JUNIPER
NETWORKS

"CYBERSECURITY: AN EXAMINATION OF THE COMMUNICATIONS SUPPLY CHAIN"

Statement of Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection

before the

Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives

Tuesday, May 21, 2013

EXECUTIVE SUMMARY

The Challenge

The government views its commercial supply chain as a major element in its risk profile, but many of its risk management efforts are not coordinated and were not developed in collaboration with industry even though industry also is concerned about supply chain security.

The government continues to make purchases from untrusted and unauthorized sources. The incentive to save money pushes agencies to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers (OEM). This also is an area where much mischief takes place from both counterfeiters and those attempting to penetrate the government supply chain with malicious equipment.

When the government purchases equipment from unauthorized sources and then identifies it as counterfeit, it often assumes the OEM had a gap in its supply chain. The government does not instead ask why it bought sensitive ICT products from an untrusted source.

Industry Initiatives

While Juniper understands the importance of improving supply chain assurance for the Federal government, it often appears that the government does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain.

Juniper Networks has a supply chain assurance and brand integrity program for securing our products and supply chain. We employ best practices for supply chain security from organizations regarding component integrity; traceability of products; anti-counterfeit features; supplier selection; physical security; information and IP security; and channel monitoring and incident response. Finally, we work with industry partners and the government to identify emerging risks and on best practices to mitigate those risks.

Recommendations

1. The Government Should Purchase from Authorized and Trusted Sources
2. The Government Should Require that Small Business Vendors be Certified as Authorized Resellers and Partners
3. Enact Information Sharing Legislation as a Means toward Situational Awareness
4. Share Information about Tactics, Techniques, and Procedures More Broadly
5. Establish Incentives for Businesses to Certify their Security Practices
6. Education and Awareness Campaign

Good afternoon Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee. Thank you for inviting me to be a participant in today's hearing on the cybersecurity of the communications supply chain.

Background

My name is Bob Dix, and I serve as Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks. Juniper Networks is a publicly-held private corporation headquartered in Sunnyvale, California, with offices and operations around the world. We deliver trusted, high-performance networking and security solutions that help public sector agencies (spanning civilian, defense, and intelligence functions), private enterprises, and service providers deploy networks that are open, scalable, simple, secure, and automated. Juniper's portfolio includes software and systems for routing, switching, and security.

The Challenge

The government views its commercial supply chain as a significant element in its overall security risk profile; as a result, there are more than 100 different supply chain risk management efforts across the United States Government. Unfortunately, many of those efforts are not coordinated and were not developed in collaboration with private industry despite the fact that industry also is concerned about supply chain assurance (please see Attachment A).

I will address three aspects of this important subject of cybersecurity in the communications supply chain: first, the risk created by government procurement practices utilizing unauthorized equipment providers; second, supply chain integrity initiatives by industry generally, and

Juniper specifically; and third, several recommendations where the government can improve both government and private sector supply chain integrity.

Risky Procurement Practices

While industry is confronted with the challenge of monitoring and engaging with more than 100 different government supply chain risk management efforts, the Federal government itself continues to make purchases from untrusted and unauthorized sources on a routine basis. There was a well-publicized presentation in 2008 in which the FBI acknowledged that government agencies purchased networking equipment that was determined to be counterfeit through an online broker. This happens far too often, and we all know why this happens – it is about saving dollars.

There is an on-going culture across the Federal government, particularly at the program and project manager level, to be driven by cost and schedule. This is not malicious; it is just the way things have been for a long time. Many of our talented civil servants have their individual performance evaluations based on their ability to deliver projects and meet cost and schedule. This will often drive them to shop online to save dollars on a particular project. More often than not, this pushes them to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers (OEM). This also is an area where much mischief takes place from both counterfeiters and those attempting to penetrate the supply chain with tainted or malicious equipment. Counterfeiters know the government's acquisition practices and use it to their advantage – they set up small gray market entities to sell equipment cheaply and online. This situation could get worse given the current budget climate.

Interestingly, when the government purchases equipment and then identifies it as counterfeit, it often assumes the OEM had a gap in its supply chain - pointing fingers at the private sector when, in many cases, they need to be looking in the mirror. The government does not instead ask why it bought a sensitive piece of IT hardware from an untrusted source. Here are a few real world examples:

- In April 2013, a Federal civilian agency issued a solicitation for maintenance of its Juniper Networks equipment. The Statement of Work that the Bureau issued with the solicitation states "Support has to be from Juniper directly or a Juniper approved support partner. This allows for diagnostics in order to determine the problem areas of the equipment and fast replacements of any parts that might fail." Approximately one week after the solicitation and Statement of Work issued, the agency awarded the contract to a company that is not an authorized support partner of Juniper.
- In July 2012, a defense agency purchased what it thought were new Juniper router interface cards from Unauthorized Reseller A. When the agency received the products, the boxes were open, ant-static bags were torn, and the products appeared to have been tampered with. The agency contacted Juniper, and our investigation revealed that Unauthorized Reseller A had purchased used Juniper equipment from a broker and sold it to the government as "new." It should be noted that the agency devoted significant resources to conducting a risk assessment with Juniper on the integrity of our products (presumably assuming that we were at fault), but this effort was rendered superfluous once it was determined that the agency had procured interface cards from an unauthorized entity.

- In October 2011, one of the military departments awarded a purchase order to Unauthorized Reseller S for Juniper Networks products. We contacted the military department and advised them that Unauthorized Reseller S was not authorized by us, but the buyer wanted to continue with the purchase because Unauthorized Reseller S was cheaper. In our investigation, we discovered that Unauthorized Reseller S was not a registered company; instead, it was a fictitious business name established by the individual owner of a previous business. The individual established the fictitious business name Unauthorized Reseller S following his 2011 release from prison for a conviction for trafficking in counterfeit network hardware. Once we provided this information to the military department, the department canceled the purchase order in favor of an authorized Juniper partner.

Industry Initiatives

While Juniper understands the importance of improving supply chain assurance for the Federal government, it often appears that the government does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain from concept to delivery. It is important to the business interests and brand reputation of Juniper Networks and other vendors and providers to maintain a productive and robust approach to supply chain security.

In fact, corporate supply chain integrity and assurance programs evolved at a very early stage in the technology sector, starting with the semiconductor industry in the early to mid 1980s when outsourcing of semiconductor packaging and assembly began occurring in many countries in Asia. These efforts continue and have been expanded partly due to high levels of chip theft in the semiconductor transport industry and high levels of substandard product remarking, reselling, and gray marketing (please see Attachment B for a more comprehensive list of such efforts).

At a very early stage in our history, Juniper Networks established a formal supply chain assurance and brand integrity program for securing our products and our supply chain. The Juniper brand integrity program is one component of a comprehensive corporate security plan. At Juniper, we believe brand protection programs are inherently reactive to problems discovered in the channels. Juniper's philosophy has been to implement security and integrity best practices throughout our product lifecycle process to prevent instances of counterfeit products or components, and to ensure that our customers receive the highest quality products available in the marketplace.

Juniper references numerous international standards in the operation of its supply chain and brand integrity programs, including:

- ISO 27001 for information security
- ISO 9001 / TL9000 Quality management system (Certified)
- C-TPAT and AEO supply chain security criteria (Certified Tier 3 C-TPAT and AEO- Security)
- Common Criteria product certifications

We also employ best practices for supply chain security from organizations such as The Open Group Trusted Technology Forum (O-TTF); the Alliance for Gray Market and Counterfeit Abatement; and the Software Assurance Forum for Excellence in Code (SAFECode). Some of these best practices include: component integrity assurance; traceability of products and components; anti-counterfeit features within our products; supplier selection (including an evaluation of foreign interests, relationships, and potential for foreign control); physical security; information and IP security; and channel monitoring and incident response. Finally, we work with our industry partners and the government to identify new and emerging risks and collaborate on best practices to mitigate those risks.

Recommendations

As is clear from the variety and breadth of standards bodies and organizations that industry relies on, many companies believe that a variety of standards and best practices contribute to supply chain integrity; but, as discussed earlier, there also is compelling evidence that there are gaps and contradictions in the government's policy and practices that contribute to supply chain risk. Here are a few proposals that, if addressed, could have immediate impact on securing the communications supply chain:

1. The Government Should Purchase from Authorized and Trusted Sources

The Executive Branch should issue a directive requiring Federal departments and agencies to purchase only from trusted and authorized sources unless there is a compelling reason to go outside of that channel. If there is a compelling need to purchase from unauthorized vendors, such as for obsolete parts, the government should issue a written Justification & Authorization (J&A) and assume the liability of such a decision. In conjunction with this, acquisition officers should be evaluated based on their ability to procure goods and services that deliver the best value for the government over the long term instead of those that appear to be the lowest price in the short term; a product that is less expensive in the short term might end up costing more over the long term as a result of additional maintenance, more frequent replacement, higher energy costs, etc. Together, these reforms would mitigate a significant amount of the government's supply chain risk.

2. The Government Should Require that Small Business Vendors be Certified as Authorized Resellers and Partners

Requirements pertaining to small business set-asides also have the secondary impact of causing procurement officers to pursue acquisitions through gray market providers who often are not part of the authorized and trusted supply chain; gray marketers set themselves up as small businesses. While Juniper Networks understands the importance of small businesses to the government's industrial base and to the economy in general, it is important to recognize that bad actors often exploit our reliance upon small business as a means of entry. Counterfeiters and others attempt to introduce their tainted equipment into our critical infrastructure through small business enterprises.

Companies like Juniper Networks welcome and value the opportunity to work with small businesses. We have programs that invite participation by small business providers to become part of the authorized and trusted network of resellers and partners. The government should require that all of its vendors, including small businesses, be authorized to resell the equipment they are providing.

3. Enact Information Sharing Legislation as a Means toward Situational Awareness

Many of the Members of this Committee have been involved in attempting to address the issue of facilitating the exchange of intelligence information and creating a true partnership between government and industry to build enhanced situational awareness to improve detection, prevention, and mitigation of cyber events that may become incidents of national consequence.

Though the private sector is doing work internally to address the threat, the government has an important opportunity to significantly increase its communication of threat indicators and intelligence to industry. Far too often, the government continues to compartmentalize and restrict access to relevant information. In order for private industry to be able to prevent and mitigate threats, industry must have access to the threat information that the government possesses.

With this in mind, legislation introduced by a Member of this Committee, Rep. Mike Rogers (R-MI), in his capacity as Chair of the Permanent Select Committee on Intelligence, H.R. 624, the "Cyber Intelligence Sharing and Protection Act of 2013," would amend the National Security Act to facilitate the sharing of cyber threat intelligence with eligible private sector entities. This legislation will add an arrow to the protection quiver by addressing a key impediment to building cyber situational awareness and passed the House on a wide bipartisan margin. Juniper Networks hopes that you will join with your Intelligence Committee colleagues in urging the Senate to take up this important bill.

4. Share Information about Tactics, Techniques, and Procedures More Broadly

While we are working on legislation to break down barriers to improving timely, reliable, and actionable situational awareness, there is a step we could take immediately. We continue to hear that the government has significant concerns about supply chain and the threat to national and economic security. The government has access to case studies of successful, unsuccessful, interrupted, or disrupted attempts to perpetrate network intrusions through the supply chain. We should take the lessons learned from those experiences, and share the tactics, techniques, and procedures (not sources and methods that cross over into the classified space) that we can learn from and better inform the community in their own risk management decision making.

5. Establish Incentives for Businesses to Certify their Security Practices

As part of its procurement evaluation process, the government should examine incentives that would provide recognition to companies that choose to have their security processes and practices certified and accredited by recognized standards bodies. Most businesses already manage their security risk but might not seek to have their practices certified because there is no customer incentive to do so. If a large buyer, like the government, were to recognize such certifications, more businesses would potentially be incentivized to apply for them.

6. Education and Awareness Campaign

As we are all aware, the inadvertent introduction by employees and contractors of malware is one of the primary sources of infection adversely impacting cybersecurity. The communications supply chain is no exception to this problem and a larger effort to combat this has benefits in and beyond supply chain integrity. The government should develop a coordinated and long-term education and awareness campaign for cybersecurity. When our Nation was confronted with the threat of the H1N1 virus, the government mobilized agencies and the private sector to advise individuals how to protect themselves from the risk of infection. There were public service announcements, posters, radio, TV, and Internet messages regarding the need to cough into our sleeves, wash our hands, and other protective measures to secure our health. The effort included the CDC, HHS, and other federal departments and agencies, along with many non-profits, businesses, and organizations.

We have the opportunity to use the same model for a sustained awareness program to help educate citizens, small businesses, students, non-profits, and other stakeholders on how to protect themselves from the risk of malware, phishing and other forms of infection in cyberspace.

Many Federal departments and agencies routinely interact with citizens and businesses. Leveraging the Small Business Administration; the Internal Revenue Service; the U.S. Postal Service; the U.S. Department of Education; and others would provide an ability to scale the messaging across a wide range of the population. Perhaps we could even convince every Member of Congress to include a link on their website that directs constituents to where they can get more information about protecting their health in cyberspace.

Conclusion

On behalf of the more than 9,000 proud employees of Juniper Networks, thank you again for this opportunity to participate in this important discussion. Industry looks forward to continuing the collaborative relationship with Congress and the Administration on this important issue.

APPENDIX A

1. In February 2013, the President issued a cybersecurity Executive Order.

2. Recently-enacted editions of the National Defense Authorization Act (NDAA) and the Intelligence Authorization Act contained provisions that provide the government with expanded authority to exclude private sector vendors from eligibility for Federal procurements based on a presumed national security risk without notice.

3. In 2011, the Department of Commerce, acting on behalf of the Department of Defense, distributed surveys to industry under the auspices of the Defense Production Act (DPA). The Defense Supply Chain Network survey (or sector-by-sector, tier-by-tier evaluation (S2T2)) asked for sensitive and proprietary company information and suggested the threat of jail time for failure to comply.

4. In 2011, the U.S. Intellectual Property Enforcement Coordinator issued a request for comments as part of an inter-agency effort to reduce counterfeit products from the U.S. Government supply chain.

5. In 2008, there was a Federal Acquisition Regulation proposal to impose unlimited liability against private sector providers if counterfeit equipment was found in the government's operation, even if that equipment was not from a manufacturing or assembly facility of the named provider.

6. Supply chain activities taking place pursuant to the Comprehensive National Cybersecurity Initiative (CNCI) #11 have not included private sector participation.

APPENDIX B

1. Transported Asset Protection Association (TAPA) (originally the Technology Asset Protection Association)

2. High-Tech Crime Investigators Association (HTCIA)

3. ASIS International

4. International Security Management Association (ISMA)

5. Coalition Against Counterfeit and Piracy (CACP)

6. CSO Roundtable

7. Internet Consortium for Advancement of Security on the Internet (ICASI)

8. Information Sharing and Analysis Centers (ISACs)

9. Sector Coordinating Councils (SCCs)

10. The Partnership for Critical Infrastructure Security (PCIS)

11. The President's National Security Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC)