House Committee on Small Business
"Foreign Cyber Threats: Small Business, Big Target"

Testimony of Nova Daly
Senior Policy Advisor, Wiley Rein LLP, Washington, DC
July 6, 2016

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to appear before you today.[1]

In this age of the Internet, we have never had so much opportunity and with it so much risk. Today, I offer my perspective on cyber security, broadly, and distinctly as it pertains to small businesses. This perspective is drawn from my experience as a former official with the U.S. Department of Treasury administering the Committee on Foreign Investment in the United States ("CFIUS"), work at the National Security Council, and my ongoing efforts in the private sector with my colleagues at Wiley Rein to address these issues as they impact U.S. companies.

As this Committee knows, cyber security issues are clearly significant and growing economic risks for small business and Americans broadly. These issues have become increasingly relevant as we now allow and depend upon Internet access and connectivity in nearly every aspect of our work and lives, from the communication and processing devices we use at home and work, to the vehicles we drive, the infrastructure on which we depend, and even the appliances in our homes.

It has been forecast that, on average, 5.5 million new devices are connected to the Internet each day and, by 2020, over 20 billion devices will be connected to the Internet.[2] For small businesses, the very connectivity that allows greater freedom and versatility in conducting

[1] The views and opinions expressed in this statement are mine and do not necessarily reflect the views or opinions of Wiley Rein LLP or any of its clients.
[2] *See* http://www.gartner.com/newsroom/id/3165317

day-to-day business –linking phones, computers, routers, copiers, and even alarm and ventilation systems – also brings with it significant and sometimes paralyzing risk, risk that is often difficult to address both financially and in terms of human resources.

As small businesses increase their connectivity to the Internet, they face significant challenges and additional costs, not just in infrastructure and the 'nuts and bolts' of establishing businesses' connectivity, but also security-related costs. Both domestic and foreign criminals, as well as foreign governments, have been known to exploit and are actively targeting internet-based vulnerabilities in order to gain access to financial information, customer data, and intellectual property. Indeed, three years ago, a study issued by the Center for Strategic and International Studies estimated that the annual cost of cybercrime in the United States was approximately $100 billion. According to more recent reports, cybercrime costs quadrupled since then, and we are on target for still another quadrupling of these costs from 2015 to 2019.

While large U.S. businesses typically have the means to fund and invest in strong and resilient cyber security measures to protect their interests, small businesses generally do not have this luxury. They often lack the capabilities and/or the resources to pursue strong, entity-wide cyber security protections. Further, small businesses often may not be privy to the kinds of broad, industry-wide threat notifications to which larger companies may be. Often, larger companies have the resources to continually monitor and review threats that may arise from certain technology and supply chains, and at times are contacted by the U.S. government when breaches occur. A notable example was the 2014 Department of Justice investigation and prosecution of several Chinese military officials, who were responsible for breaches of numerous U.S. companies' security perimeters. There, at least some of the affected companies were contacted and alerted as the breaches were occurring. However, given the breadth of

existing cyber threats and the continuing growth of cybercrime, our government simply does not have the resources to address all of the cyber security-related issues faced by business, critical infrastructure, and governmental systems, much less those faced by small businesses.

In 2012, the House Permanent Select Committee on Intelligence issued a report on its findings regarding counterintelligence and security threats posed by certain telecommunications companies doing business in the United States. Despite the report's negative findings, the companies investigated continue to grow as dominant players in the global telecommunications market. While it has been effectively restricted from selling network equipment to tier-one U.S. wireless carriers, Huawei is growing its sales to smaller wireless carriers in the United States, supplying network infrastructure equipment to cities in the states of Washington and Oregon, and is targeted to continue growth in cell phone sales in the U.S. market. Last year, ZTE another of the investigated companies, was the fourth-largest smartphone vendor in the United States, with a 7.2% market share. In the fourth quarter of last year, the single largest market for ZTE smartphones was the United States. These companies also sell tablets, routers, hotspots, data storage, and cloud computing infrastructure and services, all of which are used by small businesses.

Although larger U.S. companies can engage other vendors to provide certain cyber security monitoring and reinforcement of their security perimeters, small businesses often do not have the funds or capacity to do so. Notably, this year, ZTE was sanctioned, and according to reports, Huawei has been subpoenaed by the U.S. Department of Commerce for potential violations of U.S. export laws in sending controlled items to countries that have been designated as supporters of international terrorism, or are otherwise subject to U.S. trade sanctions and economic embargoes, such as Cuba, Iran, North Korea, Sudan, and Syria.

While doing business with such companies can present heightened risk, it should not be overlooked that there is significant and growing vulnerability within the entire U.S. technology supply chain. Increasingly, our telecommunications equipment and systems are produced or assembled abroad, and we are seeing nations taking strong measures to grow their own semiconductor and other technology industries. Further, the United States is finding itself with a talent shortage in cybersecurity know-how. Thus, there are also broader structural problems that should be closely addressed. Cyber security or insecurity, as compounded for small business, does have a correlation to the capability of our cyber work force and security of our entire technology supply chains.

So how do we ensure that small businesses are not left to fend for themselves in an increasingly hostile cyber world? For the consideration of this Committee I respectfully submit the following recommendations.

A focus on current laws. A continued focus on the enforcement of our export control, cyber and other national security laws, such as CFIUS, is appropriate. Understandably, when implementing restrictions that prohibit exports, reexports, and transfers (in-country) of items subject to the punitive action, an administration must take into consideration the broader effects that such actions will cause. However, ensuring that our laws are enforced against those who violate them sends important signals to the market. Such signals can make their way to small businesses, allowing them to be better served through purchases of products by vendors who follow the laws.

Promoting cyber standards. This Committee should continue to consider actions that build and promote industry-led cyber security standards in the framework of ISO standards, or otherwise, of best practice. Such standards could be applied to government procurement,

ensuring that government agencies access equipment from vendors that achieve acceptable standards of cyber security protection. Doing so could ensure that such equipment permeates to the private sector broadly and especially to small business. Agencies such as the Small Business Administration could help to educate small businesses on these standards so that they are aware of where best to turn for equipment and services that reduce their cyber risk.

Engaging small businesses. Increasing outreach and education to small businesses and finding appropriate funding so that they are aware of the risks to their systems and have the means to address that risk could be pursued. As part of those efforts, it would be useful to strengthen information-sharing initiatives between entities in order to provide small businesses with a more immediate understanding of emerging threats and patterns, and arm these businesses with the lessons learned from others. We could also consider ways to build incentives for purchasing safer equipment. Such market-based cyber incentives, whether in purchasing, insurance, or otherwise would help justify investments in cyber security. Profit-minded organizations must see clear benefits to their actions, as every dollar or hour spent on cyber security is not spent on the organization's core goals. These actions accompanied with industry norms and standards could highlight cyber security investments as requisite. Passage of H.R.5064, The Improving Small Business Cyber Security Act of 2016, would be important to these ends.

Addressing supply chain security issues and closing the cyber deficit. As noted earlier, given the global nature of technology production and cyber threats, we must find ways to address the threats that emanate from these supply chains. While important work is being done in the government and private sector to find and achieve the right answers, this should continue to be a focus of U.S. policy. Toward that end, and as has been widely reported, we have a

troubling cyber deficit in terms of talent and training here in the United States. We need to build the next generation of cyber technicians and engineers. If we do not build this capacity, it will be sourced from abroad, and doing so could put us behind the technology and innovation curve. One element that makes America strong is our ability to innovate, and that comes with building the next technologies. We need to reclaim that field.

Thank you very much again for the opportunity to testify before this Committee today on this important topic. I look forward to answering any questions that you may have.