Proposed risk management guidelines aim to bolster security of federal ICTsupply chains

June 4 2014

Products from across the world add risk to information communications supply chains. Credit: freshidea-Fotolia_com

The National Institute of Standards and Technology (NIST) has published a second public draft of Supply Chain Risk Management Practices for Federal Information Management Systems and Organizations for public comment. The new version incorporates changes made in response to comments on the original draft issued Aug. 16, 2013.

Between the growing sophistication and complexity of modern information and communication technology (ICT) and the lengthy and geographically diverse ICT supply chains, important federal information systems are at risk of being compromised by counterfeits, tampering, theft, malicious software and poor manufacturing practices. A counterfeit chip could cause a computer system to break down; malware could lead to loss of critical information.

The NIST guide to securing ICT supply chains details a set of processes for evaluating and managing that risk. "It builds on NIST's Managing Information Security Risk publication," explains lead author Jon Boyens.

NIST recommends that evaluating ICT supply chains should be part of an organization's overall risk management activities and should involve identifying and assessing applicable risks, determining appropriate mitigating actions, and developing a plan to document mitigating actions and monitoring performance. The plan should be adapted to fit each organization's mission, threats and operating environment, as well as its existing ICT supply chains.

The draft publication also calls for building ICT supply chain risk management activities on existing supply chain and cybersecurity practices, employing an organization-wide approach, and focusing on the systems and components that are most vulnerable and can cause the largest impact if compromised.

The guidance is designed for use with high-impact systems as categorized in NIST's Standards for Security Categorization of Federal Information and Information Systems and can be used on moderate systems, if deemed appropriate, Boyens says.

This second public draft is based on an extensive review and comments contributed by the ICT community. NIST is asking for feedback on some of the key changes that appear in this draft, including:

- Increased emphasis on balancing the risks and costs of ICT supply chain risk management processes and controls throughout the publication,
- An ICT supply chain risk management controls summary table that provides a baseline and maps to NIST Special Publication 800-53 Revision 4 High baseline controls in Appendix D, and
- An annotated ICT Supply Chain Risk Management Plan Template in Appendix H.

More information: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Second Public Draft (NIST SP 800-161) can be downloaded from csrc.nist.gov/scrm/publications.html. The public comment period ends July 18, 2-14. Comments may be submitted by email to scrm-nist@nist.gov using the template on the web page.

Provided by National Institute of Standards and Technology

Citation: Proposed risk management guidelines aim to bolster security of federal ICTsupply chains (2014, June 4) retrieved 9 April 2024 from https://phys.org/news/2014-06-guidelines-aim-bolster-federal-ictsupply.html