NEWS & EVENTS

News -- 2011

NIST Computer Security Division Released Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
March 1, 2011

The National Institute of Standards and Technology (NIST) announces the final publication of ***Special Publication 800-39***, *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39 is the fourth in the series of risk management and information security guidelines being developed by the Joint Task Force Transformation Initiative, a joint partnership among the Department of Defense, Intelligence Community, NIST, and the Committee on National Security Systems. The partnership, under the leadership of the Secretary of Defense, the Director of National Intelligence, and the Secretary of Commerce continues to collaborate on the development of a unified information security and risk management framework for the federal government to address the challenges of protecting federal information and information systems as well as the Nation's critical information infrastructure.

NIST Special Publication 800-39, the capstone publication in the Joint Task Force publications, provides guidance to federal agencies and their contractors on how to manage information security risk associated with the operation and use of information systems. For decades, organizations have managed risk at the information system level. This information system focus provided a very narrow, stovepiped, perspective that constrained risk-based decisions by senior leaders/executives to the *tactical* level—devoid, in many cases, of any direct linkage or traceability to the important organizational missions/business functions being carried out by enterprises. The concentration on information systems security resulted in a focus on *vulnerability management* at the expense of *strategic* risk management applied across enterprises.

Special Publication 800-39 introduces a three-tiered risk management approach that recommends federal agencies focus, initially, on establishing an enterprise-wide *risk management strategy* as part of a mature governance structure involving senior leaders/executives and a robust risk executive (function). The risk management strategy addresses some of the fundamental issues that organizations face in how information security risk is assessed, responded to, and monitored over time in the context of critical missions and business functions. The strategic focus of the risk management strategy allows organizations to influence the design of key mission and business processes—making these processes risk aware. Risk-aware mission/business processes drive enterprise architecture decisions and facilitate the development and implementation of an effective, embedded information security architecture that provides a roadmap for allocating safeguards and countermeasures to information systems and the environments in which those systems operate.

The multitiered risk management approach (moving from organization to missions to systems) ensures that strategic considerations (including top-level organizational goals and objectives), drive investment and operational decisions with regard to managing risk to organizational operations (including mission, function, image, and reputation), organizational assets, individuals, other organizations (collaborating or partnering with federal agencies and contractors), and the Nation. This type of risk-based decision making is especially important with respect to how organizations address *advanced persistent threats* which have the potential through sophisticated cyber attacks, to degrade or debilitate information systems supporting the critical applications and operations of the federal government.