NIST publishes methods to manage risk in the federal ICT supply chain

November 28 2012

The National Institute of Standards and Technology (NIST) has published the final version of *Notional Supply Chain Risk Management Practices for Federal Information Systems*. This guide offers an array of supply chain assurance methods to help federal agencies manage the risks associated with purchasing and implementing information and communications technologies (ICT) products and services.

Security risks introduced via the supply chain—both intentional and unintentional—are substantial and on the rise. The global ICT supply chain's growing sophistication and increasing speed and scale leave government agencies vulnerable to be exploited through a variety of means, including counterfeit materials, malicious software or untrustworthy products.

The guide describes ICT supply chain risk management as a multidisciplinary practice with a number of interconnected enterprise processes that, when performed correctly, will help departments and agencies manage the risk of using ICT products and services. The publication calls for procurement organizations to establish a coordinated team approach to assess the ICT supply chain risk and to manage this risk by using technical and programmatic mitigation techniques.

The new guide is based on information technology security practices and procedures published by NIST, the National Defense University, the National Defense Industrial Association and others. These practices were

expanded to include supply chain implications. This version of *Notional Supply Chain Risk Management Practices for Federal Information Systems* has been through two public review periods, allowing for input from a broad array of stakeholders. The final publication differs from previous drafts in that it provides a more specific definition of the supply chain threat and further details on the roles of integrator and supplier and how they apply to the federal government's acquisition of commercial off-the-shelf products.

NIST is developing a draft Special Publication based on the proceedings of the Oct. 15-16, 2012, Supply Chain Risk Management Workshop and ongoing discussions with industry, academic and government stakeholders. PowerPoint presentations from that workshop are available at www.nist.gov/itl/csd/scrm_2012workshop.cfm . NIST will continue to engage public- and private-sector stakeholders throughout the publication development process.

Notional Supply Chain Risk Management Practices for Federal Information Systems (NIST IR 7622) is available at nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf .

Provided by National Institute of Standards and Technology