NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

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

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Such information security standards and guidelines shall not apply to national security systems without the express approval of the 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.

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, OMB Director, 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.

National Institute of Standards and Technology Special Publication 800-53, Revision 5
Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, **492 pages** (September 2020)

CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

Certain commercial entities, equipment, or materials may be identified in this document 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, practices, 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 draft publications during the designated public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://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
Email: sec-cert@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) 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 (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security 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 systems security and privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.

Keywords

Assurance; availability; computer security; confidentiality; control; cybersecurity; FISMA; information security; information system; integrity; personally identifiable information; Privacy Act; privacy controls; privacy functions; privacy requirements; Risk Management Framework; security controls; security functions; security requirements; system; system security.

Acknowledgements

This publication was developed by the *Joint Task Force* Interagency Working Group. The group includes representatives from the civil, defense, and intelligence communities. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Department of Commerce, Department of 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 this publication.

Department of Defense

Dana Deasy
Chief Information Officer

John Sherman
Principal Deputy CIO

Mark Hakun
Deputy CIO for Cybersecurity and DoD SISO

Kevin Dulany
Director, Cybersecurity Policy and Partnerships

Office of the Director of National Intelligence

Matthew A. Kozma
Chief Information Officer

Michael E. Waschull
Deputy Chief Information Officer

Clifford M. Conner
Cybersecurity Group and IC CISO

Vacant
Director, Security Coordination Center

National Institute of Standards and Technology

Charles H. Romine
Director, Information Technology Laboratory

Kevin Stine
Acting Cybersecurity Advisor, ITL

Matthew Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Mark G. Hakun
Chair

Susan Dorr
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Chris Johnson
Tri-Chair—Intelligence Community

Vicki Michetti
Tri-Chair—Civil Agencies

Joint Task Force Working Group

Victoria Pillitteri
NIST, JTF Leader

Ehijele Olumese
The MITRE Corporation

Esten Porter
The MITRE Corporation

David Black
The MITRE Corporation

Eduardo Takamura
NIST

McKay Tolboe
DoD

Lydia Humphries
Booz Allen Hamilton

Julie Nethery Snyder
The MITRE Corporation

Rich Graubart
The MITRE Corporation

Ned Goren
NIST

Dorian Pappas
Intelligence Community

Daniel Faigin
Aerospace Corporation

Christina Sames
The MITRE Corporation

Peter Duspiva
Intelligence Community

Andrew Regenscheid
NIST

Kelley Dempsey
NIST

Naomi Lefkovitz
NIST

Christian Enloe
NIST

Kaitlin Boeckl
NIST

Jon Boyens
NIST

In addition to the above acknowledgments, a special note of thanks goes to Jeff Brewer, Jim Foti, and the NIST web team for their outstanding administrative support. The authors also wish to recognize Kristen Baldwin, Carol Bales, John Bazile, Jennifer Besceglie, Sean Brooks, Ruth Cannatti, Kathleen Coupe, Keesha Crosby, Charles Cutshall, Ja'Nelle DeVore, Jennifer Fabius, Jim Fenton, Hildy Ferraiolo, Ryan Galluzzo, Robin Gandhi, Mike Garcia, Paul Grassi, Marc Groman, Matthew Halstead, Kevin Herms, Scott Hill, Ralph Jones, Martin Kihiko, Raquel Leone, Jason Marsico, Kirsten Moncada, Ellen Nadeau, Elaine Newton, Michael Nieles, Michael Nussdorfer, Taylor Roberts, Jasmeet Seehra, Joe Stuntz, Jeff Williams, the professional staff from the NIST Computer Security Division and Applied Cybersecurity Division, and the representatives from the Federal CIO Council, Federal CISO Council, Federal Privacy Council, Control Baseline Interagency Working Group, Security and Privacy Collaboration Working Group, and Federal Privacy Council Risk Management Subcommittee for their ongoing contributions in helping to improve the content of the publication. Finally, the authors gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose insightful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-53

The authors wanted to acknowledge the many individuals who contributed to previous versions of Special Publication 800-53 since its inception in 2005. They include Marshall Abrams, Dennis Bailey, Lee Badger, Curt Barker, Matthew Barrett, Nadya Bartol, Frank Belz, Paul Bicknell, Deb Bodeau, Paul Brusil, Brett Burley, Bill Burr, Dawn Cappelli, Roger Caslow, Corinne Castanza, Mike Cooper, Matt Coose, Dominic Cussatt, George Dinolt, Randy Easter, Kurt Eleam, Denise Farrar, Dave Ferraiolo, Cita Furlani, Harriett Goldman, Peter Gouldmann, Tim Grance, Jennifer Guild, Gary Guissanie, Sarbari Gupta, Priscilla Guthrie, Richard Hale, Peggy Himes, Bennett Hodge, William Hunteman, Cynthia Irvine, Arnold Johnson, Roger Johnson, Donald Jones, Lisa Kaiser, Stuart Katzke, Sharon Keller, Tom Kellermann, Cass Kelly, Eustace King, Daniel Klemm, Steve LaFountain, Annabelle Lee, Robert Lentz, Steven Lipner, William MacGregor, Thomas Macklin, Thomas Madden, Robert Martin, Erika McCallister, Tim McChesney, Michael McEvilley, Rosalie McQuaid, Peter Mell, John Mildner, Pam Miller, Sandra Miravalle, Joji Montelibano, Douglas Montgomery, George Moore, Rama Moorthy, Mark Morrison, Harvey Newstrom, Sherrill Nicely, Robert Niemeyer, LouAnna Notargiacomo, Pat O'Reilly, Tim Polk, Karen Quigg, Steve Quinn, Mark Riddle, Ed Roback, Cheryl Roby, George Rogers, Scott Rose, Mike Rubin, Karen Scarfone, Roger Schell, Jackie Snouffer, Ray Snouffer, Murugiah Souppaya, Gary Stoneburner, Keith Stouffer, Marianne Swanson, Pat Toth, Glenda Turner, Patrick Viscuso, Joe Weiss, Richard Wilsher, Mark Wilson, John Woodward, and Carol Woody.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

RISK MANAGEMENT

Organizations must exercise *due diligence* in managing information security and privacy risk. This is accomplished, in part, by establishing a comprehensive risk management program that uses the flexibility inherent in NIST publications to categorize systems, select and implement security and privacy controls that meet mission and business needs, assess the effectiveness of the controls, authorize the systems for operation, and continuously monitor the systems. Exercising due diligence and implementing robust and comprehensive information security and privacy risk management programs can facilitate compliance with applicable laws, regulations, executive orders, and governmentwide policies. Risk management frameworks and risk management processes are essential in developing, implementing, and maintaining the protection measures necessary to address stakeholder needs and the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, methods, and technologies ensures that information systems and organizations have the necessary trustworthiness and resiliency to support essential mission and business functions, the U.S. critical infrastructure, and continuity of government.

COMMON SECURITY AND PRIVACY FOUNDATIONS

In working with the Office of Management and Budget to develop standards and guidelines required by FISMA, NIST consults with federal agencies, state, local, and tribal governments, and private sector organizations to improve information security and privacy, avoid unnecessary and costly duplication of effort, and help ensure that its publications are complementary with the standards and guidelines used for the protection of national security systems. In addition to a comprehensive and transparent public review and comment process, NIST is engaged in a collaborative partnership with the Office of Management and Budget, Office of the Director of National Intelligence, Department of Defense, Committee on National Security Systems, Federal CIO Council, and Federal Privacy Council to establish a Risk Management Framework (RMF) for information security and privacy for the Federal Government. This common foundation provides the Federal Government and their contractors with cost-effective, flexible, and consistent ways to manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. The framework provides a basis for the reciprocal acceptance of security and privacy control assessment evidence and authorization decisions and facilitates information sharing and collaboration. NIST continues to work with public and private sector entities to establish mappings and relationships between the standards and guidelines developed by NIST and those developed by other organizations. NIST anticipates using these mappings and the gaps they identify to improve the control catalog.

DEVELOPMENT OF INFORMATION SYSTEMS, COMPONENTS, AND SERVICES

With a renewed emphasis on the use of trustworthy, secure information systems and supply chain security, it is essential that organizations express their security and privacy requirements with clarity and specificity in order to obtain the systems, components, and services necessary for mission and business success. Accordingly, this publication provides controls in the System and Services Acquisition (SA) and Supply Chain Risk Management (SR) families that are directed at developers. The scope of the controls in those families includes information system, system component, and system service development *and* the associated developers whether the development is conducted internally by organizations or externally through the contracting and acquisition processes. The affected controls in the control catalog include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, and SR-11.

INFORMATION SYSTEMS — A BROAD-BASED PERSPECTIVE

As we push computers to "the edge," building an increasingly complex world of interconnected systems and devices, security and privacy continue to dominate the national dialogue. There is an urgent need to further strengthen the underlying systems, products, and services that we depend on in every sector of the critical infrastructure to ensure that those systems, products, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. NIST Special Publication 800-53, Revision 5, responds to this need by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations a comprehensive set of security and privacy safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud systems, mobile systems, industrial control systems, and Internet of Things (IoT) devices. Safeguarding measures include both security and privacy controls to protect the critical and essential operations and assets of organizations and the privacy of individuals. The objective is to make the systems we depend on more penetration resistant to attacks, limit the damage from those attacks when they occur, and make the systems resilient, survivable, and protective of individuals' privacy.

CONTROL BASELINES

The control baselines that have previously been included in NIST Special Publication 800-53 have been relocated to NIST Special Publication 800-53B. SP 800-53B contains security and privacy control baselines for federal information systems and organizations. It provides guidance for tailoring control baselines and for developing overlays to support the security and privacy requirements of stakeholders and their organizations. CNSS Instruction 1253 provides control baselines and guidance for security categorization and security control selection for national security systems.

USE OF EXAMPLES IN THIS PUBLICATION

Throughout this publication, *examples* are used to illustrate, clarify, or explain certain items in chapter sections, controls, and control enhancements. These examples are illustrative in nature and are *not* intended to limit or constrain the application of controls or control enhancements by organizations.

FEDERAL RECORDS MANAGEMENT COLLABORATION

Federal records management processes have a nexus with certain information security and privacy requirements and controls. For example, records officers may be managing records retention, including when records will be deleted. Collaborating with records officers on the selection and implementation of security and privacy controls related to records management can support consistency and efficiency and ultimately strengthen the organization's security and privacy posture.

Table of Contents

Executive Summary

As we push computers to "the edge," building an increasingly complex world of connected information systems and devices, security and privacy will continue to dominate the national dialogue. In its 2017 report, *Task Force on Cyber Deterrence* [DSB 2017], the Defense Science Board (DSB) provides a sobering assessment of the current vulnerabilities in the U.S. critical infrastructure and the information systems that support mission-essential operations and assets in the public and private sectors.

> *"…The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed…"*

There is an urgent need to further strengthen the underlying information systems, component products, and services that the Nation depends on in every sector of the critical infrastructure—ensuring that those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. This update to NIST Special Publication (SP) 800-53 responds to the call by the DSB by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations a comprehensive set of safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud-based systems, mobile devices, Internet of Things (IoT) devices, weapons systems, space systems, communications systems, environmental control systems, super computers, and industrial control systems. Those safeguarding measures include implementing security and privacy controls to protect the critical and essential operations and assets of organizations and the privacy of individuals. The objectives are to make the information systems we depend on more penetration-resistant, limit the damage from attacks when they occur, make the systems cyber-resilient and survivable, and protect individuals' privacy.

Revision 5 of this foundational NIST publication represents a multi-year effort to develop the next generation of security and privacy controls that will be needed to accomplish the above objectives. It includes changes to make the controls more usable by diverse consumer groups (e.g., enterprises conducting mission and business functions; engineering organizations developing information systems, IoT devices, and systems-of-systems; and industry partners building system components, products, and services). The most significant changes to this publication include:

- Making the controls more *outcome-based* by removing the entity responsible for satisfying the control (i.e., information system, organization) from the control statement;
- Integrating information security and privacy controls into a seamless, consolidated control catalog for information systems and organizations;
- Establishing a new supply chain risk management control family;
- Separating control selection *processes* from the *controls*, thereby allowing the controls to be used by different communities of interest, including systems engineers, security architects, software developers, enterprise architects, systems security and privacy engineers, and mission or business owners;

- Removing control baselines and tailoring guidance from the publication and transferring the content to NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*;
- Clarifying the relationship between requirements and controls and the relationship between security and privacy controls; and
- Incorporating new, state-of-the-practice controls (e.g., controls to support cyber resiliency, support secure systems design, and strengthen security and privacy governance and accountability) based on the latest threat intelligence and cyber-attack data.

In separating the process of control selection from the controls and removing the control baselines, a significant amount of guidance and other informative material previously contained in SP 800-53 was eliminated. That content will be moved to other NIST publications such as SP 800-37 (Risk Management Framework) and SP 800-53B during the next update cycle. In the near future, NIST also plans to offer the content of SP 800-53, SP 800-53A, and SP 800-53B to a web-based portal to provide its customers interactive, online access to all control, control baseline, overlay, and assessment information.

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

"Networking and information technology [are] transforming life in the 21st century, changing the way people, businesses, and government interact. Vast improvements in computing, storage, and communications are creating new opportunities for enhancing our social wellbeing; improving health and health care; eliminating barriers to education and employment; and increasing efficiencies in many sectors such as manufacturing, transportation, and agriculture.

The promise of these new applications often stems from their ability to create, collect, transmit, process, and archive information on a massive scale. However, the vast increase in the quantity of personal information that is being collected and retained, combined with the increased ability to analyze it and combine it with other information, is creating valid concerns about privacy and about the ability of entities to manage these unprecedented volumes of data responsibly…. A key challenge of this era is to assure that growing capabilities to create, capture, store, and process vast quantities of information will not damage the core values of the country…."

"…When systems process personal information, whether by collecting, analyzing, generating, disclosing, retaining, or otherwise using the information, they can impact privacy of individuals. System designers need to account for individuals as stakeholders in the overall development of the solution.…Designing for privacy must connect individuals' privacy desires with system requirements and controls in a way that effectively bridges the aspirations with development…."

THE NATIONAL PRIVACY RESEARCH STRATEGY
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

Errata

This table contains changes that have been incorporated into SP 800-53, Revision 5. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the SP 800-53, Revision 5 publication details.

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Acknowledgements (ODNI): Add "Matthew A. Kozma, Chief Information Officer"	iii
12-10-2020	Editorial	Acknowledgements (ODNI): Add "Michael E. Waschull, Deputy Chief Information Officer"	iii
12-10-2020	Editorial	Acknowledgements (ODNI): Add "Clifford M. Conner, Cybersecurity Group and IC CISO"	iii
12-10-2020	Editorial	Call Out Box: Change "Special Publication 800-53B contains control baselines" to "SP 800-53B contains security and privacy control baselines"	x
12-10-2020	Editorial	Chapter One (Footnote 7): Add "[SP 800-53A]"	1
12-10-2020	Editorial	Section 1.4: Delete "The controls have also been mapped to the requirements for federal information systems included in [OMB A-130]."	5
12-10-2020	Editorial	Section 1.4 (Footnote 23): Delete "[OMB A-130] establishes policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services."	5
12-10-2020	Editorial	Section 2.4 (first paragraph): Change "personally identifiable information (PII)" to "PII"	13
12-10-2020	Editorial	Control AC-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	18
12-10-2020	Editorial	Control AC-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	18
12-10-2020	Editorial	Control Enhancement AC-3(2) Discussion: Change "authorization duties to other individuals" to "authorization duties"	23
12-10-2020	Editorial	Control Enhancement AC-3(9) Discussion: Change "mitigating control" to "mitigation measure"	26
12-10-2020	Editorial	Control Enhancement AC-3(14) Related Controls: Add ", PT-6"	28
12-10-2020	Editorial	Control Enhancement AC-4(17): Change "*organization, system, application, service, individual*" to "*organization; system; application; service; individual*"	33
12-10-2020	Editorial	Control Enhancement AC-4(25): Change "*Selection (one or more:*" to "*Selection (one or more):*"	34
12-10-2020	Editorial	Control AC-12: Change "*conditions,*" to "*conditions*"	43
12-10-2020	Editorial	Control AC-14 Discussion: Change "assignment" to "assignment operation"	44
12-10-2020	Editorial	Control AC-19 Discussion: Change "the organizational network" to "its network"	52

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Control AC-19 Discussion: Change "Many controls for mobile devices are reflected in other controls allocated to the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some overlap by the security controls within the different families of controls." to "Many safeguards for mobile devices are reflected in other controls."	52
12-10-2020	Editorial	Control AC-20 Discussion: Change "organizational systems" to "organizational systems,"	53
12-10-2020	Editorial	Control Enhancement AC-20(3) Discussion: Change "AC-20(6)" to "AC-20 b."	54
12-10-2020	Editorial	Control AT-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	59
12-10-2020	Editorial	Control AT-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	59
12-10-2020	Editorial	Control AT-2d.: Change "security or privacy incidents" to "security incidents or breaches"	60
12-10-2020	Editorial	Control AT-2 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	60
12-10-2020	Editorial	Control AT-3c.: Change "security or privacy incidents" to "security incidents or breaches"	62
12-10-2020	Editorial	Control AT-3 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	63
12-10-2020	Editorial	Control AT-3 Related Controls: Change "IR-10" to "IR-4"	63
12-10-2020	Editorial	Control AT-6 Discussion: Change "assessment and update" to "evaluation and update"	64
12-10-2020	Editorial	Control AT-6 Discussion: Change "organization training" to "organizational training"	64
12-10-2020	Editorial	Control AU-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	65
12-10-2020	Editorial	Control AU-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	65
12-10-2020	Editorial	Control CA-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	83
12-10-2020	Editorial	Control CA-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	83
12-10-2020	Editorial	Control CA-1 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	84
12-10-2020	Editorial	Control CA-1 References: Add "[SP 800-137A],"	84
12-10-2020	Editorial	Control Enhancement CA-2(2): Change "*data loss assessment*" to "*data loss assessment;*"	86
12-10-2020	Editorial	Control CA-3 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	88
12-10-2020	Editorial	Control CA-7 Discussion: Change "SC-18c" to "SC-18b"	91
12-10-2020	Editorial	Control CM-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	96
12-10-2020	Editorial	Control CM-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	96
12-10-2020	Editorial	Control CM-2b.2.: Change "*Assignment*" to "*Assignment:*"	97
12-10-2020	Editorial	Control Enhancement CM-7(4) Title: Change "UNAUTHORIZED SOFTWARE" to "UNAUTHORIZED SOFTWARE – DENY-BY-EXCEPTION"	106

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Control Enhancement CM-7(5) Title: Change "AUTHORIZED SOFTWARE" to "AUTHORIZED SOFTWARE – ALLOW-BY-EXCEPTION"	106
12-10-2020	Editorial	Control CM-8 Related Controls: Add "CP-9,"	108
12-10-2020	Editorial	Control CP-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	115
12-10-2020	Editorial	Control CP-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	115
12-10-2020	Editorial	Control CP-3 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	119
12-10-2020	Editorial	Control Enhancement CP-9(7) Title: Change "DUAL AUTHORIZATION" to "DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION"	127
12-10-2020	Editorial	Control Enhancement CP-10(3): Change "tailoring procedures" to "tailoring"	128
12-10-2020	Editorial	Control IA-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	131
12-10-2020	Editorial	Control IA-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	131
12-10-2020	Editorial	Control Enhancement IA-2(1) Discussion: Change "Common Access Card" to "Common Access Card (CAC)"	132
12-10-2020	Editorial	Control Enhancement IA-2(7) Title: Change "ACCESS" to "NETWORK ACCESS"	134
12-10-2020	Editorial	Control Enhancement IA-8(5) Discussion: Change "Personal Identity Verification (PIV)" to "PIV"	145
12-10-2020	Editorial	Control IR-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	149
12-10-2020	Editorial	Control IR-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	149
12-10-2020	Editorial	Control Enhancement IR-2(1) Discussion: Delete "Incident response training includes tabletop exercises that simulate a breach. See IR-2(3)."	150
12-10-2020	Editorial	Control IR-4 Related Controls: Add "IR-5,"	152
12-10-2020	Editorial	Control IR-5 Related Controls: Add "IR-4, IR-6,"	156
12-10-2020	Editorial	Control Enhancement IR-5(1) Related Controls: Change "AU-7, IR-4" to "None"	156
12-10-2020	Editorial	Control IR-10: Change "Incident Analysis" to "Integrated Information Security Analysis Team"	161
12-10-2020	Editorial	Control IR-10: Change "Incorporated into" to "Moved to"	161
12-10-2020	Editorial	Control MA-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	162
12-10-2020	Editorial	Control MA-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	162
12-10-2020	Editorial	Control Enhancement MA-4(2): Change "MA-1, MA-4" to "MA-1 and MA-4"	166
12-10-2020	Editorial	Control MP-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	171
12-10-2020	Editorial	Control MP-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	171
12-10-2020	Editorial	Control MP-3 References: Add "[EO 13556],"	172

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Control PE-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	179
12-10-2020	Editorial	Control PE-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	179
12-10-2020	Editorial	Control Enhancement PE-3(8) Discussion: Delete ", or mantrap,"	183
12-10-2020	Editorial	Control Enhancement PE-3(8) Discussion: Change "Mantraps" to "Vestibules"	183
12-10-2020	Editorial	Control Enhancement PE-19(1) Title: Delete "AND TEMPEST"	192
12-10-2020	Editorial	Control PL-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	194
12-10-2020	Editorial	Control PL-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	194
12-10-2020	Editorial	Control PL-2 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	196
12-10-2020	Editorial	Control PL-7 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	198
12-10-2020	Editorial	Control PL-11 Discussion: Change "[FISMA] and [PRIVACT]" to "[FISMA], [PRIVACT], and [OMB A-130]"	201
12-10-2020	Editorial	Control PM-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	204
12-10-2020	Editorial	Control PM-2 References: Add ", [SP 800-181]"	204
12-10-2020	Editorial	Control PM-5 References: Add "[OMB A-130],"	206
12-10-2020	Editorial	Control PM-8 References: Add "[EO 13636],"	207
12-10-2020	Editorial	Control PM-10 References: Add ", [SP 800-181]"	208
12-10-2020	Editorial	Control PM-11 Related Controls: Add "RA-9,"	209
12-10-2020	Editorial	Control PM-12 References: Add "[NITP12],"	210
12-10-2020	Editorial	Control PM-17 References: Add "[SP 800-172],"	212
12-10-2020	Editorial	Control PM-19 Related Controls: Add ", PM-27"	213
12-10-2020	Editorial	Control PM-22 References: Add "[OMB M-19-15],"	216
12-10-2020	Editorial	Control PM-24 Related Controls: Add "PT-2,"	216
12-10-2020	Editorial	Control PM-24 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	217
12-10-2020	Editorial	Control PM-25 Related Controls: Add ", SI-12"	217
12-10-2020	Editorial	Control PM-25 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	217
12-10-2020	Editorial	Control PM-29 References: Add ", [SP 800-181]"	219
12-10-2020	Editorial	Control PM-30 References: Add "[CNSSD 505],"	220
12-10-2020	Editorial	Control PM-31 Discussion: Change "SC-18c" to "SC-18b"	220
12-10-2020	Editorial	Control PM-31 References: Add ", [SP 800-137A]"	221
12-10-2020	Editorial	Control PM-32 References: Change "[SP 800-137]" to "[SP 800-160-1], [SP 800-160-2]"	221
12-10-2020	Editorial	Control PS-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	222
12-10-2020	Editorial	Control PS-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	222
12-10-2020	Editorial	Control Enhancement PS-3(3) Title: Change "WITH" to "REQUIRING"	224
12-10-2020	Editorial	Control PT-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	229
12-10-2020	Editorial	Control PT-1 Discussion: Change "privacy breaches" to "breaches"	229

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Control Enhancement PT-2(1): Change "permissible" to "authorized"	230
12-10-2020	Editorial	Control PT-2 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	231
12-10-2020	Editorial	Control PT-3a.: Change "[Assignment organization-defined purpose(s)]" to "[*Assignment: organization-defined purpose(s)*]"	231
12-10-2020	Editorial	Control PT-3 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	232
12-10-2020	Editorial	Control PT-5 Related Controls: Add "SC-42,"	234
12-10-2020	Editorial	Control Enhancement PT-6(2): Change "[Assignment: organization-defined frequency]" to "[*Assignment: organization-defined frequency*]"	235
12-10-2020	Editorial	Control PT-7 References: Add ", [NARA CUI]"	236
12-10-2020	Editorial	Control PT-8 References: Add "[CMPPA],"	237
12-10-2020	Editorial	Control RA-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	238
12-10-2020	Editorial	Control RA-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	238
12-10-2020	Editorial	Control RA-2 References: Add ", [NARA CUI]"	240
12-10-2020	Editorial	Control RA-3 Related Controls: Add "PT-2,"	240
12-10-2020	Editorial	Control RA-8 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	247
12-10-2020	Editorial	Control RA-9 Related Controls: Add "PM-11,"	247
12-10-2020	Editorial	Control SA-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	249
12-10-2020	Editorial	Control SA-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	249
12-10-2020	Editorial	Control SA-2 References: Add "[SP 800-37], "	250
12-10-2020	Editorial	Control SA-4 References: Add "[ISO 29148], "	255
12-10-2020	Editorial	Control Enhancement SA-9(5) Discussion: Change "security or privacy incidents" to "security incidents or breaches"	273
12-10-2020	Editorial	Control Enhancement SA-10(2) Title: Change "ALTERNATIVE CONFIGURATION MANAGEMENT" to "ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES"	274
12-10-2020	Editorial	Control SA-11a.: Change "assessments" to "control assessments"	276
12-10-2020	Editorial	Control Enhancement SA-12(13): Change "MA-6, RA-9" to "MA-6 and RA-9"	280
12-10-2020	Editorial	Control Enhancement SA-12(14): Change "SR-4(1), SR-4(2)" to "SR-4(1) and SR-4(2)"	280
12-10-2020	Editorial	Control Enhancement SA-17(4)(b): Change "*informal demonstration,*" to "*informal demonstration;*"	286
12-10-2020	Editorial	Control SA-23: Change "*design modification, augmentation, reconfiguration*" to "*design; modification; augmentation; reconfiguration*"	291
12-10-2020	Editorial	Control SC-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	292
12-10-2020	Editorial	Control SC-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	292
12-10-2020	Editorial	Control SC-6: Change "*Selection (one or more);*" to "*Selection (one or more):*"	297

DATE	TYPE	REVISION	PAGE
12-10-2020	Substantive	Control SC-7 Discussion: Add "[SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses."	297
12-10-2020	Substantive	Control Enhancement SC-7(4) Discussion: Delete "Unauthorized control plane traffic can occur through a technique known as spoofing."	298
12-10-2020	Substantive	Control Enhancement SC-7(4) Discussion: Change "routing" to "Border Gateway Protocol (BGP) routing"	298
12-10-2020	Substantive	Control Enhancement SC-7(4) Discussion: Change "management" to "management protocols"	298
12-10-2020	Substantive	Control Enhancement SC-7(4) Discussion: Add "See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements."	298
12-10-2020	Editorial	Control Enhancement SC-7(4) Related Controls: Add ", SC-20, SC-21, SC-22"	298
12-10-2020	Editorial	Control Enhancement SC-7(5): Change "*Selection (one or more);*" to "*Selection (one or more):*"	298
12-10-2020	Editorial	Control SC-14: Change "SI-7," to "SI-7, and"	309
12-10-2020	Editorial	Control SC-17 Discussion: Change "Public Key Infrastructure" to "Public Key Infrastructure (PKI)"	311
12-10-2020	Editorial	Control SC-19: Change "addressed by other controls for protocols" to "addressed as any other technology or protocol"	313
12-10-2020	Editorial	Control Enhancement SC-30(4) Related Controls: Change "SC-26" to "None"	319
12-10-2020	Editorial	Control Enhancement SC-31(2): Change "*Selection (one or more);*" to "*Selection (one or more):*"	320
12-10-2020	Editorial	Control SC-42b.: Change "*class of users*" to "*group of users*"	326
12-10-2020	Editorial	Control SI-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	332
12-10-2020	Editorial	Control SI-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	332
12-10-2020	Editorial	Control SI-3c.1.: Change "*Selection (one or more);*" to "*Selection (one or more):*"	334
12-10-2020	Editorial	Control SI-9: Change "AC-5," to "AC-5, and"	349
12-10-2020	Editorial	Control SI-10 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	351
12-10-2020	Editorial	Control Enhancement SI-12(1): Change "PII" to "personally identifiable information"	352
12-10-2020	Editorial	Control Enhancement SI-12(1) Related Controls: Delete "PT-2, PT-3, RA-3"	352
12-10-2020	Editorial	Control Enhancement SI-12(3) Related Controls: Change "MP-6" to "None"	353
12-10-2020	Editorial	Control SI-12 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	353
12-10-2020	Editorial	Control SI-18 Related Controls: Add "PT-2,"	356
12-10-2020	Editorial	Control Enhancement SI-18(1) Related Controls: Delete "PM-22,"	357
12-10-2020	Editorial	Control Enhancement SI-18(4) Related Controls: Change "PM-22" to "None"	358
12-10-2020	Editorial	Control SI-18 References: Add "[OMB M-19-15],"	358
12-10-2020	Editorial	Control SI-19 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	360
12-10-2020	Editorial	Control SI-20 References: Change "[OMB A-130, Appendix II]" to "[OMB A-130]"	361

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Control SR-1a.1.: Change "*organization-level; mission/business process-level; system-level*" to "*Organization-level; Mission/business process-level; System-level*"	363
12-10-2020	Editorial	Control SR-1 Discussion: Change "security or privacy incidents" to "security incidents or breaches"	363
12-10-2020	Editorial	Control SR-1 References: Add "[CNSSD 505],"	364
12-10-2020	Editorial	Control SR-2 References: Add "[SP 800-181],"	365
12-10-2020	Editorial	Control SR-2 References: Add "[CNSSD 505],"	365
12-10-2020	Editorial	Control Enhancement SR-5(2) Related Controls: Delete "SR-9"	369
12-10-2020	Editorial	Control Enhancement SR-6(1): Change "*organizational analysis, independent third-party analysis, organizational testing, independent third-party testing*" to "*organizational analysis; independent third-party analysis; organizational testing; independent third-party testing*"	370
12-10-2020	Editorial	References [ATOM54]: Change "Atomic Energy Act (P.L. 107)" to "Atomic Energy Act (P.L. 83-703)"	374
12-10-2020	Editorial	References [ISO 15026-1]: Change "International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-1:2013, Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary, November 2013. https://www.iso.org/standard/62526.html" to "International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2019, Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary, March 2019. https://www.iso.org/standard/73567.html"	377
12-10-2020	Editorial	References: Delete "[ISO 28001]"	378
12-10-2020	Editorial	References [ISO 29148]: Change "International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2011, Systems and software engineering—Life cycle processes—Requirements engineering, December 2011. https://www.iso.org/standard/45171.html" to "International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2018, Systems and software engineering—Life cycle processes—Requirements engineering, November 2018. https://www.iso.org/standard/72089.html"	379
12-10-2020	Editorial	References [SP 800-53B]: Change "Draft NIST" to "NIST"	381
12-10-2020	Editorial	References [SP 800-53B]: Change "https://doi.org/10.6028/NIST.SP.800-53B-draft" to "https://doi.org/10.6028/NIST.SP.800-53B"	381
12-10-2020	Editorial	References: Delete "[SP 800-58]"	382
12-10-2020	Editorial	References: Add "[SP 800-137A] Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A"	387
12-10-2020	Editorial	References: Delete "[SP 800-161-1]"	387

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	References [SP 800-181]: Change "Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181" to "Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1"	388
12-10-2020	Editorial	References [DODTERMS]: Change "http://www.dtic.mil/dtic/tr/fulltext/u2/a485800.pdf" to "https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf"	391
12-10-2020	Editorial	Appendix A Glossary (counterfeit): Change "[SP 800-161-1]" to [SP 800-161]"	400
12-10-2020	Editorial	Appendix A Glossary (supplier): Delete "[SP 800-161-1]"	419
12-10-2020	Editorial	Appendix A Glossary (supply chain): Delete "[SP 800-161-1]"	419
12-10-2020	Editorial	Appendix A Glossary (supply chain risk): Delete "[SP 800-161-1]"	420
12-10-2020	Editorial	Appendix A Glossary (supply chain risk assessment): Delete "[SP 800-161-1]"	420
12-10-2020	Editorial	Appendix A Glossary (supply chain risk management): Delete "[SP 800-161-1]"	420
12-10-2020	Editorial	Appendix B Acronyms: Add "BGP Border Gateway Protocol"	424
12-10-2020	Editorial	Appendix B Acronyms: Add "CAC Common Access Card"	424
12-10-2020	Editorial	Appendix B Acronyms: Add "CONOPS Concept of Operations"	424
12-10-2020	Editorial	Appendix B Acronyms: Add "DSB Defense Science Board"	424
12-10-2020	Editorial	Appendix B Acronyms: Add "FICAM Federal Identity, Credential, and Access Management"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "IEEE Institute of Electrical and Electronics Engineers"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "ISAC Information Sharing and Analysis Centers"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "ISAO Information Sharing and Analysis Organizations"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "ITL Information Technology Laboratory"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "MLS Multilevel Secure"	425
12-10-2020	Editorial	Appendix B Acronyms: Add "NDA Non-Disclosure Agreement"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "ODNI Office of the Director of National Intelligence"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "OPM Office of Personnel Management"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "PDS Position Designation System"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "RPKI Resource Public Key Infrastructure"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "SCRM Supply Chain Risk Management"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "SDLC System Development Life Cycle"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "SIEM Security Information and Event Management"	426
12-10-2020	Editorial	Appendix B Acronyms: Add "SWID Software Identification"	427
12-10-2020	Editorial	Appendix B Acronyms: Add "TIC Trusted Internet Connections"	427
12-10-2020	Editorial	Appendix B Acronyms: Add "UEFI Unified Extensible Firmware Interface"	427

DATE	TYPE	REVISION	PAGE
12-10-2020	Editorial	Appendix B Acronyms: Add “UPS Uninterruptible Power Supply”	427
12-10-2020	Editorial	Appendix C Control Summaries: Change “w” to “W”	428
12-10-2020	Editorial	Table C-1 (AC-3(1)) Title: Change “FUNCTION” to “FUNCTIONS”	429
12-10-2020	Editorial	Table C-1 (AC-3(6)): Change “MP-4, SC-28” to “MP-4 and SC-28”	429
12-10-2020	Editorial	Table C-1 (AC-13): Change “AC-2, AU-6” to “AC-2 and AU-6”	431
12-10-2020	Editorial	Table C-3 (AU-7(2)) Title: Change “SEARCH AND SORT” to “SORT AND SEARCH”	434
12-10-2020	Editorial	Table C-3 AU-15: Change “Incorporated into” to “Moved to”	435
12-10-2020	Editorial	Table C-4 (CA-3(1)) Title: Change “CONNECTIONS” to “SYSTEM CONNECTIONS”	436
12-10-2020	Editorial	Table C-5 (CM-7(4)) Title: Change “UNAUTHORIZED SOFTWARE” to “UNAUTHORIZED SOFTWARE – DENY-BY-EXCEPTION”	437
12-10-2020	Editorial	Table C-5 (CM-7(5)) Title: Change “AUTHORIZED SOFTWARE” to “AUTHORIZED SOFTWARE – ALLOW-BY-EXCEPTION”	437
12-10-2020	Editorial	Table C-5: Delete duplicate row CM-8(5).	438
12-10-2020	Editorial	Table C-6 (CP-9(7)) Title: Change “DUAL AUTHORIZATION” to “DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION”	440
12-10-2020	Editorial	Table C-7 (IA-5(11)): Change “IA-2(1)(2)” to “IA-2(1) and IA-2(2)”	441
12-10-2020	Editorial	Table C-8 (IR-10) Title: Change “Integrated Information Security Analysis” to “Integrated Information Security Analysis Team”	444
12-10-2020	Editorial	Table C-9 (MA-4(2)): Change “MA-1, MA-4” to “MA-1 and MA-4”	445
12-10-2020	Editorial	Table C-11 (PE-7): Change “PE-2, PE-3” to “PE-2 and PE-3”	447
12-10-2020	Editorial	Table C-11 (PE-19(1)) Title: Delete ”AND TEMPEST”	448
12-10-2020	Editorial	Table C-14 (PS-3(1)) Title: Change “INFORMATION” to “INFORMATION”	451
12-10-2020	Editorial	Table C-14 (PS-3(3)) Title: Change “WITH” to “REQUIRING”	451
12-10-2020	Editorial	Table C-17 (SA-6): Change “CM-10, SI-7” to “CM-10 and SI-7”	454
12-10-2020	Editorial	Table C-17 (SA-7): Change “CM-11, SI-7” to “CM-11 and SI-7”	454
12-10-2020	Editorial	Table C-17 (SA-12(13)): Change “MA-6, RA-9” to “MA-6 and RA-9”	456
12-10-2020	Editorial	Table C-17 (SA-12(14)): Change “SR-4(1)(2)” to “SR-4(1) and SR-4(2)”	456
12-10-2020	Editorial	Table C-17 (SA-12(15)) Title: Change “PROCESS” to “PROCESSES”	456
12-10-2020	Editorial	Table C-18 (SC-7(25)) Title: Change “CONNECTIONS” to “SYSTEM CONNECTIONS”	459
12-10-2020	Editorial	Table C-18 (SC-12(4)): Change “SC-12” to “SC-12(3)”	459
12-10-2020	Editorial	Table C-18 (SC-12(5)): Change “SC-12” to “SC-12(3)”	459
12-10-2020	Editorial	Table C-18 (SC-14): Change “SI-7,” to “SI-7, and”	459
12-10-2020	Editorial	Table C-18 (SC-19): Change “addressed by other controls for protocols” to “addressed as any other technology or protocol.”	460
12-10-2020	Editorial	Table C-19 (SI-9): Change “AC-5,” to “AC-5, and”	463
12-10-2020	Editorial	Table C-19 (SI-19(7)) Title: Change “SOFTWARE” to “AND SOFTWARE”	464

CHAPTER ONE

INTRODUCTION

THE NEED TO PROTECT INFORMATION, SYSTEMS, ORGANIZATIONS, AND INDIVIDUALS

Modern information systems[1] can include a variety of computing platforms (e.g., industrial control systems, general purpose computing systems, cyber-physical systems, super computers, weapons systems, communications systems, environmental control systems, medical devices, embedded devices, sensors, and mobile devices such as smart phones and tablets). These platforms all share a common foundation—computers with complex hardware, software and firmware providing a capability that supports the essential mission and business functions of organizations.[2]

Security controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security[3] risk. Privacy controls are the administrative, technical, and physical safeguards employed within a system or an organization to manage privacy risks and to ensure compliance with applicable privacy requirements.[4] Security and privacy controls are selected and implemented to satisfy security and privacy requirements levied on a system or organization. Security and privacy requirements are derived from applicable laws, executive orders, directives, regulations, policies, standards, and mission needs to ensure the confidentiality, integrity, and availability of information processed, stored, or transmitted and to manage risks to individual privacy.

The selection, design, and implementation of security and privacy controls[5] are important tasks that have significant implications for the operations[6] and assets of organizations as well as the welfare of individuals and the Nation. Organizations should answer several key questions when addressing information security and privacy controls:

- What security and privacy controls are needed to satisfy security and privacy requirements and to adequately manage mission/business risks or risks to individuals?
- Have the selected controls been implemented or is there a plan in place to do so?
- What is the required level of assurance (i.e., grounds for confidence) that the selected controls, as designed and implemented, are effective?[7]

[1] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [OMB A-130].

[2] 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).

[3] The two terms *information security* and *security* are used synonymously in this publication.

[4] [OMB A-130] defines *security* and *privacy controls*.

[5] Controls provide safeguards and countermeasures in systems security and privacy engineering processes to reduce risk during the system development life cycle.

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

[7] Security and privacy 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 designated security and privacy requirements [SP 800-53A].

The answers to these questions are not given in isolation but rather in the context of a risk management process for the organization that identifies, assesses, responds to, and monitors security and privacy risks arising from its information and systems on an ongoing basis.[8] The security and privacy controls in this publication are recommended for use by organizations to satisfy their information security and privacy requirements. The control catalog can be viewed as a toolbox containing a collection of safeguards, countermeasures, techniques, and processes to respond to security and privacy risks. The controls are employed as part of a well-defined risk management process that supports organizational information security and privacy programs. In turn, those information security and privacy programs lay the foundation for the success of the mission and business functions of the organization.

It is important that responsible officials understand the security and privacy risks that could adversely affect organizational operations and assets, individuals, other organizations, and the Nation.[9] These officials must also understand the current status of their security and privacy programs and the controls planned or in place to protect information, information systems, and organizations in order to make informed judgments and investments that respond to identified risks in an acceptable manner. The objective is to manage these risks through the selection and implementation of security and privacy controls.

1.1 PURPOSE AND APPLICABILITY

This publication establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information. The use of these controls is mandatory for federal information systems[10] in accordance with Office of Management and Budget (OMB) Circular A-130 [OMB A-130] and the provisions of the Federal Information Security Modernization Act[11] [FISMA], which requires the implementation of minimum controls to protect federal information and information systems.[12] This publication, along with other supporting NIST publications, is designed to help organizations identify the security and privacy controls needed to manage risk and to satisfy the security and privacy requirements in FISMA, the Privacy Act of 1974 [PRIVACT], OMB policies (e.g., [OMB A-130]), and designated Federal Information Processing Standards (FIPS), among others. It accomplishes this objective by providing a comprehensive and flexible catalog of security and privacy controls to meet current and future protection needs based on changing threats, vulnerabilities, requirements, and technologies. The publication also improves communication among organizations by providing a common lexicon that supports the discussion of security, privacy, and risk management concepts.

[8] The Risk Management Framework in [SP 800-37] is an example of a comprehensive risk management process.

[9] This includes risk to critical infrastructure and key resources described in [HSPD-7].

[10] A *federal information system* is an information system used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency.

[11] Information systems that have been designated as national security systems, as defined in 44 U.S.C., Section 3542, are not subject to the requirements in [FISMA]. However, the controls established in this publication may be selected for national security systems as otherwise required (e.g., the Privacy Act of 1974) or with the approval of federal officials exercising policy authority over such systems. [CNSSP 22] and [CNSSI 1253] provide guidance for national security systems. [DODI 8510.01] provides guidance for the Department of Defense.

[12] While the controls established in this publication are mandatory for federal information systems and organizations, other organizations such as state, local, and tribal governments as well as private sector organizations are encouraged to consider using these guidelines, as appropriate. See [SP 800-53B] for federal control baselines.

Finally, the controls are independent of the process employed to select those controls. The control selection process can be part of an organization-wide risk management process, a systems engineering process [SP 800-160-1],[13] the Risk Management Framework [SP 800-37], the Cybersecurity Framework [NIST CSF], or the Privacy Framework [NIST PF].[14] The control selection criteria can be guided and informed by many factors, including mission and business needs, stakeholder protection needs, threats, vulnerabilities, and requirements to comply with federal laws, executive orders, directives, regulations, policies, standards, and guidelines. The combination of a catalog of security and privacy controls and a risk-based control selection process can help organizations comply with stated security and privacy requirements, obtain adequate security for their information systems, and protect the privacy of individuals.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience, including:

- Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;
- Individuals with system development responsibilities, including mission owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials;
- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;
- Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;
- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts; and
- Commercial entities, including industry partners, producing component products and systems, creating security and privacy technologies, or providing services or capabilities that support information security or privacy.

1.3 ORGANIZATIONAL RESPONSIBILITIES

Managing security and privacy risks is a complex, multifaceted undertaking that requires:

- Well-defined security and privacy requirements for systems and organizations;
- The use of trustworthy information system components based on state-of-the-practice hardware, firmware, and software development and acquisition processes;

[13] Risk management is an integral part of systems engineering, systems security engineering, and privacy engineering.

[14] [OMB A-130] requires federal agencies to implement the NIST Risk Management Framework for the selection of controls for federal information systems. [EO 13800] requires federal agencies to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity* to manage cybersecurity risk. The NIST frameworks are also available to nonfederal organizations as optional resources.

- Rigorous security and privacy planning and system development life cycle management;
- The application of system security and privacy engineering principles and practices to securely develop and integrate system components into information systems;
- The employment of security and privacy practices that are properly documented and integrated into and supportive of the institutional and operational processes of organizations; and
- Continuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization-wide.

Organizations continuously assess the security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Security and privacy risks arise from the planning and execution of organizational mission and business functions, placing information systems into operation, or continuing system operations. Realistic assessments of risk require a thorough understanding of the susceptibility to threats based on the specific vulnerabilities in information systems and organizations and the likelihood and potential adverse impacts of successful exploitations of such vulnerabilities by those threats.[15] Risk assessments also require an understanding of privacy risks.[16]

To address the organization's concerns about assessment and determination of risk, security and privacy requirements are satisfied with the knowledge and understanding of the organizational risk management strategy.[17] The risk management strategy considers the cost, schedule, performance, and supply chain issues associated with the design, development, acquisition, deployment, operation, sustainment, and disposal of organizational systems. A risk management process is then applied to manage risk on an ongoing basis.[18]

The catalog of security and privacy controls can be effectively used to protect organizations, individuals, and information systems from traditional and advanced persistent threats and privacy risks arising from the processing of personally identifiable information (PII) in varied operational, environmental, and technical scenarios. The controls can be used to demonstrate compliance with a variety of governmental, organizational, or institutional security and privacy requirements. Organizations have the responsibility to select the appropriate security and privacy controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying security and privacy requirements.[19] Security and privacy controls can also be used in developing specialized *baselines* or *overlays* for unique or specialized missions or business applications, information systems, threat concerns, operational environments, technologies, or communities of interest.[20]

[15] [SP 800-30] provides guidance on the risk assessment process.

[16] [IR 8062] introduces privacy risk concepts.

[17] [SP 800-39] provides guidance on risk management processes and strategies.

[18] [SP 800-37] provides a comprehensive risk management process.

[19] [SP 800-53A] provides guidance on assessing the effectiveness of controls.

[20] [SP 800-53B] provides guidance for tailoring security and privacy control baselines and for developing overlays to support the specific protection needs and requirements of stakeholders and their organizations.

Organizational risk assessments are used, in part, to inform the security and privacy control selection process. The selection process results in an agreed-upon set of security and privacy controls addressing specific mission or business needs consistent with organizational risk tolerance.[21] The process preserves, to the greatest extent possible, the agility and flexibility that organizations need to address an increasingly sophisticated and hostile threat space, mission and business requirements, rapidly changing technologies, complex supply chains, and many types of operational environments.

1.4 RELATIONSHIP TO OTHER PUBLICATIONS

This publication defines controls to satisfy a diverse set of security and privacy requirements that have been levied on information systems and organizations and that are consistent with and complementary to other recognized national and international information security and privacy standards. To develop a broadly applicable and technically sound set of controls for information systems and organizations, many sources were considered during the development of this publication. These sources included requirements and controls from the manufacturing, defense, financial, healthcare, transportation, energy, intelligence, industrial control, and audit communities as well as national and international standards organizations. In addition, the controls in this publication are used by the national security community in publications such as Committee on National Security Systems (CNSS) Instruction No. 1253 [CNSSI 1253] to provide guidance specific to systems designated as national security systems. Whenever possible, the controls have been mapped to international standards to help ensure maximum usability and applicability.[22] The relationship of this publication to other risk management, security, privacy, and publications can be found at [FISMA IMP].

1.5 REVISIONS AND EXTENSIONS

The security and privacy controls described in this publication represent the state-of-the-practice protection measures for individuals, information systems, and organizations. The controls are reviewed and revised periodically to reflect the experience gained from using the controls; new or revised laws, executive orders, directives, regulations, policies, and standards; changing security and privacy requirements; emerging threats, vulnerabilities, attack and information processing methods; and the availability of new technologies.

The security and privacy controls in the control catalog are also expected to change over time as controls are withdrawn, revised, and added. In addition to the need for change, the need for stability is addressed by requiring that proposed modifications to security and privacy controls go through a rigorous and transparent public review process to obtain public and private sector feedback and to build a consensus for such change. The review process provides a technically sound, flexible, and stable set of security and privacy controls for the organizations that use the control catalog.

1.6 PUBLICATION ORGANIZATION

The remainder of this special publication is organized as follows:

[21] Authorizing officials or their designated representatives, by accepting the security and privacy plans, agree to the security and privacy controls proposed to meet the security and privacy requirements for organizations and systems.

[22] Mapping tables are available at [SP 800-53 RES].

- **Chapter Two** describes the fundamental concepts associated with security and privacy controls, including the structure of the controls, how the controls are organized in the consolidated catalog, control implementation approaches, the relationship between security and privacy controls, and trustworthiness and assurance.
- **Chapter Three** provides a consolidated catalog of security and privacy controls including a discussion section to explain the purpose of each control and to provide useful information regarding control implementation and assessment, a list of related controls to show the relationships and dependencies among controls, and a list of references to supporting publications that may be helpful to organizations.
- **References**, **Glossary**, **Acronyms**, and **Control Summaries** provide additional information on the use of security and privacy controls.[23]

[23] Unless otherwise stated, all references to NIST publications refer to the most recent version of those publications.

CHAPTER TWO

THE FUNDAMENTALS

STRUCTURE, TYPE, AND ORGANIZATION OF SECURITY AND PRIVACY CONTROLS

This chapter presents the fundamental concepts associated with security and privacy controls, including the relationship between requirements and controls, the structure of controls, how controls are organized in the consolidated control catalog, the different control implementation approaches for information systems and organizations, the relationship between security and privacy controls, the importance of the concepts of trustworthiness and assurance for security and privacy controls, and the effects of the controls on achieving trustworthy, secure, and resilient systems.

2.1 REQUIREMENTS AND CONTROLS

It is important to understand the relationship between requirements and controls. For federal information security and privacy policies, the term *requirement* is generally used to refer to information security and privacy obligations imposed on organizations. For example, [OMB A-130] imposes information security and privacy requirements with which federal agencies must comply when managing information resources. The term *requirement* can also be used in a broader sense to refer to an expression of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). The term *requirement*, as used in this guideline, includes both legal and policy requirements, as well as an expression of the broader set of stakeholder protection needs that may be derived from other sources. All of these requirements, when applied to a system, help determine the necessary characteristics of the system—encompassing security, privacy, and assurance.[24]

Organizations may divide security and privacy requirements into more granular categories, depending on where the requirements are employed in the system development life cycle (SDLC) and for what purpose. Organizations may use the term *capability requirement* to describe a capability that the system or organization must provide to satisfy a stakeholder protection need. In addition, organizations may refer to system requirements that pertain to particular hardware, software, and firmware components of a system as *specification requirements*—that is, capabilities that implement all or part of a control and that may be assessed (i.e., as part of the verification, validation, testing, and evaluation processes). Finally, organizations may use the term *statement of work requirements* to refer to actions that must be performed operationally or during system development.

[24] The system characteristics that impact security and privacy vary and include the system type and function in terms of its primary purpose; the system make-up in terms of its technology, mechanical, physical, and human elements; the modes and states within which the system delivers its functions and services; the criticality or importance of the system and its constituent functions and services; the sensitivity of the data or information processed, stored, or transmitted; the consequence of loss, failure, or degradation relative to the ability of the system to execute correctly and to provide for its own protection (i.e., self-protection); and monetary or other value [SP 800-160-1].

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include administrative, technical, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of *derived requirements* or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for particular controls within the SDLC.

2.2 CONTROL STRUCTURE AND ORGANIZATION

Security and privacy controls described in this publication have a well-defined organization and structure. For ease of use in the security and privacy control selection and specification process, controls are organized into 20 *families*.[25] Each family contains controls that are related to the specific topic of the family. A two-character identifier uniquely identifies each control family (e.g., *PS* for Personnel Security). Security and privacy controls may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms that are implemented by systems or actions by individuals. Table 1 lists the security and privacy control families and their associated family identifiers.

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Families of controls contain base controls and control enhancements, which are directly related to their base controls. Control enhancements either add functionality or specificity to a base control or increase the strength of a base control. Control enhancements are used in systems and environments of operation that require greater protection than the protection provided by the base control. The need for organizations to select and implement control enhancements is due to the potential adverse organizational or individual impacts or when organizations require additions to the base control functionality or assurance based on assessments of risk. The

[25] Of the 20 control families in NIST SP 800-53, 17 are aligned with the minimum security requirements in [FIPS 200]. The Program Management (PM), PII Processing and Transparency (PT), and Supply Chain Risk Management (SR) families address enterprise-level program management, privacy, and supply chain risk considerations pertaining to federal mandates emergent since [FIPS 200].