DRAFT Notional Supply Chain Risk Management Practices for Federal Information Systems NIST IR 7622

ISPAB

May 31, 2012

Jon Boyens
Computer Security Division

National Institute of Standards and Technology

NIST Interagency Reports (NIST IRs)

- Describe research of a technical nature of interest to a specialized audience.
- Include interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment).
- May also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

HISTORY

- Grew out of Comprehensive National Cybersecurity Initiative (CNCI) 11 – 2008
- Initial public draft – June 2010
- Second public draft – March 23 - May 25, 2012

Purpose

- Guidance and recommended practices to manage supply chain risk to a level commensurate with the criticality of information systems or networks for the acquiring federal agency only
- High-Impact Level Systems (FIPS 199) medium-impact dependent upon risk management approach
- System Development Life Cycle (SDLC) (COTS & GOTS.)
  - Design, development, acquisition, integration, operation, and disposal
- Broad Audience
  - System owners, acquisition staff, system security personnel, system engineers, etc.

Changes to Second Draft

- Problem
  - Lack of visibility, understanding and control to allow for risk management.
- Resources – What are we asking actors to do?
  - Many activities already practiced that address various disciplines, including logistics, security, reliability, safety, quality control, etc.
- Description vs. Prescription

Thank you

Contact: Jon Boyens - jon.boyens@nist.gov

http://scrm.nist.gov