Revision of SP 800-53 addresses current cybersecurity threats, adds privacy controls

February 29 2012

A major revision of a Federal Information Security Management Act (FISMA) publication released today by the National Institute of Standards and Technology (NIST) adds guidance for combating new information security threats and incorporates new privacy controls to the framework that federal agencies use to protect their information and information systems.

To handle insider threats, supply chain risk, mobile and cloud computing technologies, and other cybersecurity issues and challenges, NIST has released Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4 (Initial Public Draft). The document is considered a principal catalog of security standards and guidelines used by federal government agencies that NIST is required to publish by law.

“The changes we propose in Revision 4 are directly linked to the current state of the threat space—the capabilities, intentions and targeting activities of adversaries—and analysis of attack data over time,” explained Ron Ross, FISMA Implementation Project Leader and NIST fellow.

The revision also adds a new privacy appendix to the publication that provides privacy controls and associated implementation guidance. “Privacy and security are complementary, so we decided to combine them in SP 800-53," said Ross.

Other areas addressed in the update in addition to those mentioned above include application security, firmware integrity, distributed systems and advanced persistent threat. “Many organizations are concerned about advanced persistent threats, so we added new controls that will allow organizations to use different strategies to combat those types of threats,” Ross added.

NIST also modified its guidance on security assurance Appendix E, which outlines how agencies can establish measures of confidence that the security controls put in place are providing the necessary security capability to protect critical missions and business operations. Ross explains, “Having security functionality in your information systems without the appropriate assurance is like skydiving without a backup parachute—you don’t need it until you need it. And without it, the outcome is very predictable.”

As part of the update to SP 800-53, NIST addressed potential gaps in coverage, added new security controls and control enhancements, provided additional supplemental guidance for these controls, and clarified security control requirements and specification language. Keeping the potential threats in mind, the security control baselines were updated and minimum assurance requirements revised.

This document, when finalized, will be used by the entire federal government. The project was conducted as part of the Joint Task Force Transformation Initiative, which is composed of security experts from NIST, the Department of Defense, the Intelligence Community, the Committee on National Security Systems, and the Department of Homeland Security.

The public draft of Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4 may be found at csrc.nist.gov/publications/Pub …