Executive Summary

Statement of Jennifer Bisceglie

President

Interos Solutions, Inc

Before the

Subcommittee on Communications and Technology

Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Interos Solutions, Inc, a woman-owned small business, is built on 20 years of global supply chain and IT implementation experience. Interos predicted this growing wave of concern over cyber security and were at the forefront of leading the cyber-supply chain discussion within government and industry.

Summary of the major points of my testimony:

- Awareness and Education needs to be universal and started at the top of an organization in effort to be adopted by those actually executing the mission.
- Fund the program, assign someone within each agency to 'own' the issue, and measure the success.
- The lowest-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure.
- We Need Contractual Language That Works. The private sector is looking for the Federal Government to come out with contractual language that they can work with. Doing as much as possible via internal policy changes and contractual language, as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization, is a much less expensive way to approach the problem than regulation and legislation.

Statement of Jennifer Bisceglie

President

Interos Solutions, Inc

Before the

Subcommittee on Communications and Technology

Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Good morning Mr. Chairman and Members of the Subcommittee. My name is Jennifer Bisceglie, President of Interos, Inc. Thank you for inviting us to testify on behalf of our industry peers focused on supply chain risk management or SCRM.

My company, Interos, is built on my 20 years of global supply chain and IT implementation experience. We have had the opportunity to see many waves of compliance and security implemented during our careers – from the initial application of bar codes to boxes, to more sophisticated RFID, and the heightened requirement for advanced shipment notification. These compliance requirements were put in place to help with quality assurance, ensuring the right labor was in place to unload shipments at the customer's delivery site, and provide end-to-end visibility within the supply chain.

The concern for today's discussion, the cyber threat in the supply chain, began bubbling up about six years ago, building to the fever pitch we see today. Interos predicted this growing wave of concern and were at the forefront of leading the discussion within government and industry. The discussions turned from simple compliance to resiliency – ensuring the business operations would continue even if the supply chain was interrupted. Now the issue has morphed the supply chain risk management concept into a combination of resiliency and product integrity caused by an actual man-made attack. In response to this, Interos is again on the forefront of our peers, having stood up a SCRM Global Treat

Information Center that offers capabilities to help both public and private sector organizations implement SCRM frameworks, conduct supplier audits, and conduct open source research to identify potential threats with current or future suppliers.

The lexicon of supply chain risk management is brought up often – a common definition does not exist. Neither does a standard definition of cyber security exist. To some government entities, cyber security is technical and only refers to systems being hacked. To some private entities, cyber security is something they don't need to worry about as they're not big enough for anyone to want anything from. To me, the definition of cyber security extends to the supply chain vs. just IT security. Cyber security means where things are coming from, where they are going to, and who has access to them along the way. That is also the definition of supply chain risk management. Now, we've consolidated resiliency of the supply chain, i.e. what to do if a tsunami hits, into the same bucket as product integrity within the supply chain, i.e. getting the product that you ordered, protected from malware, counterfeits, and back doors into our National Security Systems. In industry, this is another hazard we're carefully watching and are finding the right avenues to protect ourselves.

Another point we would like to bring up is the cost of implementing supply chain risk management mitigations and countermeasures. Supply chain risk management needs to be viewed as an investment instead of expenditure. Interos has had the opportunity to work with the Department of Energy (DOE) on their enterprise SCRM program. They have stood up a Focal Point, which is the hub of their SCRM expertise. With only three Interos team members supporting the DOE Focal Point Program Manager; they have an infrastructure that can share resources and information throughout the entire enterprise.

Interos has taken the stance that the best supply chain risk management practices are implemented in the current workflow – in everyone's day to day job. With this approach, the increased security is cost effective and is viewed as an investment not an expense. This approach is more of a cultural shift that

supports current business processes and reduces the need to develop new stovepipe processes that increase cost and create additional work for the risk owner. If SCRM costs too much, or if it is seen as 'another thing people have to do,' it will not be adopted by the stakeholders or user community.

From our perspective, Congress can take four steps to protect our Nation's critical infrastructure.

- **Awareness and Education needs to be universal and started at the top of an organization in effort to be adopted by those actually executing the mission.** In working with Federal agencies across the spectrum from the Intelligence Community, DoD, and .Gov, the level of awareness of the challenge varies across the Federal Agencies. Similarly, so does their level of attention to managing their supply chain risk. Awareness and education is critical to communicate that supply chain risk impacts everyone within the Federal infrastructure. It may be a different level for DOE than for Department of Education, but they are both impacted. At this time, there is not a common level of understanding across the Federal agencies. We see the same varied level of attention and understanding in the private sector. Resiliency has departments stood up and focused on it, normally within an organization's supply chain arm. The amount of attention paid to cyber-supply chain issues depends on where you exist in the supply chain, i.e. manufacturer (being the highest as they care the most about brand and product integrity) down to distributor and customer, where the main focus is financial, i.e. revenue and cost.

- **Fund the program, assign someone within each agency to 'own' the issue, and measure the success –** We have seen RFPs come out various agencies with a myriad of SCRM requirements. We have also seen focal points, as directed by the Bush and the Obama Administration, being implemented in different areas within the agencies. We all agree that the ultimate responsibility – or acceptance of risk – remains with the risk owner, which in the case of the federal government is

the program manager. Having said this, without the top-down support within the agencies, without an 'owner' of the concern (being supply chain risk management) and without funding, these programs are being bootstrapped and implemented in various fashions. I understand the budget issues we have as a Federal Government. But with the implications that a breach will significantly impact National Security, it seems to us that funding for cyber-supply chain risk management is an investment the Federal Government needs to make because it is an investment in future security challenges. The private sector is working through many of the same issues, as the protection of the cyber-supply chain crosses the technical into the operational workforce.

- **The lowest-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure** – While we understand the severely constrained federal budget and the temptation to fund program objective with the lowest bid, when it comes to cyber security, this is not a good strategy. As I mentioned earlier, the federal government needs to see this as an investment in the future of our government's critical infrastructure. Failure to protect our critical infrastructure and educate risk owners on the threats that are brought into an organization by buying from unvalidated sources, will result in continue and increasingly harmful attacks. We see them daily – some are mere nuisances, some are stealing personally identifiable information (PII), corporate espionage, or worse. Manufacturers have a need for good distribution networks and are spending money, annually, to ensure those network distributors are handling their products appropriately. Using certified vendors and distributors provides at least a minimum level of assurance that the products deployed across the critical Federal Infrastructure are authentic. Procurement for those products or components that support our critical infrastructure should always be evaluated with the strictest adherence to industry standards. Lowest price, technical

acceptable competition adds additional risk to our Nation's critical infrastructure and should not be an acceptable model for these types of procurements.

We do understand there are acquisitions that do not relate to our Nation's critical infrastructure. In our mind, and from a common sense standpoint, each acquisition needs to be looked at independently, as well as with other systems it may interface with, to assess the risk tolerance of the organization– and the level of supply chain risk management rigor that must be applied to each acquisition. It is too expensive to try to protect everything – and we're not proposing this. But there are easy ways to prioritize what process or functions are critical to an organization, and what systems are supporting those functions. From there, there are processes to drive the conversation down to the components of the systems – which provides you a list of suppliers you need to work with.

- **Contractual Language That Works** – The private sector is looking for the Federal Government to come out with contractual language that they can work with. We understand that as a part of Executive Order 13636, GSA, NIST, and DoD are working with potential recommendations to update the FAR language. In addition, there are multiple industry associations working on standards for SCRM that can be spread across the cyber-supply chain risk management focused community. This will initially increase costs to the private sector and the government purchasers, but if done correctly, should spread the costs over the supply chain as purchasers understand what level of rigor each acquisition requires and the private sector learns how to build that into its cost structure. The increase in cost to the private sector may include additional layers of security, which are Government customer specific, and are not part of their current corporate Cybersecurity policies.

As long as the business case can be made, the two parties will be able to walk through the economics of it. As more informed discussions take place, we will come to the realization that many of us, both in the public and private sector, have the same vulnerabilities that our supply chains need to be secured against. Doing as much as possible via internal policy changes and contractual language, as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization, is a much less expensive way to approach the problem than regulation and legislation.

We see the adoption of many of these increased security practices being very similar to how bar-coding was adopted back in the 1990's. The big box retailers would charge the manufacturer money if the boxes were not marked correctly, or if the advanced shipment notice had not been received in time for the retailer to plan their dock labor. There was an initial outcry and then the private sector learned to spread the cost and absorb it. We are not asking for anything that will go away any time soon – the standards that are being created right now for SCRM are here to solve a problem that will only become more prevalent.

The topic of information sharing has been brought up repeatedly, and is a large part of the Executive Order 13636. This needs to be encouraged and enabled – not legislated and mandated. What we are seeing in the private sector is that organizations are open to sharing given a level of trust across all vendors and distributors within the supply chain. If the Federal Government took some of the steps above, and provided the private sector with a dependable and repeatable SCRM position, trust will grow between the public and private sectors.

Can we all improve our security practices? Yes we can. The private sector can do a more rigorous job and still remain profitable. That said, the Federal Government needs to own its own problem, starting with adoption of a common level of understanding that this threat is here, it is an important investment, and collectively a solution needs to be crafted. The argument that over 75% of Federal acquisitions are commercial-off-the-shelf (COTS) products, thereby throwing the responsibility over the fence to the private sector does not work. Federal agencies should be able to articulate their level of risk tolerance, and have processes and funding in place, to acquire products based on that information.

For our final point, we would like to stress the far-reaching nature of this threat. Although much of today's conversations, as well as that of the Federal Government and their contractor base's focus, are on information communications technology (ICT) that supports our nation's critical infrastructure, the cyber-supply chain risk issue is all inclusive. It is Interos' position that anyone that purchases technology should look at where they are sourcing from, and how they are using the technology. We used the comparison of DOE vs. Dept of Education earlier – we are sure that although no classified systems may be used, the Dept of Education has information that needs to be protected. By instituting some of the ideas laid out in the four bullets above, both the public and private sector can make some low cost, high value changes in their business processes which will create more security in their supply chains.

We, at Interos, feel the threat is real for every agency and one we should all take very seriously.

Conclusion

Due to Interos' unique position in the marketplace, we have had the opportunity to see the past and current situation of SCRM from multiple perspectives.

We call to your attention a quote from the *National Strategy for Global Supply Chain Security* (January 2012), which states *'We reject the false choice between security and efficiency and firmly believe that we can promote economic growth while protecting our core value as a nation as a people.'* The solution needs to be viewed as an investment in national security, not just another expense. The key is for industry and the government to separately work on their internal risk tolerance levels through good business practices, including awareness, training, and contractual agreements. This will enable each to meet collaboratively, and have informed discussions about where vulnerabilities lie and what it will take to protect our country.

The enemy is smart and persistent but not unstoppable. If we invest the time, use common sense, and work together to improve the government's cyber-supply chain security business practices, our national security will be greatly enhanced.

Thank you for this opportunity to present our views. I look forward to answering any questions.