Supply Chain Risk Management Awareness, May 2013

Hello, my name is Gil Vega. I am the Department of Energy Associate Chief Information Officer for Cybersecurity and the Chief Information Security Officer. I manage the agency's Supply Chain Risk Management Program and would like to take a moment to discuss the critical role that this program plays in our daily lives.

The DOE's Supply Chain Risk Management Program is an enterprise approach to managing risk and vulnerabilities associated with the acquisition, sustainment, and disposal of critical Information and Communication Technology, or ICT, components. These components store, retrieve, and transmit digital information that connects the DOE's enterprise and ensures the success of the mission. Despite ICT's benefits, increased connectivity brings increased risk of theft, fraud, and abuse. No country, industry, or agency is immune from the inherent risks associated with global supply chains and cybersecurity. Our ability to identify and mitigate these threats is essential to achieving America's energy, environmental and nuclear challenges.

The Department of Energy has designed a 2013 Supply Chain Awareness Campaign to engage, educate and raise awareness about the risk associated with an unsecure ICT supply chain. The campaign focuses on mitigating risk by empowering stakeholders to recognize how counterfeits, malware, and malicious software or hardware expose the enterprise to cybersecurity attacks and insider threats. It also reminds us that online safety and security is a shared responsibility. If all DOE employees do their part to implement stronger security practices, raise community awareness, and educate employees; together we can foster a literate, resilient, and secure online society.

Throughout the Supply Chain Awareness Campaign and beyond, DOE employees should implement common security practices that minimize our exposure to risk. By following these simple practices, we will significantly enhance our online security; making the Internet a safer place for ourselves, our organization, and our Nation. Some ICT SCRM best practices are:

- Purchase ICT products from certified reputable vendors, not eBay or Craig's List;
- Leverage threat assessment capabilities for vendor investigations;
- Know your ICT products and have an expert analyze devices not operating correctly;
- Set strong passwords and don't share them with anyone;
- Keep a clean machine and install all regular updates; and
- Limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.

I encourage you to participate in the 2013 Supply Chain Awareness Campaign forums and training courses. They are an excellent opportunity to enhance your awareness of growing supply chain threats and simple protection strategies. Also, please remember that securing your personal cyberspace requires continuous vigilance, so let us not limit our efforts to this campaign.

My office is always available to provide supply chain awareness information. Please contact enterprisescrm@hq.doe.gov for more information.

Thank you for your time. Sincerely Gil Vega.