Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Evolving Threats to the Homeland"

September 13, 2018

Jennifer Bisceglie
CEO and President of Interos Solutions, Inc.

Chairman Johnson (R-Wis.), Ranking Member McCaskill (D-Mo.), and Members of the Committee, thank you for the invitation and opportunity to speak with you today on the underappreciated threats to the homeland that, if not mitigated, could significantly damage the nation's critical infrastructure and/or disrupt people's lives, especially as it relates to the global supply chain and the use of information and communications technology, or ICT.

By way of introduction, Interos is a company I founded over 13- years ago to evaluate risks in the global economy and the business partnerships, alliances and distribution networks that comprise our supply chains. Interos is built on my over 25 years in the global supply chain industry, having helped numerous US-based companies off-shore their manufacturing and take advantage of different skillsets, labor pools and competitive business arrangements with partners around the world.

During those years, I've watched risk concerns in the supply chain transition and grow from quality, to physical security, to resiliency and now to include product integrity. Interos recently supported the U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION for their report ('the Report") on Supply Chain Vulnerabilities from China in the U.S. Federal Information and Communications Technology (ICT) which outlines several recommendations, the most important being that the U.S. establish a "National Strategy for Supply Chain Risk Management (SCRM) in U.S. ICT" with supporting policies, so that the Nation's security posture is forward-leaning vs reactive and based on incident response. Our adversaries have strategies they are executing; it's my opinion this is missing in the U.S. and providing easy opportunities for nefarious actors to drive up risk exposure and cost.

In being invited here, today, I'd like to address six (6) areas that are directly related to the Report and remain highly relevant to this hearing's discussion. However, I would like to stress that whether it is 5G, blockchain, the Internet of Things (IoT), or any other emerging technology or threat, an underlying foundation for security is an understanding of who the stakeholders are across your business partnerships, alliances and distribution eco-systems, where your vulnerabilities lie, - what's most important - and having a comprehensive strategy for security and risk management.

Given its position in the market, Interos has had the opportunity to work with many public and private sector organizations across industries and the situation is always the same – if the organization's leadership doesn't take a focused and comprehensive approach to risk management - there will be unmanaged exposure and invariably negative impact.

The rest of my testimony is organized as follows:

- *A brief assessment of the emerging economic and national security risks from next generation connectivity and devices (particularly the IoT and 5G networks) for the U.S. with specific reference to the risks posed by other economies such as China, Russia and other sensitive countries. What*

additional risks, if any, does use of IT, standards, and/or equipment developed in sensitive countries pose to U.S. security? Are existing authorities and regulations adequate to address these challenges?

- *How reliant are the U.S. government and U.S. IT firms on sensitive country firms and the IT products and services of those countries?*

- *What are the potential vulnerabilities from U.S. usage of sensitive country, China for example, IT, standards, and/or equipment?*

- *How, if at all, has the government of sensitive countries leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyber-attacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?*

- *Assess U.S. government's success in managing the risks associated with a company, and those products and services, from sensitive countries, to its IT procurement supply chains. How is the U.S. government seeking to address/mitigate its supply chain risks? How successful have those efforts been? What are the remaining challenges? Is existing legislation and regulations adequate to address these challenges?*

- *What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks from technology sourced from outside of the US?*

1. A brief assessment of the emerging economic and national security risks from next generation connectivity and devices (particularly the IoT and 5G networks) for the U.S. with specific reference to the risks posed by other economies such as China, Russia and other sensitive countries. What additional risks, if any, does use of IT, standards, and/or equipment developed in sensitive countries pose to U.S. security? Are existing authorities and regulations adequate to address these challenges?

Software supply chain attacks will become easier – and more prevalent - as developing technologies such as fifth generation (5G) mobile network technology and the IoT exponentially increase the avenues for attack.[1] Gartner predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IOT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have a significant impact on the ICT SCRM challenge. Relevant to the Report, increasing IoT installations will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet to date, the time required to detect breaches is not decreasing. The

[1] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.
[2] Peter Middleton, Tracy Tsai, Masatsune Yamaji, Anurag Gupta, Denise Rueb, "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017. https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.
[3] Benoit J. Lheureux, et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017. https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

responsibility of both the public and private sector in improving their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

The information technology (IT) supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the U.S., including China, North Korea, and Russia. These products could be modified to 1) perform below expectations or fail, 2) facilitate state or corporate espionage, or 3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

In the past, this concern was exemplified by counterfeit components entering the supply chain of U.S. defense systems, such as counterfeit integrated circuits from China discovered in the U.S. Navy's P-8A Poseidon airplane, in a U.S. Air Force cargo plane, and in assemblies intended for Special Operations helicopters.[4] In 2011, the Senate Armed Services Committee investigated 1,800 cases of counterfeit components which created vulnerabilities throughout the Department of Defense's supply chain, and reported that 70 percent of all counterfeits come from China, and a majority of the remaining counterfeits could be traced back through the supply chain to China. In these cases, recycled, obsolete, or modified components passed off as genuine circuits had potential to perform below expectations or fail, threatening U.S. national security and the safety of U.S. service members.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within it. In 2016, researchers identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their computer monitors.[5] In 2017, researchers uncovered vulnerabilities in printers manufactured by Hewlett-Packard, Dell, and Lexmark that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[6] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly installed the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[7] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[8]

---

[4] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," Press Release, May 21, 2012. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts.

[5] Lorenzo Franceschi-Bicchierai, "Hackers Could Break into Your Monitor To Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016. https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.

[6] Tom Spring, "Flaws Found in Popular Printer Models," *Threat Post*, January 31, 2017. https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

[7] Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017. https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

[8] India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017. http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25,

As information technology advances, and connectivity increases, these risks will multiply. Concepts such as the IoT, are but one avenue by which risk to federal IT systems will increase. The National Institute of Standards and Technology stated in Draft NISTIR 8200, released in February 2018, that "the adoption of IoT brings cybersecurity risks that pose a significant threat to the Nation."[9] Other aspects of supply chain risk depend on technologies that are not yet fully developed or deployed, such as 5G mobile network technology, which is expected to start deploying in 2020. The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round trip delay (latency[10]) to under one millisecond.[11] 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of IoT.[12,13] Faster connectivity supplied by 5G networks will enhance productivity, efficiency, and facilitate greater interconnectedness through the IoT. But these benefits come with increased cybersecurity risks.

What additional risks, if any, does use of IT, standards, and/or equipment developed in China pose to U.S. security?

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[14] Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[15] His four-year term began January 1, 2015 and concludes at the end of 2018.

Although the finalization of 5G standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, and China could emerge as an industry leader

---

2017. https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017. https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

[9] National Institute of Standards and Technology, *Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (Gaithersburg, MD: Computer Security Division, February 2018). https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf.

[10] Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

[11] Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," *TechRepublic.* https://www.techrepublic.com/article/does-the-world-really-need-5g/.

[12] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

[13] Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," *Data Center Dynamics*, October 7, 2016. http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

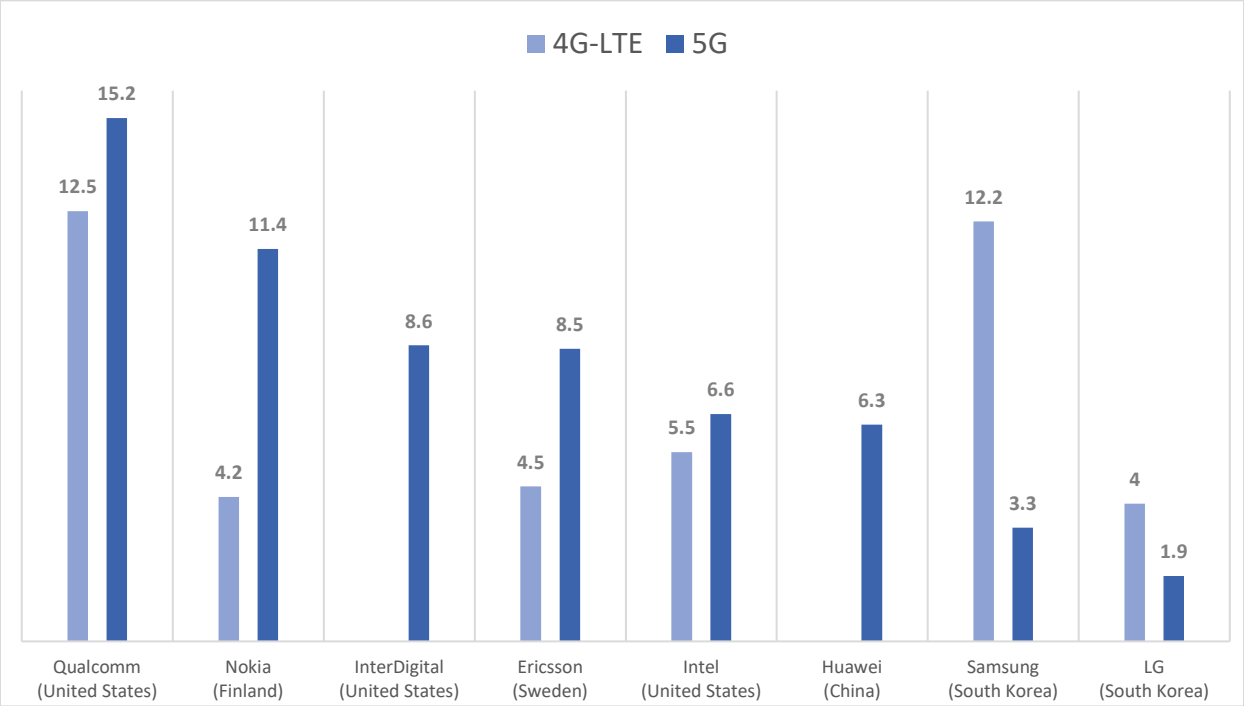
[14] 4G-LTE, or long-term evolution is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

[15] "Biography—Houlin Zhao," International Telecommunication Union, 2017. http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-general of ITU," *China Daily USA*, October 23, 2014. http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

in this technology.[16] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[17] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[18]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[19] **Exhibit 7** of the report shows the share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for 4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 7: Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



[16] Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017. https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.
[17] Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017. https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.
[18] Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.
[19] LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," March 15, 2017. http://www.lex-innova.com/resources-Reports/?id=67.

Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[20] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the U.S.

Are existing authorities and regulations adequate to address these challenges?

In short, the answer is 'no'. An example is the recently implemented Modernizing Government Technology Act (MGT Act), introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016. The Act creates a $500 million central modernization fund against which agencies can borrow to update aging IT systems. The Act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The Bill was amended to the Senate version of the FY18 National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.

The MGT Act seems to presume that legacy equipment and systems are the primary source of risk, and that this risk can be mitigated through modernization. But modernization will increase risk if newly adopted technologies, which have stronger supply chain connections to China, Russia, North Korean, Iran, Israel and other sensitive countries, are not assessed appropriately before being integrated into federal IT networks. The Bill establishes responsibilities and provides financial rewards to agencies for modernizing their IT infrastructure, naming OMB and GSA as permanent members of a supervisory board. However, it does not require any measure of supply chain security as part of modernization efforts. In the 'Implementation of the Modernizing Government Technology Act' signed by Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for SCRM as part of an Agency's modernization effort.

An understanding of emerging technologies, their pedigree, and their interconnectivity is crucial to proactively identify and mitigate future supply chain risk to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. Until U.S. leadership takes this vulnerability seriously, it will remain an 'easy button' for our adversaries.

---

[20] Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV.* http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

2. How reliant are the U.S. government and U.S. IT firms on sensitive country firms and sensitive country-made IT products and services?

Over 95 percent of all electronics components and IT systems supporting U.S. federal IT networks are commercial off-the-shelf (COTS) products, and China's role in this global supply network is significant. The supply chain for civilian IT is a global enterprise dominated by suppliers in East Asia.[21] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) noted that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[22]

Many of the top enterprise IT providers to the U.S. government are also among the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as Hewlett-Packard, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[23] Their supply chain is potentially influenced by China due to the fact that many of the companies and/or their sub-tier suppliers have manufacturing locations there.

China is not the only country the U.S. is concerned about, but their economic decision to invest in being the world's technology manufacturer should prioritize them.

3. What are the potential vulnerabilities from U.S. usage of sensitive country, China for example, IT, standards, and/or equipment?

The Chinese government considers the ICT a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. Since 2013, China has accelerated its efforts at indigenous production and independence in ways that have created a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access.

New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the Chinese government to conduct security audits on its products open federal ICT providers—and the federal ICT networks they supply—to Chinese cyberespionage efforts. China also continues to directly target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

---

[21] Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017. http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

[22] U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations," *GAO-17-688R State Department Telecommunications*, July 27, 2017. https://www.gao.gov/assets/690/686197.pdf.

[23] "Top 25 Enterprise IT Providers to Government," *FedScoop*, August 30, 2017. https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

Specific risks include intellectual property theft, theft of Personally Identifiable Information of U.S. citizens that can be used for financial gains, and the insertion of counterfeit products and services meant to create disruption and do harm.

The use of Chinese standards further complicates any security strategy the U.S. may have in place as it provides a documented path of access for our adversaries.

How will the deployment of 5G and greater usage of IoT affect these vulnerabilities?

These new emerging technologies are just two (2) more examples that need to be proactively evaluated through a security lens as part of a national supply chain risk mitigation strategy. These, and other emerging technologies will expand the attack surface and increase the potential vectors for opportunists.

4. **How, if at all, has the government of sensitive countries leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyber-attacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?**

There are multiple documented examples of the sensitive countries' governments leveraging IT for intelligence collection and economic and state espionage efforts. One of the most infamous is probably the breach of Office of Personnel Management's database in 2015, a mammoth break-in that exposed the records of more than 22 million current and former federal employees.

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the U.S. by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they further open themselves and federal ICT networks to Chinese cyberespionage efforts.

Bottom line, we need our full defenses up at all times to thwart enemy attacks.

5. **Assess the U.S. government's success in managing the risks associated with sensitive country-firms and the products and services supplied, to its IT procurement supply chains. How is the U.S. government seeking to address/mitigate its supply chain risks?**

A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, supply chain risks to federal ICT systems has been divided in multiple ways— among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems.

How successful have those efforts been? What are the remaining challenges?

In some instances, very impactful. Interos supported one federal agency where over 75% of the supply chain risk assessments conducted in the past three (3) years have identified concerns that altered acquisition decisions or influenced market analysis. That said, this mature program is in the minority when compared to those of other agencies where such programs exist. Not to mention, there are agencies that have not been resourced to implement a SCRM program at all. And, more importantly, as the Chief Information Officer (CIO) of that agency changed from a permanent to a political position, and this administration has not taken a strong stand on SCRM, the CIO cancelled the VERY SUCCESSFUL six-year running program. We were four (4) days from contract renewal and no reason for program cancellation was provided.

In the current supply chain risk ecosystem, responsibility for risk management is held at different levels within agencies. This often results in offices and lines of effort in several agencies that function largely as under-resourced stovepipes lacking in executive sponsorship or oversight, and catering to the needs and procurement policies of individual clients. The DoD and the intelligence community maintain largely separate policies, many of which are not transparent to or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons.

6. **Is existing legislation and regulations adequate to address these challenges?**

In short, no. There is little to no priority placed on SCRM, minimal leadership involvement and limited accountability. I do not know what it will take to get this level of attention or how many other incidents need to occur before Congress or the Executive Branch gets more involved, but I see this as a major flaw in U.S. national security. At the same time, I would like to commend the agencies that have taken their own initiative to set up programs for internal security reasons – they are making a difference, but unfortunately these models are not scalable or shareable in their current form.

7. **What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks from technology sourced from outside of the U.S.?**

As previously mentioned, the Federal ICT supply chain risks can be best managed by focusing on four (4) areas: 1) embracing an adaptive SCRM process, 2) promoting supply chain transparency, 3) centralizing federal ICT SCRM efforts, and 4) crafting forward-looking policies.

This concludes my testimony. I thank the Committee and I would be pleased to answer your questions.