NIST Special Publication 800-53
Revision 3

National Institute of Standards and Technology
U.S. Department of Commerce

Recommended Security Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

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

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.

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)

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.

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

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.

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies should apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors, should consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government—including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls) for federal information systems. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication. The senior leadership team, working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Assistant Secretary of Defense
DOD Chief Information Officer (Acting)

Robert Lentz
Deputy Assistant Secretary of Defense
for Cyber, Identity, and Information Assurance

Gus Guissanie
Principal Director, ODASD (CIIA)

Don Jones
Senior Policy Advisor, ODASD (CIIA)

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Associate Director of National Intelligence
and Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief
Information Officer

Mark J. Morrison
Deputy Associate Director of National
Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Cheryl J. Roby
Chairman, Committee on National Security
Systems (Acting)

Eustace D. King
CNSS Subcommittee Co-Chairman (DOD)

William Hunteman
CNSS Subcommittee Co-Chairman (DOE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Esten Porter *MITRE Corporation*	George Rogers *BAE Systems, Inc.*
Marianne Swanson *NIST*	Richard Graubart *MITRE Corporation*	Bennett Hodge *Booz Allen Hamilton*	Arnold Johnson *NIST*
Stuart Katzke *NIST*	Glenda Turner *MITRE Corporation*	Kelley Dempsey *NIST*	Christian Enloe *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support; to Donna Dodson, Pat Toth, Matt Scholl, Sharon Keller, Randy Easter, Tim Polk, Murugiah Souppaya, Kevin Stine, Matt Barrett, Steve Quinn, Bill MacGregor, Karen Scarfone, Bill Burr, Doug Montgomery, Scott Rose, Mark Wilson, Annabelle Lee, Ed Roback, and Erika McCallister for their review of the security controls and insightful recommendations. The authors also wish to recognize Marshall Abrams, Jennifer Fabius Greene, Harriett Goldman, John Woodward, Karen Quigg, Joe Weiss, Peter Gouldmann, Roger Johnson, Sarbari Gupta, Dennis Bailey, Richard Wilsher, Nadya Bartol,

Mike Rubin, Tom Madden, Denise Farrar, Paul Bicknell, Robert Niemeyer, and Brett Burley for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.

A special acknowledgment is given to the participants in the *Industrial Control System (ICS) Security Project* who have put forth significant effort in helping to augment the security controls in NIST Special Publication 800-53 for industrial control systems. These participants include: Keith Stouffer, Stu Katzke, and Marshall Abrams from the ICS Security Project Development Team; federal agencies participating in the ICS workshops; and individuals and organizations in the public and private sector ICS community providing insightful comments on the proposed augmentations.

Postscript

Making any significant changes to the publication without public review is not in keeping with the obligation we have to the public and private sector organizations employing the NIST standards and guidelines. Some thoughtful and insightful recommendations received during the final public comment period suggesting changes to the publication have been retained and deferred until the next major revision to Special Publication 800-53. We continue to balance the need for stability in the NIST publications to ensure cost-effective implementation with the need to keep the publications current.

FIPS 200 AND SP 800-53

IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security Controls for Federal Information Systems and Organizations*. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

FIPS 200 and NIST Special Publication 800-53, in combination, help ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Table of Contents

Prologue

"…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

Errata

The following changes have been incorporated into Special Publication 800-53, Revision 3, as of date indicated in table.

DATE	TYPE	CHANGE	PAGE NO.
08-12-2009	Editorial	Concatenate AC-19 d. and AC-19 e.	Page F-17
08-12-2009	Editorial	Change AC-19 f. to AC-19 e.	Page F-17
08-12-2009	Editorial	Change AC-19 g. to AC-19 f.	Page F-17
08-12-2009	Editorial	Change AC-19 h. to AC-19 g.	Page F-17
09-14-2009	Editorial	Change SC-32 Priority Code from P0 to P1.	Page D-7
09-14-2009	Editorial	Change AC-16 (3) from Enhanced to Enhancement	Page F-14
09-14-2009	Editorial	Change AC-16 (4) from Enhanced to Enhancement	Page F-14
09-14-2009	Editorial	Change SC-32 Priority Code from P0 to P1.	Page F-122

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION AND INFORMATION SYSTEMS

The selection and implementation of appropriate *security controls* for an information system[4] or a system-of-systems[5] are important tasks that can have major implications on the operations[6] and assets of an organization[7] as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[8] in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks[9] arising from its information and information systems. The security controls defined in this publication and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. The program management controls (Appendix G), complement the security controls for an information system (Appendix F) by focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

---

[4] An information system is a discrete set of *information resources* organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[5] In certain situations within an organization, an information system can be viewed from both a logical and physical perspective as a complex *system-of-systems* (e.g., Federal Aviation Administration National Air Space System) when there are multiple information systems involved with a high degree of connectivity and interaction among the systems.

[6] Organizational operations include mission, functions, image, and reputation.

[7] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[8] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

[9] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation.