Written Statement of
David M. Rothenstein
Senior Vice President, General Counsel and Secretary
Ciena Corporation

Before the Subcommittee on Communications and Technology
House Committee on Energy and Commerce
Hearing on "Cyber security: An Examination of the Communications Supply Chain"

Introduction

Chairman Walden, Ranking Member Eshoo, Members of the Committee, my name is David Rothenstein and it is my pleasure to appear before the Subcommittee this afternoon examining the intersection of cyber security and the supply chains of companies who operate and who supply equipment for communications networks.

Company Background

I serve as Senior Vice President, General Counsel and Secretary of Ciena Corporation, a Hanover, Maryland, based global provider of equipment, software and services that support the transport, switching, aggregation and management of voice, video and data traffic on communications networks. Our Packet-Optical Transport, Packet-Optical Switching and Carrier Ethernet Solutions products are used in communications networks operated by service providers such as AT&T, CenturyLink, Verizon, BT (also known as British Telecom), SingTel (Singapore's telecommunications company) and Telefonica Vivo (the largest mobile operator in Brazil); by cable operators such as Comcast and Rogers; and by research and education institutions, enterprises and other network operators around the globe.

In addition to ongoing projects with the world's largest service providers, some recent examples of our work include:

- provision of converged packet-optical and packet networking solutions to Integra, a provider of fiber-based, carrier-grade networking solutions based in Portland, Oregon, for the expansion of its long-haul fiber optic network; and
- an award to power the Illinois iFiber optical network, which is designed to service small business, local governments and universities in northwestern Illinois.

In addition, through our government solutions subsidiary, Ciena is a direct and indirect supplier of networking equipment, software and services for some of the United States' most critical government infrastructure projects. Since 2004, Ciena has provided the optical transport equipment for the U.S. Department of Defense's Global Information Grid Bandwidth Expansion (GIG-BE) Program, a net-centric transformational initiative to provide high-speed communications capability to key operating locations worldwide. In 2011, Ciena partnered with Internet2, a non-profit community of universities, companies, government agencies and others, on a 100G national network in support of the U.S. Unified Community Anchor Network (U.S. UCAN) project. And, Ciena has built assured, adaptive optical networks for a number of U.S. armed services base infrastructure projects and provided managed services for the networks of several U.S. government agencies and various state and local governments.

Ciena was founded in 1992 with the desire to radically change the possibilities and economics of networking. Over 20 years later, we have accomplished that objective, becoming an innovator in delivering solutions that enable converged, next-generation architectures around the world. Today, a number of market trends – including the proliferation of smartphones, tablets and similar devices running mobile web applications; the prevalence of video applications; and the shift of enterprise and consumer applications to cloud-based or virtualized network environments – are indicative of increasing

use and dependence by consumers and enterprises on a growing variety of broadband applications and services.

This significant increase in multiservice network traffic will require network operators to invest in next-generation, high-capacity network infrastructures that are more robust and efficient. Accordingly, Ciena's network architecture vision and approach, which underpins our solutions offerings and guides our research and development strategy, leverages the convergence of optical and packet networking technologies to increase network scale cost effectively, while emphasizing software-enabled programmability, automation and open interfaces. Through this network approach, we enable high-capacity, configurable infrastructures that can be managed and adapted by network-level applications to create new communications services, and that provide flexible interfaces for the integration of computing, storage and network resources. By increasing network flexibility for service delivery, reducing required network elements and enabling increased scale at reduced cost, our communications networking solutions create business and operational value for our customers. Simply put, our equipment, and that of our peer vendors, makes up the backbone of the global communications infrastructure. And we are enabling more people to use it with more devices at higher speeds, and more reliably, than ever before.

Our success is driven by our innovation. Years of creating solutions for the world's largest and most reliable communications networks have led to more than 1,550 U.S. patents and patent applications, as well as more than 500 foreign-issued patents and patent applications. Like many technology companies, patents are our life blood, and enable us to innovate quickly and get new products into the global market.

Cyber Security and Supply Chain

In order to support this continuous innovation, and because our equipment serves as the core of communications networks around the world, Ciena's executive leadership team spends a lot of time looking at the issue before the subcommittee today – the intersection of cyber security and supply chain. It is a topic on the minds of all of our existing and prospective customers, particularly the service providers, and we aggressively seek their input and perspectives in order to learn what they value in their suppliers and in their networking equipment.

The stated goal of our supply chain operations team is to implement a "value driven" supply chain, one which drives changes that will create value for Ciena and for our customers. A key aspect of the success of such a model is the ability to manage the inherent complexity of the supply chain while ensuring a positive and differentiated customer experience. We have heard from our customers, and they clearly value things like performance against shorter product delivery lead times, outstanding product quality and performance, security of supply, and product security and reliability.

Based on that feedback, we have undertaken a number of actions to transform and optimize our supply chain over the past few years. These actions were taken from both a business and a security perspective, as we operate in a very competitive global marketplace with competitors many times our size.

One way we use our supply chain to differentiate ourselves from our peers is by trying to be faster to market. For example, we implemented a "direct order fulfillment" (DOF) model for several of our products. Under this model, we select contract manufacturers whose facilities are located closest to our primary North America market and require the manufacturers to perform final assembly and testing of

our products and to ship the products directly to our customers. By eliminating a key step in the process, the DOF model allows us to improve our supply chain velocity and ensure performance to stated product delivery lead times in a very cost-efficient manner. Similarly, we consolidated our global logistics partners to ensure a simpler model that is geographically closer to our primary market and has cleaner and more optimized shipping lanes.

In addition to assessing our overall supply chain with the goal of improving velocity and cost, we also focused on how best to design, build and manufacture equipment and software that meets or exceeds the security and reliability needs of our customers. Given all of the news of cyber security intrusions, vulnerabilities, intellectual property infringement, data exfiltrations and the like, many parts of our customer base have been aware of the issue for some time and continually press us on issues relating to product security, integrity and assurance.

I am sure that the Members of this committee are well aware of the increasing prevalence and severity of cyber threats directed against our government and U.S.-based defense contractors, critical infrastructure owners and operators, and high technology companies, including those threats that emerge every day from China. Our government and several private sector organizations, including security firm Mandiant, have documented this very well, and it is not necessary to belabor the point. Suffice it to say that as a company selling equipment and software that sits in the core of critical communications network infrastructure, we began to question the level of supply chain exposure to the design and manufacture of key products originating in China.

With all of this in mind, we undertook a comprehensive analysis of our supply chain and considered a range of issues, including:

- the amount of the supply chain originating in China as compared to other countries around the world;
- the portions of our products that we considered to be particularly vulnerable from a security standpoint;
- the alternate sources of supply for those products, both in terms of companies and geographies;
- proximity to our key North America market;
- the cost impact of any transition, including labor and overhead costs;
- the relative political and social stability of various locations; and
- the potential impact of any transition upon product test capacity, lead times, quality or performance.

As a result of this analysis, in the middle of 2011 we made a conscious decision to begin a gradual exit of key elements of our supply chain from China. At the time, over one-fifth of our global supply chain spend on contract manufacturers originated in China, and approximately two-thirds of our global spend on finished and semi-finished assemblies originated from the China-based facilities of original equipment manufacturers.

Obviously, this was not an easy decision. China represents one of the largest and fastest growing markets for communications networking equipment in the world. And, with a very low cost manufacturing base, China is also home to the manufacturing facilities that produce many of the components and subcomponents that go into our products. However, based on what we knew about our products, our customers and the overall business and security environment in China, we decided to make this change.

In making this decision, and in contrast to some of our peers, we were not as concerned about the potential impact on our sales opportunities in China. Several years ago, we made the deliberate decision not to pursue a go-to-market sales strategy in China. Because well over 90% of networking equipment sales into the China market is controlled by Chinese equipment vendors, and because of domestic production requirements that require the transfer of intellectual property that we were not willing to entertain, we determined that the barriers to entry into the China market were too high to pursue meaningful sales opportunities in that country.

We are now two years into this aspect of our supply chain transformation. During this time, we have made substantial progress toward our goal of increasing the velocity of our supply chain and the security and assuredness of our products. By the end of 2013, we will have effectively moved all of the manufacture and assembly of our products out of China, and we will have reduced our global spend on finished and semi-finished product assemblies originating from China to less than one-half. We have effectively transitioned these elements of our supply chain to other jurisdictions – primarily Mexico and Thailand – that offer a combination of increased time-to-market, improved security of supply, and increased product security and reliability. For example, with approximately 85% of our global contract manufacturer spend now based in Mexico, we have decreased our product lead times, with the products being driven by truck across the U.S. border as opposed to being sourced from China and then sent via maritime container ship to the U.S. At the same time, by partnering effectively with our contract manufacturers and aggressively pursuing cost reductions though lower labor and landed cost rates, we have not incurred a significant increase in the cost of our products. We have remained competitive in the market from the standpoints of technology, delivery and cost, and we continue to win business from existing and new customers and take market share.

With respect to those finished or semi-finished assemblies that remain sourced from China today, we are in active discussions with our major vendors as to their plans for transitioning out of China. As a result, we expect the overall percentage of products originating from China to continue to decrease over time.

We remain focused on this effort primarily to reduce the risk of intellectual property infringement and the incorporation of counterfeit components into our products. Until then, we believe that continuing to source several specific products from China presents low risk from a security, integrity and reliability standpoint. These finished and semi-finished assemblies, such as optical passive modules, power rectifiers and mechanical assemblies, are largely “passive” products in that they are neither programmable nor capable of being embedded with damaging computer code or malware. In an abundance of caution, though, we perform system field tests on most of these products prior to deployment.

Similarly, there remain certain parts used in our products – such as capacitors (which are used to store energy), heat sinks (which cool electronic devices) and filters, often collectively referred to in the industry as “jellybean” or “peanut” parts – for which we have not attempted to transition the supply chain out of China. Because the source of supply for these parts is limited only to manufacturing facilities in China, we expect to continue procuring them from China. However, as these parts are incidental to the actual functionality of the products and are neither programmable nor susceptible to being compromised in any way from a security standpoint, we are confident that they present very limited risk to the overall integrity and security of our products.

Separately, we have taken extensive steps to ensure the security and reliability of the "active" components in our products, such as programmable logic integrated circuits, analog integrated circuits, digital signal processors, field-programmable gate arrays and microprocessor integrated circuits. First, we ensure that all of these components are sourced from outside of China. For example, the key active components in WaveLogic 3, our industry-leading 100G coherent optical chipset, were designed and developed in North America and Europe. Second, we provide an approved vendor list to our contract manufacturers, who then procure these products and incorporate them into the assembly of our products. Third, we maintain rigorous internal practices and capabilities that enable us to identify any discrepancies in the performance, behavior and security of these component assemblies. And fourth, by implementing strict controls over our software development, and by performing the final testing and validation of the software loaded onto our products, we ensure the integrity and reliability of the critical element – software – that controls and manages our products and our customers' networks.

In taking these steps, we believe not only that our company has become more efficient and able to deliver products more quickly but also that our customers are getting more secure and trusted products. Indeed, we have received extremely positive feedback from many of our service provider and government customers in response to this element of our supply chain transformation. In sum, while we recognize that this supply chain strategy may not necessarily make sense for all other companies, it has worked quite effectively for Ciena and our customers.

It is fair to say, however, that many potential purchasers of networking equipment, software and services – particularly enterprises that buy equipment for their own networks – still do not appreciate the cyber security threats facing our nation today. That is why Ciena was pleased to support the Cyber Intelligence Sharing and Protection Act, HR 624, authored by committee member and House Permanent

Select Committee on Intelligence Chairman Mike Rogers, and Ranking Member Dutch Ruppersberger. We believe that broader sharing of cyber threat information would be particularly valuable for the many private sector companies, particularly those in the critical infrastructure area, who demand trusted and secure networks but do not have access to the same level of information and resources as the largest communications service providers and governments.

Conclusion

In conclusion, Ciena applauds the subcommittee for taking on this issue of cyber security and the communications supply chain. As you now know, Ciena elected not to wait for legislation, regulation, or implementation of the Obama Administration's Executive Order on cyber security, to make changes in its supply chain. Instead, we talked to our customers, conducted a thorough business analysis and risk assessment, and made a decision that has been and is continuing to be implemented today. We are confident that taking these steps makes good business sense for our company and delivers additional security for our customers and their networks.