Targeting Security Improvements through Supply Chain Risk Management

Posted At : December 10, 2013 4:42 PM | Posted By : Kyra Fussell

Related Categories: Critical Infrastructure Protection, Technology Trends, Information Security, National Aeronautics and Space Administration, Cybersecurity, Department of Commerce, Contract Opportunities, Strategic Sourcing

National Aeronautics and Space Administration (NASA) officials started market research over a year and a half ago for the follow-on to a government-wide acquisition contract (GWAC) that supplies federal agencies with information technology products and product-based services. One new aspect of this follow-on is the growing emphasis on IT supply chain risk management.

Since the release of the Request for Proposal (RFP) for the next iteration of the Solutions for Enterprise-Wide Procurement (SEWP) contract in August, NASA's program office for SEWP has released 12 amendments and extended the submission due date into December. The security associated with IT supply chains has received increasing attention. On the vendor side, more detail around supply-chains will be disclosed in SEWP V. Information about industry supply-chains will help to clarify the various risks and costs as products move from manufacturers to government customers. Supply-chain risk management considers what technologies agencies are using and evaluates layers of risk from how a product moves from a manufacturer to a customer.

Aligned **with the Executive Order released in February**, efforts to improve critical infrastructure security have highlighted mitigating security risks introduced through the supply chain. Back in April 2013, the Cyber Security Research Alliance (CSRA) conducted **a workshop** in collaboration with the National Institute of Standards and Technology (NIST) targeting security for cyber-physical systems (CPS). Cyber-physical systems span applications in critical infrastructure including power and water, industrial systems, emergency management, security systems, and medical devices among others. Among other topics, the workshop participants explored the impact of supply chain on securing CPS. The global market for information and communication technology product manufacturing introduces numerous opportunities for products to be subject to tampering or sabotage. Both insufficient diligence around buyer practices and lack of visibility into the supply chain present challenges for reducing and managing risks.

Recommendations for moving forward included developing supplier reliability and monitoring methodologies. In particular, findings recommend advancing research and development for tools to identify vulnerabilities and corrective measures, reviewing existing practices to improve information sharing and collaboration between suppliers and buyers, building security technology refresh into life-cycle, and leveraging analytics to target potential future failures and counterfeits.

Moving forward, the practices of government contractors are likely to be subject to increasing scrutiny as agencies face growing reporting requirements, demand cost efficiencies, and strive to comply with security mandates. Past iterations of the SEWP have been leveraged by organizations across the government. With the increased performance period and ceiling value of SEWP V, it's clear that trend is expected to continue. In order for vendors to maximize the opportunity, they need to meet the modernized requirements. Deadline for submission to the **SEWP V RFP** is set for December 16, 2013.

Further perspective on current and evolving government cyber security concerns is available in our latest report: **Federal Information Security Market, FY 2013-2018**.

----

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