Corporate Citizenship and Sustainability – Supply Chain

Juniper Networks sourcing and supply chain are outsourced to a worldwide network, the key elements of which are comprised of contract manufacturers (CMs), original design manufacturers (ODMs), component suppliers, warehousing and logistic firms, and recruiting firms. Our CMs and ODMs in all locations are responsible for all phases of manufacturing, from prototypes to full production, and they assist with activities such as material procurement as well.

Supply chain management and assurance are integral to our commitment to product integrity, customer service, and corporate responsibility—all of which uphold Juniper's greater commitment to build more than a network. Our outsourced model provides a tremendous opportunity and responsibility to encourage the adoption of responsible business practices throughout the business.

Two overarching priorities drive our supply chain management approach: responsible and sustainable practices, and supply chain security and resiliency. These are growing in importance as more of our customers are requiring responsible sourcing practices and transparency throughout the entire value chain, and initiating audits to monitor compliance, including requests from members of the Joint Audit Cooperation (JAC). The JAC is an association of thirteen telecom operators with the common goal of raising social, environmental, and ethical standards across the Information Communication Technology (ICT) supply chain.

Responsible Sourcing

Juniper's supply chain is an extension of Juniper's operations, and as such, we select manufacturing partners and suppliers who share our values and goals. They are valued partners who are instrumental in helping us bring the most innovative solutions to market, accelerating the adoption and subsequent benefits of those solutions. We recognize that we have both a tremendous opportunity and responsibility to encourage the adoption of more responsible and sustainable business practices among our direct and indirect suppliers.

More than 90% of all suppliers are managed through a direct agreement and have been selected using sourcing strategies drafted in coordination with our engineering teams. In reviewing suppliers, we assess the potential risk—large or small—that each one could pose to our supply chain or product shipment protocols.

Our Supplier Management Program is based on several key elements, including:

- **Supplier Performance Evaluation:** Juniper has developed the Supplier Excellence Framework and Business Continuity Maturity Matrix to evaluate suppliers. Supplier performance is monitored through verification and audit mechanisms, and results of the monitoring are communicated during business reviews.
- **Verification and Audit:** Juniper conducts risk assessments and announced onsite audits of its CMs, ODMs, and critical partners to assess and evaluate their performance to Juniper standards.
- **Certification**: Each Juniper Networks supplier must certify compliance with Juniper's Business Partner Code of Conduct, which addresses important corporate social responsibility standards and compliance requirements and is informed by the Responsible Business Alliance Code of Conduct and the Ten Principles of the United Nations Global Compact. As Juniper refreshes supplier master service and purchase agreements, the Business Partner Code of Conduct is integrated into contracts and, thus, further emphasizes expectations of ethical behavior.

Vetting and Monitoring Suppliers

Juniper seeks suppliers who are committed to fair labor practices, ethical human rights standards, and making a positive impact on society. As part of our vetting process for all new suppliers, Juniper uses an onboarding process that includes financials, compliance and risk assessments, and background checks.

During the course of our engagement, we monitor Tier 1 suppliers who represent at least 80% of our direct material expenditure and 100% of our CMs and ODMs to verify their level of compliance with the Responsible Business Alliance (RBA) and the Juniper Business Partner codes of conduct. Additionally, Customs-Trade Partnership Against Terrorism (C-TPAT) security audits are conducted at critical supplier sites. Monitoring activities include one or more of the following techniques: supplier self-

Supplier Excellence Framework. Our Supplier Excellence Framework is designed to set clear expectations for the nine metrics we use to monitor and manage our suppliers: quality; account support; service; delivery lead time; compliance, sustainability, and risk; measurable execution; competitiveness; speed and agility; and innovation. The goal is to create productive, long-term relationships that align with our vision, values, and business objectives. The nine categories give suppliers direction and incentive about ways to improve their processes in order to grow their business with Juniper.

Business Continuity Maturity Matrix. Juniper ranks and tracks supplier performance along a continuum toward world class. In the area of business continuity, Juniper measures suppliers in four areas:

- Management commitment to a business continuity program (BCP)
- BCP readiness in production, key personnel, and test equipment
- Selection and readiness of alternative locations
- BCP structure, documentation, and training

For each of these areas, suppliers are measured and tracked for their progress in driving from basics to world-class. Key elements that Juniper tests for include: the degree to which management is involved and committed to demonstrating world-class performance in BCP; how proactive is the supplier's planning versus just reacting when a crisis occurs; and are key players who would be called upon in a crisis identified and do they know their roles during an event.

assessments, risk assessments, declarations and certifications, and announced onsite audits. To evaluate the risk in our supply chain and that associated with individual suppliers, Juniper takes into consideration factors such as past audit performance, type of operation, level of partnership with Juniper, and risk level based on the geographic location of an operation or facility.

Announced onsite audits at our CM, ODM, and critical component supplier facilities are crucial to the success of Juniper's supplier program. Annually, we conduct corporate social responsibility (CSR), security, and loss prevention audits at 100% of our CM and ODM facilities, and, based on risk assessment results and incident and performance trends, at select Tier 1 component and logistics supplier sites. Since 2015, we have formalized this process to better align with industry standards, including the RBA assessment and Validated Assessment Process (VAP). All audit findings are tracked to closure in accordance with our corrective action process, with priority focus placed on the following issues if identified, up to and including supplier termination:

Labor

- Child labor
- Forced labor
- Bonded labor
- Inhumane treatment

Health and Safety

- Imminent health and safety issues
- Imminent environmental risks

Ethics and Governance

- Falsifying records
- Bribery

When an issue is identified at a supplier facility, Juniper requests an action plan with identification of root cause, corrective actions, target closure dates, and responsible party. Suppliers are requested to provide status updates until verification of closure.

Juniper is starting to look beyond just Tier 1 suppliers to include Tier 2 and 3 suppliers in the audit process as well. The goal is to have more assurance and oversight of our supply chain, to continually monitor and drive performance improvements on CSR and security, and to uphold contractual and RBA membership requirements.

Juniper's Business Partner Code of Conduct and Human Rights

The Juniper Business Partner Code of Conduct is woven into our contracts. It outlines our expectations for ethical business practices and compliance with laws; lays out our objections to human trafficking, involuntary servitude and child labor; and articulates our alignment with the RBA Code of Conduct on fair labor practices and human rights. Juniper has a zero-tolerance policy regarding child labor and forced labor. Further information on Juniper's anti-human trafficking and modern slavery program is available in our annual disclosure statement.

We adopted the RBA Code of Conduct in 2007, and in 2015, we became an RBA member. The RBA provides guidelines and resources to drive performance and compliance with critical CSR policies to ensure that working conditions in the electronic

industry supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally responsible. Juniper fully supports the vision, mission, and principles of the RBA and is committed to the industry's collaborative approach in applying leading standards and practices throughout the supply chain.

Conflict Minerals

Conflict minerals, often referred to as 3TG, include columbite-tantalite (coltan), cassiterite, wolframite, and their derivatives tantalum, tin, and tungsten, and gold. They are also defined as minerals that are specifically determined to be financing conflict in the Democratic Republic of the Congo or an adjoining country. For more than five years, Juniper has been supporting the development of industry tools and programs that provide a common means to report and collect due diligence information on the source and chain of custody of 3TG through our membership in the Responsible Minerals Initiative (RMI) and the RMI's predecessor.

We are committed to our continual engagement with our CMs, ODMs, and first-tier suppliers in order to advance their knowledge and capacity, so they can provide complete and accurate information on the source and chain of custody of 3TG used in the products provided to Juniper. Given our downstream position in the supply chain, such that we do not have any direct relationships with the smelters or refiners in our supply chain, we rely heavily on our first-tier suppliers to provide information about the sources of 3TG used in our routing, switching, and security hardware products.

We expect our suppliers to exercise due diligence, source responsibly from certified conflict-free smelters, and support Juniper's compliance obligations, including trade compliance laws and trade restrictions from sanctioned entities and persons. More information on our disclosure of conflict minerals is available here.

CDP Carbon and Water Disclosures

As an extension of our own measurement and reporting on greenhouse gas (GHG) emissions and water usage, Juniper requests 100% of our CMs, ODMs, and those suppliers representing at least 80% of our consolidated total direct expenditure, to measure, disclose, manage, and reduce their carbon emissions and water consumption.

Specifically, we encourage these suppliers to disclose annually their performance and progress through CDP, which is a global standardized mechanism by which companies report their GHG emissions and water consumption to institutional investors and customers. For more than a decade, we have voluntarily disclosed our own climate and water impacts annually through CDP. Additionally, we were a founding member of the CDP's Supply Chain program and have built a strong supplier engagement platform in order to drive disclosure and action on climate-related risks.

Supply Chain Resilence and Security

Because Juniper relies on contract and original design manufacturers from around the world, ensuring the integrity of their work as suppliers is of highest importance. The company implements a supply chain integrity program to ensure physical security, intellectual integrity, and customer confidentiality. We do so by conducting regular tests, dissecting potential areas of vulnerability in the manufacturing process, and making improvements.

Juniper ensures that all components built into our systems are traceable and have process accountability, both of which improve component integrity. Those systems also create the means to do failure analysis on products or processes when quality problems arise. In fact, the same processes and tools meet a myriad of corporate objectives—from sustainability and social responsibility to supply chain continuity and security.

Because Juniper supplies more than 20,000 customers—including 47 of the Fortune Global 50, 44 of the top 50 global financial banks and insurance companies, and the world's top five social media properties, as well as major telecom, cable, and cloud providers—we hold the authenticity and security of our products to the highest quality standards. We work with the United States and other governments around the world to meet and exceed security standards and ward off attempts by adversaries to influence the integrity of our products.

To thwart terrorists, the U.S. government and the European Union have established standards via C-TPAT, a voluntary supply chain security program led by U.S. Customs and Border Protection that is focused on improving the security of private companies' supply chains with respect to terrorism. In our commitment to build more than a network, Juniper has incorporated these standards and security requirements into our supply chain management. Juniper's supply chain security program complies with the C-TPAT and Authorised Economic Operator (AEO) Program in the European Union. Implementing these security standards in the import supply chains not only enhances the security of cargo entering the U.S. and the European Union, but also shortens customs clearance times and results in fewer customs inspections, reducing the time to customer.

Supply Chain Risk Management

To evaluate potential risks within our supply chain, Juniper proactively maps and monitors our global network of suppliers. Doing so empowers us to better respond to supply chain occurrences and proactively prepare for any what-if situations that may arise.

To improve our global supply chain resiliency and maintain business continuity, Juniper implemented a supply chain risk management system. The system monitors 365 different types of events that are destabilizing, such as natural disasters, labor strikes, factory fires, political upheaval, or power outages; and tracks the products, parts, and revenue that would potentially be impacted. This information, coupled with data collected from key suppliers that maps components to production factories,

allows Juniper to instantly see and predict critical events and the severity of impact to the supply chain. With these notifications, Juniper can immediately contact suppliers to understand potential impacts to delivery and, if needed, create mitigation plans. The proactive risk mitigation planning dynamically assesses resiliency; financial, location, and recovery risks; and revenue impacts. The real-time data helps the operations team make strategic decisions, which maximize uptime throughout the entire supply chain and minimize trade-offs. Additionally, Juniper is able to simulate disaster events and run recovery drills. This robust information gathering and contingency planning allows the company to identify and respond to potential crises in order to avoid losses.

We are currently developing a customized risk score at the component and product level, modeling the risk to our finances and business continuity, which we plan to introduce in the near future. The information gleaned from it will help us when developing new products as the risk to the supply chain is more important at earlier stages. The matrix profile gives us clear definitions on how to get to each next step.

Supply Chain Security

Our strategy regarding supply chain security is three-pronged: we focus on brand integrity rather than brand protection; we are customer focused; and we take a life-cycle approach.

Brand integrity is proactive, whereas conventional brand protection strategies tend to be reactive. In conventional brand protection, for example, the focus would be on identifying and investigating counterfeit products and tracking down the criminals. This approach does not address the root causes or conditions that allowed counterfeit products to enter the marketplace in the first place. Brand integrity requires life-cycle threat modeling that identifies and proactively addresses weak points, from product development through production to shipping and warehousing.

Given that our primary manufacturing partners are global companies with factories all over the world, including the U.S., Mexico, Malaysia, and China, we conduct a detailed analysis on the ability of a foreign government or foreign entity to impact the activities at a facility, no matter where it is located.

On behalf of our customers, we carefully manage and audit:

- Whether those products are authorized by the manufacturer
- Our requirement that suppliers contract only from authorized channels
- The documented origin of the product and who has touched the product in the distribution process
- Whether the legitimacy of the product has been confirmed with the manufacturer

When the design and production processes are largely invisible and the resulting output is boxed products, it is difficult to have a high level of certainty that nothing has been compromised or corrupted. To mitigate this process challenge, Juniper breaks the product life cycle into smaller and more transparent pieces, each of which is tested for potential weaknesses. All component parts are evaluated according to the importance of their security to a Juniper product. Level A goods that impact the security of programs or products undergo greater scrutiny and control over their supply chain and shipping security.

Juniper's supply chain program is evolving quickly as we work with industry partners, customers, and governments to identify new and emerging risks, and collaborate on best practices to mitigate those risks.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3000098-001-EN Jan 2018