

# NIST Issues Final Guidelines on Computer Security Controls for Federal Systems

February 28 2005

---

The Commerce Department's National Institute of Standards and Technology (NIST) today released its final version of recommended security controls for federal information systems. The new guideline will be the basis for a proposal to be made later this year by NIST for a Federal Information Processing Standard (FIPS) that will become mandatory for federal agencies in December 2005.

"This document of security guidelines is going to play a key role in helping federal agencies effectively select and implement security controls and, by using a risk-based approach, do so in a cost-effective manner," said Shashi Phoha, director of NIST's Information Technology Laboratory.

This fourth and final version of Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53) includes changes based on more than 1,200 comments to earlier drafts. Expected to have a wide audience beyond the federal government, the publication recommends management, operational and technical controls needed to protect the confidentiality, integrity and availability of all federal information systems that are not national security systems. The controls cover 17 key security focus areas, including risk assessment, contingency planning, incident response, access control, and identification and authentication. The security guidelines also provide information on selecting the appropriate controls needed to achieve security for low-, moderate-, and high-impact information systems.

NIST SP 800-53 is one of a series of key standards and guidelines produced by NIST's Computer Security Division to help federal agencies improve their security and comply with the Federal Information Security Management Act (FISMA) of 2002 and Office of Management and Budget security policies. Other recently published NIST security standards and guidelines include Standards for the Security Categorization of Federal Information and Information Systems (FIPS 199) and Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37). All of NIST's security standards and guidelines are available at [csrc.nist.gov](https://csrc.nist.gov).

As a non-regulatory agency of the U.S. Department of Commerce's Technology Administration, NIST develops and promotes measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life.

Source: NIST

Citation: NIST Issues Final Guidelines on Computer Security Controls for Federal Systems (2005, February 28) retrieved 25 April 2024 from <https://phys.org/news/2005-02-nist-issues-guidelines-federal.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--