risk Management Practices for Federal Information Systems
- Informed by NIST SP 800-53, DISA Application Security and Development STIG and Industry Initiatives such as the Software Assurance forum for Excellence in Code (SAFECode)
- Compliant with DoD DTEM 09-016, ICD 731 and other Department of Defense policies related to SCRM

There has neve been any report of, or evidence of, any counterfeit Juniper Networks products reaching our customers

Supply Chain Integrity and Security Is Not A New Issue For Technology Companies

- Chip Thefts in the late 1970s and early 1980s
- Remarked and upscreening components
- Outsourcing of manufacturing to low cost regions created additional risk
  - Complex global supply chains
  - In-house to contracted manufacturing
- The Expansion of the Gray market in the mid 1990s
  - The internet facilitated global broker networks
- 9/11 and protecting the import supply chain into the U.S.
- Counterfeit hardware in Government networks and in Government / Military systems in 2008
- Cyber attacks and Advance Persistent Threats in 2009 and beyond
  - IP Loss
  - Source Code Theft

Many Product Integrity Issues are Preventable

- Root cause analysis of numerous cases identify internal issues which contribute to the ability for adversaries to compromise ICT products:

  Product Design and Technology

  IP Protection
- Internal Company Behaviors:
  - Purchasing materials and components from untrusted sources
  - Lack of focus on the issue
  - Lack of supplier oversight and due diligence
  - Lack of discipline in the distribution channel
  - Internal communications and education
- Supply Chain Visibility and Traceability
- Development Practices
- Production Network Security and Hygiene

Juniper Networks Brand Integrity Program

- Provides a framework to ensure the security and integrity of Juniper Networks' products and intellectual property by employing standards and security best practices at all stages of the product lifecycle:
  - R & D – Software and Hardware
  - Procurement
  - Supply Chain
  - Sales and Marketing
  - Distribution
  - Customer Support
  - End of Life & Disposal
- Preventative in nature
- Enhances Business Continuity

Supply Chain Security

- Alignment with trusted, vetted manufacturing partners
- Security Standards implemented at all levels of the supply chain
- Component Integrity and Traceability Requirements
- Corporate Social Responsibility Factors

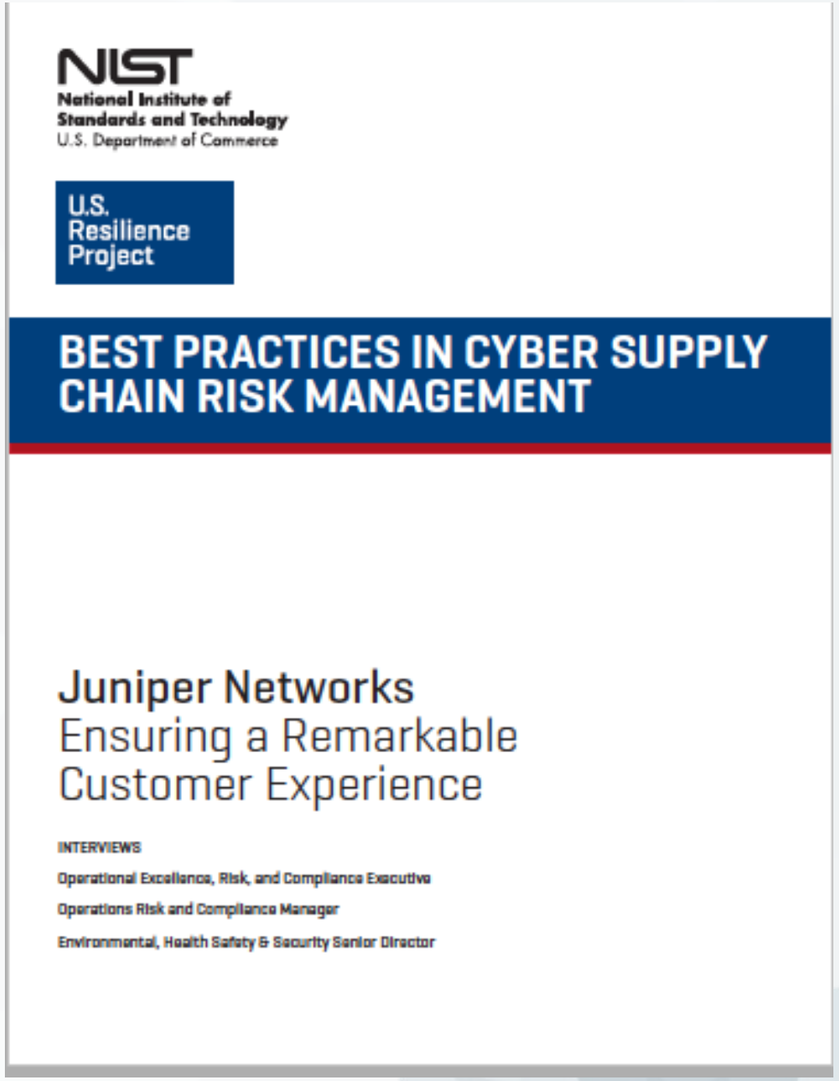
Supply Chain Risk Management Council established to oversee the program

- Legal Department/Corporate Security
- Government Affairs
- Information Security
- Operations Procurement and Logistics
- International Trade Compliance / Export Compliance
- Finance / Risk Management
- Internal Audit

Mature security assessment and continual improvement program with metrics dashboard in place

Juniper Leadership in Supply Chain Risk Management

- Participated in the development of NIST IR 7622
- NIST Recognized Best Practice- https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Juniper-Cyber-SCRM-Case-Study.pdf
- Vetted by DHS, DIA, DISA, and others



Areas of Strategic Focus

Protect the Product at all Stages of the Product Lifecycle

Designed to be counterfeit resistant

- One previous, but unsuccessful counterfeiting attempt
  - Lessons learned
- Hardware designed to be difficult to counterfeit
- Juniper designed custom ASICs in many products (app specific)
- Use of special anti-counterfeit chips in most products
- Software looks for a hardware cryptographic digital signature.
  - Won’t run with invalid signature

Secure Development Lifecycle

- Secure Coding Training
- Security Consideration in Design
- Threat Modeling
- Penetration Testing
- Release Security Review
- Incident Response Plan

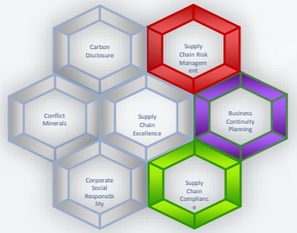
Examples of Security Consideration in Design

- Avoidance of default passwords in Junos
  - Operator must create and save unique root password at initial configuration
- Granular, Role based authentication to support concept of least privilege
- Junos software is digitally signed
- Junos verified exec (veriexec) prohibits the execution of any binary that is not signed by Juniper
- New products include Trusted Platform Modules (TPN) allowing secure boot

Thoroughly vetted and supervised Contract Manufacturers and Original Design Manufacturers

- Contract Manufacturers
  - Flextronics
  - Celestica
- Original Design Manufacturers
  - Accton
  - Alpha Networks
  - SuperMicro
- Thorough Analysis of FOCI Factors
- Juniper quality and manufacturing experts on site
- Annual on-site security assessments

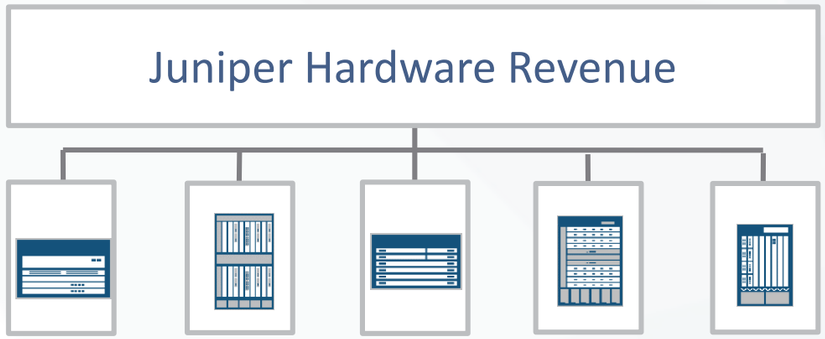
VISIBILITY TO OUR GLOBAL, MULTI-TIER SUPPLY BASE, AND EACH OF THEIR SITES



Accountability for over 3,000 SKU's

Assembly, manufacturing and sub-tier suppliers

- Code of Conduct
- Working conditions
- Material composition
- Event risks
- Security
- Energy use and carbon emissions



- Contract Manufacturers (CM)
- Outside Design Manufacturers (ODM)
- Directly manage key suppliers

Supply base visibility:

- 300+ of our direct and sub-tier suppliers
- 2,000+ supplier sites worldwide
- 24,000+ part numbers

Traceability of components

- Juniper Quality process dictates device and component serialization and monitoring of performance in the field
- Agile software system used to track changes to hardware and details for components
- Manufacturers not permitted to change component sources without Juniper approvals
- Major component vendors thoroughly vetted and monitored
- Quality management system tracks performance of hardware in the field
  - Out of box failures

Vetted and Certified Shipping

- Ordering entity emailed serial numbers of products at time of shipment
  - Helps insure provenance (you should receive what was sent)
- Tamper evident packaging
- Juniper Networks distribution supply chain certified at highest level (Tier 3) by the US Customs and Border Protection Customs/Trade Partnership Against Terrorism (C/TPAT) and the European Union's Authorized Economic Operator (Security) Programs.

Juniper Networks J-Partner Program

- Vetted and authorized business partner program
- Rigorously enforce our reseller agreements, which mandate that sales be made directly to end-users, to ensure provenance within the supply chain.
- Terminate gray market activity

Third Party Security Assessments

- NIST FIPS 140-2 testing and certification
- NIAP Common Criteria testing and certification
- DoD UC APL Certification testing and certification
- NSA Commercial Systems for Classified (CSfC) vetting and certification
- ICSA Labs Commercial Certifications
- Certification testing by major service providers
- Routine Supply Chain analysis and vetting by
  - DHS
  - CBP
  - DIA
  - DISA
  - US Intelligence Community

Recommendation to Our Customers and Their Responsibilities

- Only purchase Juniper Products from Juniper Networks authorized partners
  - Require bidders to document partner authorization
- Maintain support for purchased Juniper Networks products to maintain access to software updates
- Only purchase support for Juniper Networks products from Juniper Networks authorized partners
- Subscribe to Juniper Security Advisories/Follow Juniper SIRT
- Report any potential Security Vulnerabilities to Juniper SIRT
- If you have questions about the provenance of Juniper products, engage your Juniper account team

Our Goal: No Products Should Ever End Up Here

Thank you

dzeedick@juniper.net