NIST issues major revision of core computer security guide: SP 800-53

May 1 2013

SP 800-53 Rev. 4 identification and authentication controls are met when employees use their government-issued personal identity verification cards to use their computers. Credit: Kelly Talbott, NIST

The National Institute of Standards and Technology (NIST) has published the fourth revision of the government's foundational computer security guide, Security and Privacy Controls for Federal information Systems and Organizations. Better known to the federal computer

security and contractor community as "SP (Special Publication) 800-53," this fourth revision is the most comprehensive update to the security controls catalog since the document's inception in 2005.

"This update was motivated by the expanding threats we all face," explained Project Leader and NIST Fellow Ron Ross, "These include the increasing sophistication of cyber attacks and the fact that we are being challenged more frequently and more persistently."

State-of-the-practice security controls and control enhancements have been integrated into the new revision to address the evolving technology and threat space. Examples include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems. The revision also features eight new families of privacy controls that are based on the internationally accepted Fair Information Practice Principles.

SP 800-53, Revision 4 also takes a more holistic approach to information security and risk management. The publication calls for maintaining "cybersecurity hygiene"—the routine best practices that help reduce information security risks—but also appeals for hardening those systems by applying state-of-the-practice architecture and engineering principles to minimize the impacts of cyber attacks and other threats.

"This 'Build It Right' strategy, coupled with security controls for continuous monitoring, provide organizations with near real-time information that leaders can use to make ongoing risk-based decisions to protect their critical missions and business functions," said Ross.

To provide organizations with greater flexibility and agility in building information security programs, the baseline set of security controls can

be tailored for specific needs according to the organization's missions, environments of operation, and technologies used. Specific lists of controls and implementation guidance, or overlays, focus on a variety of missions, including space operations, military tactical operations and health care applications. Overlays also support specific technologies such as cloud computing and mobile devices.

"This specialization approach to security control selection is important as the number of threat-driven controls and control enhancements increases and organizations develop specific risk management strategies," Ross said.

More information: The new revision of SP 800-53, Security and Privacy Controls for Federal information Systems and Organizations, was developed by NIST, the Department of Defense, the Intelligence Community and the Committee on National Security Systems as part of the Joint Task Force, which was formed in 2009. It can be obtained at dx.doi.org/10.6028/NIST.SP.800-53r4

Provided by National Institute of Standards and Technology