**ATTACHMENT 4:**

**Recommended Security Controls for Federal Information Systems and Organizations**

Recommended Security Controls

for Federal Information Systems

and Organizations

**JOINT TASK FORCE**

**TRANSFORMATION INITIATIVE**

I N F O R M A T I O N S E C U R I T Y

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

***August 2009***

INCLUDES UPDATES AS OF 09-14-2009 (ERRATA PAGE XI)

**U.S. Department of Commerce**

*Gary Locke, Secretary*

**National Institute of Standards and Technology**

*Patrick D. Gallagher, Deputy Director*

Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PAGE ii

**Reports on Computer Systems Technology**

The Information Technology Laboratory (ITL) at the National Institute of Standards and

Technology (NIST) promotes the U.S. economy and public welfare by providing technical

leadership for the nation’s measurement and standards infrastructure. ITL develops tests, test

methods, reference data, proof of concept implementations, and technical analyses to advance the

development and productive use of information technology. ITL’s responsibilities include the

development of management, administrative, technical, and physical standards and guidelines for

the cost-effective security and privacy of other than national security-related information in

federal information systems. The Special Publication 800-series reports on ITL’s research,

guidelines, and outreach efforts in information system security, and its collaborative activities

with industry, government, and academic organizations.

Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PAGE iii

**Authority**

This publication has been developed by NIST to further its statutory responsibilities under the

Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is

responsible for developing information security standards and guidelines, including minimum

requirements for federal information systems, but such standards and guidelines shall not apply to

national security systems without the express approval of appropriate federal officials exercising

policy authority over such systems. This guideline is consistent with the requirements of the

Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency

Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections.

Supplemental information is provided in Circular A-130, Appendix III.

Nothing in this publication should be taken to contradict the standards and guidelines made

mandatory and binding on federal agencies by the Secretary of Commerce under statutory

authority. Nor should these guidelines be interpreted as altering or superseding the existing

authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

This publication may be used by nongovernmental organizations on a voluntary basis and is not

subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-53, Revision 3, 237 pages

**(August 2009)**

**Comments on this publication may be submitted to:**

National Institute of Standards and Technology

Attn: Computer Security Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Electronic mail: sec-cert@nist.gov

Certain commercial entities, equipment, or materials may be identified in this document in order to

describe an experimental procedure or concept adequately. Such identification is not intended to imply

recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or

equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST

in accordance with its assigned statutory responsibilities. The information in this publication, including

concepts and methodologies, may be used by federal agencies even before the completion of such

companion publications. Thus, until each publication is completed, current requirements, guidelines,

and procedures, where they exist, remain operative. For planning and transition purposes, federal

agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and

provide feedback to NIST. All NIST publications, other than the ones noted above, are available at

http://csrc.nist.gov/publications.

Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PAGE iv

**Compliance with NIST Standards and Guidelines**

In accordance with the provisions of FISMA,1 the Secretary of Commerce shall, on the basis of

standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to

federal information systems. The Secretary shall make standards compulsory and binding to the

extent determined necessary by the Secretary to improve the efficiency of operation or security of

federal information systems. Standards prescribed shall include information security standards

that provide minimum information security requirements and are otherwise necessary to improve

the security of federal information and information systems.

• Federal Information Processing Standards (FIPS) are approved by the Secretary of

Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and

binding for federal agencies.2 FISMA requires that federal agencies comply with these

standards, and therefore, agencies may not waive their use.

• Special Publications (SPs) are developed and issued by NIST as recommendations and

guidance documents. For other than national security programs and systems, federal

agencies must follow those NIST Special Publications mandated in a Federal Information

Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as

amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA

and Agency Privacy Management), state that for other than national security programs

and systems, federal agencies must follow certain specific NIST Special Publications.3

• Other security-related publications, including interagency reports (NISTIRs) and ITL

Bulletins, provide technical and other information about NIST's activities. These

publications are mandatory only when specified by OMB.

• Compliance schedules for NIST security standards and guidelines are established by

OMB.