2 NIST publications recommend organization-wide IT security risk management

January 6 2011

Two new draft publications from the National Institute of Standards and Technology provide the groundwork for a three-tiered risk-management approach that encompasses computer security risk planning from the highest levels of management to the level of individual systems. The draft documents have been released for public comment.

Both publications are a part of NIST's risk management guidelines, which have been developed in support of the Federal Information Security Management Act (FISMA), and adopted government wide to improve the security of government systems and information. Both call for upper-level management to understand that information security is a key component to mission-critical functions and that top managers need to manage information security risk in coordination with chief information officers, chief information security officers and system owners to meet the organization's goals.

Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View (Special Publication 800-39, available in pdf format at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-39), is the capstone document that applies this new perspective on how federal agencies and their contractors should manage information security risk.

"Most organizations currently manage risk using a tactical, system-by-system approach," said Ron Ross, NIST Fellow and FISMA Implementation Project Leader. "This new framework suggests a three-

tiered risk management approach that moves from organization to missions to information systems. The goal is for senior leaders and executives to manage risks strategically and drive investment and operational decisions based on the organization's core missions and business functions."

The new approach is particularly important as organizations address advanced persistent threats, which have the potential to degrade or debilitate federal information systems that support critical applications and operations of the federal government.

This publication is the fourth in the series developed by the Joint Task Force Transformation Initiative, a joint partnership among the Department of Defense, the Intelligence Community, NIST, and the Committee on National Security Systems. This draft provides significant changes from earlier versions of the publication and includes input from all partners in the Joint Task Force.

SP 800-39, once finalized, will supersede Risk Management Guide for Information Technology Systems (SP 800-30) as the source for guidance on risk management. A revised version of SP 800-30 will provide guidance on risk assessment consistent with SP 800-39 and is expected to be published in 2011.

Comments are requested on the draft of SP800-39. Please send them to sec-cert@nist.gov by Jan. 25, 2011.

The initial public draft of a second new NIST publication, Information Security Continuous Monitoring for Federal Information Systems and Organizations (Special Publication 800-137, available in pdf format at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-137), is a guide to developing and implementing a comprehensive continuous monitoring strategy for computer security risk management using a three-

tiered approach, organization level, mission/business level and system level. A robust strategy for continuous monitoring of information security helps maintain ongoing awareness of information security and ensures that organizational security practice reflects the organization's risk tolerance. It helps ensure that accurate, up-to-date information is available to enable timely risk management decisions.

"SP 800-137 encourages a holistic approach to managing risk through information security continuous monitoring." explains IT Specialist Kelley Dempsey. The publication describes how to develop a comprehensive continuous monitoring strategy. It provides methods to implement a continuous monitoring program including determination of measures and metrics, determination of monitoring frequencies, review and analysis of security-related information, response to information security risk, and revision of the strategy.

Comments are requested on the draft of SP 800-137. Please send them to 800-137comments@nist.gov by March 15, 2011.

Provided by National Institute of Standards and Technology