

NIST publishes final version of new cybersecurity recommendations

Published 12 August 2009

NIST's cybersecurity recommendations for government aim to create a unified framework which will result in the defense, intelligence and civil communities using a common strategy to protect critical federal information systems and associated infrastructure

The National Institute of Standards and Technology (NIST) has released the final version of "NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations." The document was released in draft form for public review in June.

"This final publication represents a solidification of the partnership between the Department of Defense, the Intelligence Community, and NIST and their efforts to bring common security solutions to the federal government and its support contractors," said Ron Ross, of NIST's computer security division. "The aim is to provide greater protection for federal information systems against cyber attacks."

Comments received from the public since June did not result in any major changes in the final publication.

Historically, information systems at civilian agencies have operated under different security controls than military and intelligence information systems. When complete, the unified framework will result in the defense, intelligence and civil communities using a common strategy to protect critical federal information systems and associated infrastructure.

A copy of the publication is [available here](#) as a PDF.

