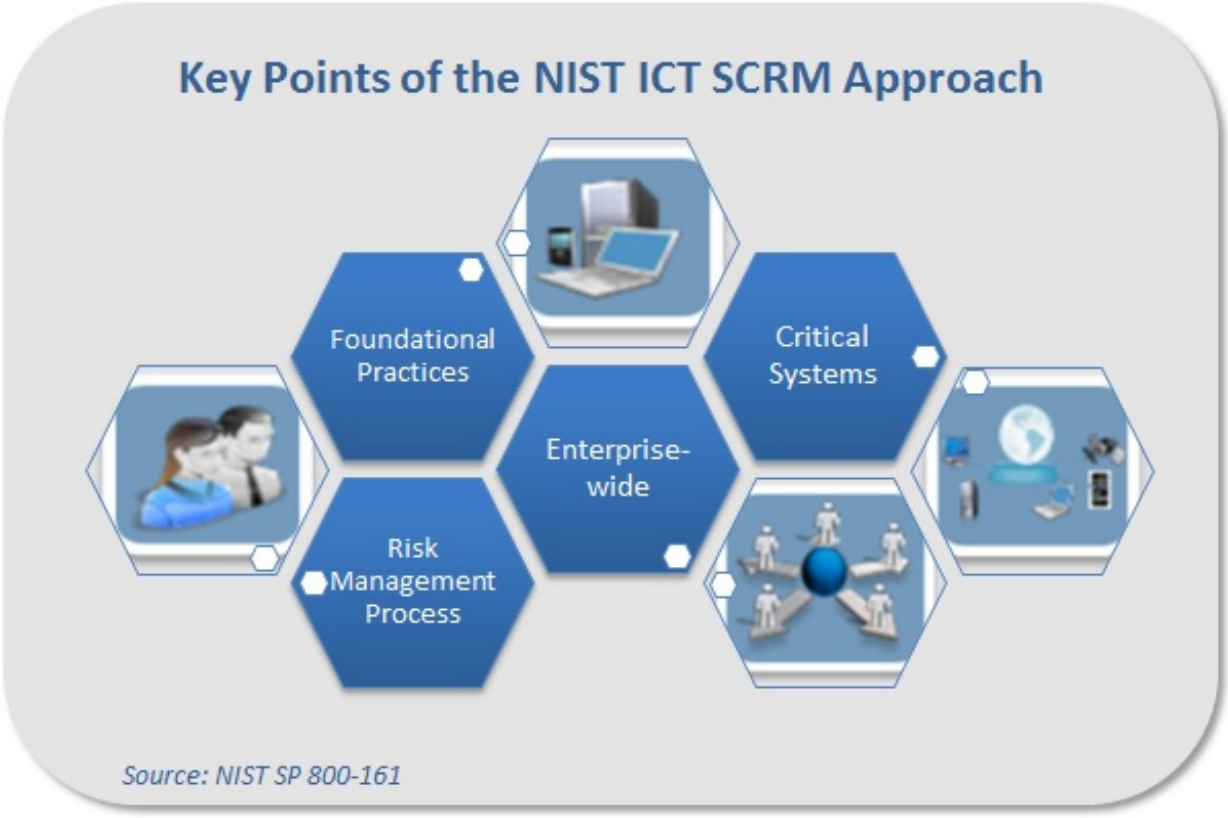
New Guidance Targets Federal Supply Chain Risk Management Practices

Posted At : May 12, 2015 11:20 AM | Posted By : Kyra Fussell
Related Categories: Digital Government, Information Security, Cybersecurity, Department of Commerce

Federal agencies are increasingly relying on commercially provided systems to advance capabilities and deliver cost savings. However, globalization and increasing complexity of technology increases the risks of threats to technology supply chains such as theft, tampering, poor development practices, as well as counterfeit and malicious hardware or software components. In April 2015, the National Institute for Standards and Technology (NIST) published new guidance on securing federal information technology supply chains.

The NIST information and communications technology supply chain risk management (ICT SCRM) program began in 2008 by kicking off development of risk management practices for non-national security information systems aligned with Comprehensive National Cybersecurity Initiative aiming to address global supply chain concerns. In 2012, NIST published an interagency report on methods and practices for supply chain risk management for federal information systems. The interagency report and related activities contributed to the drafting process for this new guidance.

The special publication, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," notes that federal information systems and networks are increasingly complex. These systems and networks are composed of information and communications technology (ICT) products and services acquired through suppliers, system integrators, and external service providers. In order to manage ICT supply chain risks, the integrity, security, and resilience of the supply chain must be ensured as well as the quality of products and services. The new guidance aims to help government organizations understand the risks around ICT and identify approaches to mitigate threats and vulnerabilities. Specifically, the document outlines steps for identifying, assessing, and mitigating risks throughout the ICT supply chain. These guidelines offer an approach to supply chain risk management that addresses key areas around foundational practices, organization-wide implementation, integration with the overall risk management process, and identification of priority components and/or systems.



The processes and controls in the guidance can be augmented with organization-specific requirements (e.g. from policies, guidelines, and other documents) to enable organizations to develop technology supply chain risk management mitigation strategies that are tailored to their needs. The guidance does not provide contract language or a complete list of supply chain risk management methods and techniques to mitigate specific threats.While these guidelines have been specified for federal agencies, the recommendations could be applied to all sectors. Contractors can expect to start seeing language related to supply chain risk management in requests for proposals as agencies adopt the approach.

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWinIQ**. Follow me on twitter **@FIAGovWin**.*