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].

selection and implementation of control enhancements *always* requires the selection and implementation of the base control.

The families are arranged in alphabetical order, while the controls and control enhancements within each family are in numerical order. The order of the families, controls, and control enhancements does *not* imply any logical progression, level of prioritization or importance, or order in which the controls or control enhancements are to be implemented. Rather, it reflects the order in which they were included in the catalog. Control designations are not re-used when a control is withdrawn.

Security and privacy controls have the following structure: a *base control* section, a *discussion* section, a *related controls* section, a *control enhancements* section, and a *references* section. Figure 1 illustrates the structure of a typical control.

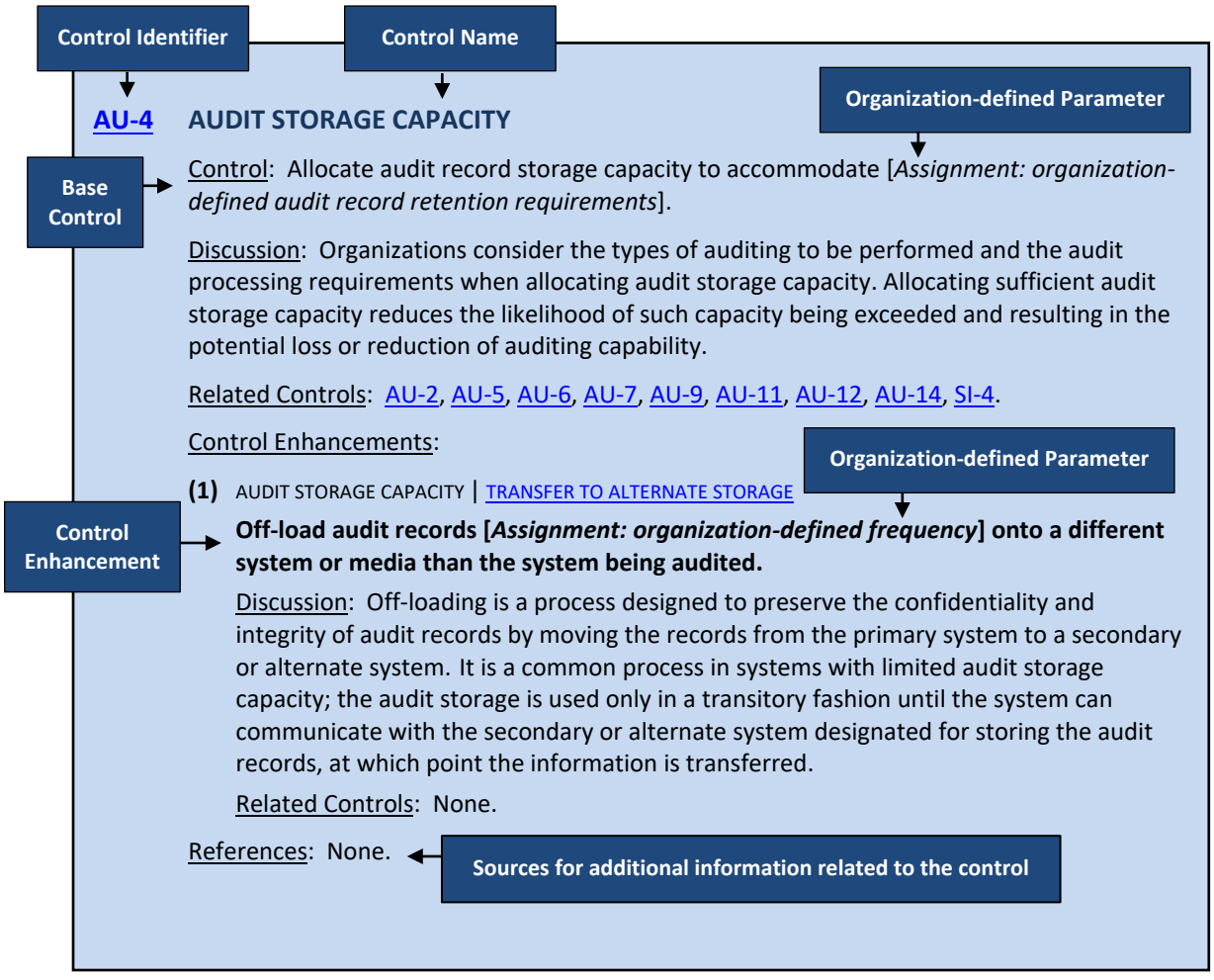

FIGURE 1: CONTROL STRUCTURE

The *control* section prescribes a security or privacy capability to be implemented. Security and privacy capabilities are achieved by the activities or actions, automated or nonautomated, carried out by information systems and organizations. Organizations designate the responsibility for control development, implementation, assessment, and monitoring. Organizations have the

flexibility to implement the controls selected in whatever manner that satisfies organizational mission or business needs consistent with law, regulation, and policy.

The *discussion* section provides additional information about a control. Organizations can use the information as needed when developing, tailoring, implementing, assessing, or monitoring controls. The information provides important considerations for implementing controls based on mission or business requirements, operational environments, or assessments of risk. The additional information can also explain the purpose of controls and often includes examples. Control enhancements may also include a separate discussion section when the discussion information is applicable only to a specific control enhancement.

The *related controls* section provides a list of controls from the control catalog that impact or support the implementation of a particular control or control enhancement, address a related security or privacy capability, or are referenced in the discussion section. Control enhancements are inherently related to their base control. Thus, related controls that are referenced in the base control are not repeated in the control enhancements. However, there may be related controls identified for control enhancements that are not referenced in the base control (i.e., the related control is only associated with the specific control enhancement). Controls may also be related to enhancements of other base controls. When a control is designated as a related control, a corresponding designation is made on that control in its source location in the catalog to illustrate the two-way relationship. Additionally, each control in a given family is inherently related to the -1 control (Policy and Procedures) in the same family. Therefore, the relationship between the -1 control and the other controls in the same family is not specified in the *related controls* section for each control.

The *control enhancements* section provides statements of security and privacy capability that augment a base control. The control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the base control. Each control enhancement has a short subtitle to indicate the intended function or capability provided by the enhancement. In the AU-4 example, if the control enhancement is selected, the control designation becomes AU-4(1). The numerical designation of a control enhancement is used only to identify that enhancement within the control. The designation is not indicative of the strength of the control enhancement, level of protection, priority, degree of importance, or any hierarchical relationship among the enhancements. Control enhancements are not intended to be selected independently. That is, if a control enhancement is selected, then the corresponding base control is also selected and implemented.

The *references* section includes a list of applicable laws, policies, standards, guidelines, websites, and other useful references that are relevant to a specific control or control enhancement.[26] The references section also includes hyperlinks to publications for obtaining additional information for control development, implementation, assessment, and monitoring.

For some controls, additional flexibility is provided by allowing organizations to define specific values for designated parameters associated with the controls. Flexibility is achieved as part of a tailoring process using *assignment* and *selection* operations embedded within the controls and

[26] References are provided to assist organizations in understanding and implementing the security and privacy controls and are not intended to be inclusive or complete.

enclosed by brackets. The assignment and selection operations give organizations the capability to customize controls based on organizational security and privacy requirements. In contrast to assignment operations which allow complete flexibility in the designation of parameter values, selection operations narrow the range of potential values by providing a specific list of items from which organizations choose.

Determination of the organization-defined parameters can evolve from many sources, including laws, executive orders, directives, regulations, policies, standards, guidance, and mission or business needs. Organizational risk assessments and risk tolerance are also important factors in determining the values for control parameters. Once specified by the organization, the values for the assignment and selection operations become a part of the control. Organization-defined control parameters used in the base controls also apply to the control enhancements associated with those controls. The implementation of the control is assessed for effectiveness against the completed control statement.

In addition to assignment and selection operations embedded in a control, additional flexibility is achieved through *iteration* and *refinement* actions. Iteration allows organizations to use a control multiple times with different assignment and selection values, perhaps being applied in different situations or when implementing multiple policies. For example, an organization may have multiple systems implementing a control but with different parameters established to address different risks for each system and environment of operation. Refinement is the process of providing additional implementation detail to a control. Refinement can also be used to narrow the scope of a control in conjunction with iteration to cover all applicable scopes (e.g., applying different authentication mechanisms to different system interfaces). The combination of assignment and selection operations and iteration and refinement actions when applied to controls provides the needed flexibility to allow organizations to satisfy a broad base of security and privacy requirements at the organization, mission and business process, and system levels of implementation.

SECURITY AS A DESIGN PROBLEM

"Providing satisfactory security controls in a computer system is….a system design problem. A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security….software safeguards alone are not sufficient."

-- ***The Ware Report***
Defense Science Board Task Force on Computer Security, 1970

2.3 CONTROL IMPLEMENTATION APPROACHES

There are three approaches to implementing the controls in Chapter Three: (1) a *common* (inheritable) control implementation approach, (2) a *system-specific* control implementation approach, and (3) a *hybrid* control implementation approach. The control implementation approaches define the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and

authorization. Each control implementation approach has a specific objective and focus that helps organizations select the appropriate controls, implement the controls in an effective manner, and satisfy security and privacy requirements. A specific control implementation approach may achieve cost benefits by leveraging security and privacy capabilities across multiple systems and environments of operation.[27]

Common controls are controls whose implementation results in a capability that is *inheritable* by multiple systems or programs. A control is deemed inheritable when the system or program receives protection from the implemented control, but the control is developed, implemented, assessed, authorized, and monitored by an internal or external entity other than the entity responsible for the system or program. The security and privacy capabilities provided by common controls can be inherited from many sources, including mission or business lines, organizations, enclaves, environments of operation, sites, or other systems or programs. Implementing controls as common controls can introduce the risk of a single point of failure.

Many of the controls needed to protect organizational information systems—including many physical and environmental protection controls, personnel security controls, and incident response controls—are inheritable and, therefore, are good candidates for common control status. Common controls can also include technology-based controls, such as identification and authentication controls, boundary protection controls, audit and accountability controls, and access controls. The cost of development, implementation, assessment, authorization, and monitoring can be amortized across multiple systems, organizational elements, and programs using the common control implementation approach.

Controls not implemented as common controls are implemented as *system-specific* or *hybrid* controls. System-specific controls are the primary responsibility of the system owner and the authorizing official for a given system. Implementing system-specific controls can introduce risk if the control implementations are not interoperable with common controls. Organizations can implement a control as *hybrid* if one part of the control is common (inheritable) and the other part is system-specific. For example, an organization may implement control CP-2 using a predefined template for the contingency plan for all organizational information systems with individual system owners tailoring the plan for system-specific uses, where appropriate. The division of a hybrid control into its common (inheritable) and system-specific parts may vary by organization, depending on the types of information technologies employed, the approach used by the organization to manage its controls, and assignment of responsibilities. When a control is implemented as a hybrid control, the common control provider is responsible for ensuring the implementation, assessment, and monitoring of the *common* part of the hybrid control, and the system owner is responsible for ensuring the implementation, assessment, and monitoring of the *system-specific* part of the hybrid control. Implementing controls as hybrid controls can introduce risk if the responsibility for the implementation and ongoing management of the common and system-specific parts of the controls is unclear.

The determination as to the appropriate control implementation approach (i.e., common, hybrid, or system-specific) is context-dependent. The control implementation approach cannot be determined to be common, hybrid, or system-specific simply based on the language of the

[27] [SP 800-37] provides additional guidance on control implementation approaches (formerly referred to as control designations) and how the different approaches are used in the *Risk Management Framework*.

control. Identifying the control implementation approach can result in significant savings to organizations in implementation and assessment costs and a more consistent application of the controls organization-wide. Typically, the identification of the control implementation approach is straightforward. However, the implementation takes significant planning and coordination.

Planning for the implementation approach of a control (i.e., common, hybrid, or system-specific) is best carried out early in the system development life cycle and coordinated with the entities providing the control [SP 800-37]. Similarly, if a control is to be inheritable, coordination is required with the inheriting entity to ensure that the control meets its needs. This is especially important given the nature of control parameters. An inheriting entity cannot assume that controls are the same and mitigate the appropriate risk to the system just because the control identifiers (e.g., AC-1) are the same. It is essential to examine the control parameters (e.g., assignment or selection operations) when determining if a common control is adequate to mitigate system-specific risks.

2.4 SECURITY AND PRIVACY CONTROLS

The selection and implementation of security and privacy controls reflect the objectives of information security and privacy programs and how those programs manage their respective risks. Depending on the circumstances, these objectives and risks can be independent or overlapping. Federal information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized activity or system behavior) to provide confidentiality, integrity, and availability. Those programs are also responsible for managing security risk and for ensuring compliance with applicable security requirements. Federal privacy programs are responsible for managing risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as "processing") of PII and for ensuring compliance with applicable privacy requirements.[28] When a system processes PII, the information security program and the privacy program have a shared responsibility for managing the security risks for the PII in the system. Due to this overlap in responsibilities, the controls that organizations select to manage these security risks will generally be the same regardless of their designation as security or privacy controls in control baselines or program or system plans.

There also may be circumstances in which the selection and/or implementation of the control or control enhancement affects the ability of a program to achieve its objectives and manage its respective risks. The control discussion section may highlight specific security and/or privacy considerations so that organizations can take these considerations into account as they determine the most effective method to implement the control. However, these considerations are not exhaustive.

For example, an organization might select AU-3 (Content of Audit Records) to support monitoring for unauthorized access to an information asset that does not include PII. Since the

[28] Privacy programs may also choose to consider the risks to individuals that may arise from their interactions with information systems, where the processing of personally identifiable information may be less impactful than the effect that the system has on individuals' behavior or activities. Such effects would constitute risks to individual autonomy, and organizations may need to take steps to manage those risks in addition to information security and privacy risks.

potential loss of confidentiality of the information asset does not affect privacy, security objectives are the primary driver for the selection of the control. However, the implementation of the control with respect to monitoring for unauthorized access could involve the processing of PII which may result in privacy risks and affect privacy program objectives. The discussion section in AU-3 includes privacy risk considerations so that organizations can take those considerations into account as they determine the best way to implement the control. Additionally, the control enhancement AU-3(3) (Limit Personally Identifiable Information Elements) could be selected to support managing these privacy risks.

Due to permutations in the relationship between information security and privacy program objectives and risk management, there is a need for close collaboration between programs to select and implement the appropriate controls for information systems processing PII. Organizations consider how to promote and institutionalize collaboration between the two programs to ensure that the objectives of both disciplines are met and risks are appropriately managed.[29]

2.5 TRUSTWORTHINESS AND ASSURANCE

The trustworthiness of systems, system components, and system services is an important part of the risk management strategies developed by organizations.[30] *Trustworthiness*, in this context, means worthy of being trusted to fulfill whatever requirements may be needed for a component, subsystem, system, network, application, mission, business function, enterprise, or other entity.[31] Trustworthiness requirements can include attributes of reliability, dependability, performance, resilience, safety, security, privacy, and survivability under a range of potential adversity in the form of disruptions, hazards, threats, and privacy risks. Effective measures of trustworthiness are meaningful only to the extent that the requirements are complete, well-defined, and can be accurately assessed.

Two fundamental concepts that affect the trustworthiness of systems are *functionality* and *assurance*. Functionality is defined in terms of the security and privacy features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems and programs and the environments in which those systems and programs operate. Assurance is the measure of confidence that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system—thus possessing the capability to accurately mediate and enforce established security and privacy policies.

In general, the task of providing meaningful assurance that a system is likely to do what is expected of it can be enhanced by techniques that simplify or narrow the analysis by, for example, increasing the discipline applied to the system architecture, software design, specifications, code style, and configuration management. Security and privacy controls address functionality and assurance. Certain controls focus primarily on functionality while other controls focus primarily on assurance. Some controls can support functionality and assurance.

[29] Resources to support information security and privacy program collaboration are available at [SP 800-53 RES].

[30] [SP 800-160-1] provides guidance on systems security engineering and the application of security design principles to achieve trustworthy systems.

[31] See [NEUM04].

Organizations can select assurance-related controls to define system development activities, generate evidence about the functionality and behavior of the system, and trace the evidence to the system elements that provide such functionality or exhibit such behavior. The evidence is used to obtain a degree of confidence that the system satisfies the stated security and privacy requirements while supporting the organization's mission and business functions. Assurance-related controls are identified in the control summary tables in Appendix C.

EVIDENCE OF CONTROL IMPLEMENTATION

During control selection and implementation, it is important for organizations to consider the evidence (e.g., artifacts, documentation) that will be needed to support current and future control assessments. Such assessments help determine whether the controls are implemented correctly, operating as intended, and satisfying security and privacy policies—thus, providing essential information for senior leaders to make informed *risk-based* decisions.

CHAPTER THREE

THE CONTROLS

SECURITY AND PRIVACY CONTROLS AND CONTROL ENHANCEMENTS

This catalog of security and privacy controls provides protective measures for systems, organizations, and individuals.[32] The controls are designed to facilitate risk management and compliance with applicable federal laws, executive orders, directives, regulations, policies, and standards. With few exceptions, the security and privacy controls in the catalog are policy-, technology-, and sector-neutral, meaning that the controls focus on the fundamental measures necessary to protect information and the privacy of individuals across the information life cycle. While the security and privacy controls are largely policy-, technology-, and sector-neutral, that does not imply that the controls are policy-, technology-, and sector-unaware. Understanding policies, technologies, and sectors is necessary so that the controls are relevant when they are implemented. Employing a policy-, technology-, and sector-neutral control catalog has many benefits. It encourages organizations to:

- Focus on the security and privacy functions and capabilities required for mission and business success and the protection of information and the privacy of individuals, irrespective of the technologies that are employed in organizational systems;
- Analyze each security and privacy control for its applicability to specific technologies, environments of operation, mission and business functions, and communities of interest; and
- Specify security and privacy policies as part of the tailoring process for controls that have variable parameters.

In the few cases where specific technologies are referenced in controls, organizations are cautioned that the need to manage security and privacy risks may go beyond the requirements in a single control associated with a technology. The additional needed protection measures are obtained from the other controls in the catalog. Federal Information Processing Standards, Special Publications, and Interagency/Internal Reports provide guidance on selecting security and privacy controls that reduce risk for specific technologies and sector-specific applications, including smart grid, cloud, healthcare, mobile, industrial control systems, and Internet of Things (IoT) devices.[33] NIST publications are cited as references as applicable to specific controls in Sections 3.1 through 3.20.

Security and privacy controls in the catalog are expected to change over time as controls are withdrawn, revised, and added. To maintain stability in security and privacy plans, controls are not renumbered each time a control is withdrawn. Rather, notations of the controls that have been withdrawn are maintained in the control catalog for historical purposes. Controls may be withdrawn for a variety of reasons, including when the function or capability provided by the control has been incorporated into another control, the control is redundant to an existing control, or the control is deemed to be no longer necessary or effective.

[32] The controls in this publication are available online and can be obtained in various formats. See [NVD 800-53].

[33] For example, [SP 800-82] provides guidance on risk management and control selection for industrial control systems.

New controls are developed on a regular basis using threat and vulnerability information and information on the tactics, techniques, and procedures used by adversaries. In addition, new controls are developed based on a better understanding of how to mitigate information security risks to systems and organizations and risks to the privacy of individuals arising from information processing. Finally, new controls are developed based on new or changing requirements in laws, executive orders, regulations, policies, standards, or guidelines. Proposed modifications to the controls are carefully analyzed during each revision cycle, considering the need for stability of controls and the need to be responsive to changing technologies, threats, vulnerabilities, types of attack, and processing methods. The objective is to adjust the level of information security and privacy over time to meet the needs of organizations and individuals.

3.1 ACCESS CONTROL

Quick link to Access Control Summary Table

AC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: IA-1, PM-9, PM-24, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [IR 7874].

AC-2 ACCOUNT MANAGEMENT

Control:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [*Assignment: organization-defined prerequisites and criteria*] for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

   3. Access authorizations (i.e., privileges) and [*Assignment: organization-defined attributes (as required)*] for each account;

e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*];

g. Monitor the use of accounts;

h. Notify account managers and [*Assignment: organization-defined personnel or roles*] within:

   1. [*Assignment: organization-defined time period*] when accounts are no longer required;

   2. [*Assignment: organization-defined time period*] when users are terminated or transferred; and

   3. [*Assignment: organization-defined time period*] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

   1. A valid access authorization;

   2. Intended system usage; and

   3. [*Assignment: organization-defined attributes (as required)*];

j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Support the management of system accounts using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Related Controls: None.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

Automatically [*Selection: remove; disable*] temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls: None.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

Disable accounts within [*Assignment: organization-defined time period*] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for [*Assignment: organization-defined time period*].

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls: None.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls: AU-2, AU-6.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Require that users log out when [*Assignment: organization-defined time period of expected inactivity or description of when to log out*].

Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls: AC-11.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT

Implement [*Assignment: organization-defined dynamic privilege management capabilities*].

Discussion: In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime access control decisions facilitated by dynamic privilege management, such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.

Related Controls: AC-16.

(7) ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS

(a) Establish and administer privileged user accounts in accordance with [*Selection: a role-based access scheme; an attribute-based access scheme*];

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

Discussion: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

Related Controls: None.

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT

Create, activate, manage, and deactivate [*Assignment: organization-defined system accounts*] dynamically.

Discussion: Approaches for dynamically creating, activating, managing, and deactivating system accounts rely on automatically provisioning the accounts at runtime for entities that were previously unknown. Organizations plan for the dynamic management, creation, activation, and deactivation of system accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.

Related Controls: AC-16.

(9) ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS

Only permit the use of shared and group accounts that meet [*Assignment: organization-defined conditions for establishing shared and group accounts*].

Discussion: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

Related Controls: None.

(10) ACCOUNT MANAGEMENT | SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE

[Withdrawn: Incorporated into AC-2k.]

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

Enforce [*Assignment: organization-defined circumstances and/or usage conditions*] for [*Assignment: organization-defined system accounts*].

Discussion: Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

Related Controls: None.

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE

(a) Monitor system accounts for [*Assignment: organization-defined atypical usage*]; and

(b) Report atypical usage of system accounts to [*Assignment: organization-defined personnel or roles*].

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical

usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Disable accounts of individuals within [*Assignment: organization-defined time period*] of discovery of [*Assignment: organization-defined significant risks*].

Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related Controls: AU-6, SI-4.

References: [SP 800-162], [SP 800-178], [SP 800-192].

AC-3 ACCESS ENFORCEMENT

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related Controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Control Enhancements:

(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6.]

(2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION

Enforce dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].

Discussion: Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute. To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related Controls: CP-9, MP-6.

(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL

Enforce [*Assignment: organization-defined mandatory access control policy*] over the set of covered subjects and objects specified in the policy, and where the policy:

(a) Is uniformly enforced across the covered subjects and objects within the system;

(b) Specifies that a subject that has been granted access to information is constrained from doing any of the following;

(1) Passing the information to unauthorized subjects or objects;

(2) Granting its privileges to other subjects;

(3) Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components;

(4) Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and

(5) Changing the rules governing access control; and

(c) Specifies that [*Assignment: organization-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges*] such that they are not limited by any defined subset (or all) of the above constraints.

Discussion: Mandatory access control is a type of nondiscretionary access control. Mandatory access control policies constrain what actions subjects can take with information obtained from objects for which they have already been granted access. This prevents the subjects from passing the information to unauthorized subjects and objects. Mandatory access control policies constrain actions that subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the system has control. Otherwise, the access control policy can be circumvented. This enforcement is provided by an implementation that meets the reference monitor concept as described in AC-25. The policy is bounded by the system (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect).

The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges necessary for satisfying organizational mission/business needs relative to the above policy. The control is most applicable when there is a mandate that establishes a policy regarding access to controlled unclassified information or classified information and some users of the system are not authorized access to all such information resident in the system. Mandatory access control can operate in conjunction with discretionary access control as described in AC-3(4). A subject constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of AC-3(4), but mandatory access control policies take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint that prevents a subject from passing information to another subject operating at a different impact or classification level, AC-3(4) permits the subject to pass the information to any other subject with the same impact or classification level as the subject. Examples of mandatory access control policies include the Bell-LaPadula policy to protect confidentiality of information and the Biba policy to protect the integrity of information.

Related Controls: SC-7.

(4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL

Enforce [*Assignment: organization-defined discretionary access control policy*] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:

(a) Pass the information to any other subjects or objects;

(b) Grant its privileges to other subjects;

(c) Change security attributes on subjects, objects, the system, or the system's components;

(d) Choose the security attributes to be associated with newly created or revised objects; or

(e) Change the rules governing access control.

Discussion: When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing the information to other subjects or objects (i.e., subjects have the discretion to pass). Discretionary access control can operate in conjunction with mandatory access control as described in AC-3(3) and AC-3(15). A subject that is constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of discretionary access control. Therefore, while AC-3(3) imposes constraints that prevent a subject from passing information to another subject operating at a different impact or classification level, AC-3(4) permits the subject to pass the information to any subject at the same impact or classification level. The policy is bounded by the system. Once the information is passed outside of system control, additional means may be required to ensure that the constraints remain in effect. While traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this particular use of discretionary access control.

Related Controls: None.

(5) ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION

Prevent access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Discussion: Security-relevant information is information within systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security and privacy policies or maintain the separation of code and data. Security-relevant information includes access control lists, filtering rules for routers or firewalls, configuration parameters for security services, and cryptographic key management information. Secure, non-operable system states include the times in which systems are not performing mission or business-related processing, such as when the system is offline for maintenance, boot-up, troubleshooting, or shut down.

Related Controls: CM-6, SC-39.

(6) ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION

[Withdrawn: Incorporated into MP-4 and SC-28.]

(7) ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL

Enforce a role-based access control policy over defined subjects and objects and control access based upon [*Assignment: organization-defined roles and users authorized to assume such roles*].

Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase

privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: None.

(8) ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS

Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].

Discussion: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process acting on behalf of a user) is removed from a group, access may not be revoked until the next time the object is opened or the next time the subject attempts to access the object. Revocation based on changes to security labels may take effect immediately. Organizations provide alternative approaches on how to make revocations immediate if systems cannot provide such capability and immediate revocation is necessary.

Related Controls: None.

(9) ACCESS ENFORCEMENT | CONTROLLED RELEASE

Release information outside of the system only if:

(a) The receiving [*Assignment: organization-defined system or system component*] provides [*Assignment: organization-defined controls*]; and

(b) [*Assignment: organization-defined controls*] are used to validate the appropriateness of the information designated for release.

Discussion: Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy.

Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.

Related Controls: CA-3, PT-7, PT-8, SA-9, SC-16.

(10) ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS

Employ an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*] by [*Assignment: organization-defined roles*].

Discussion: In certain situations, such as when there is a threat to human life or an event that threatens the organization's ability to carry out critical missions or business functions, an override capability for access control mechanisms may be needed. Override conditions are defined by organizations and used only in those limited circumstances. Audit events are defined in AU-2. Audit records are generated in AU-12.

Related Controls: AU-2, AU-6, AU-10, AU-12, AU-14.

(11) ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES

Restrict access to data repositories containing [*Assignment: organization-defined information types*].

Discussion: Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.

Related Controls: CM-8, CM-12, CM-13, PM-5.

(12) ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS

(a) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [*Assignment: organization-defined system applications and functions*];

(b) Provide an enforcement mechanism to prevent unauthorized access; and

(c) Approve access changes after initial installation of the application.

Discussion: Asserting and enforcing application access is intended to address applications that need to access existing system applications and functions, including user contacts, global positioning systems, cameras, keyboards, microphones, networks, phones, or other files.

Related Controls: CM-7.

(13) ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL

Enforce attribute-based access control policy over defined subjects and objects and control access based upon [*Assignment: organization-defined attributes to assume access permissions*].

Discussion: Attribute-based access control is an access control policy that restricts system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document). Organizations can create rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules. When users are assigned to attributes defined in attribute-based access control policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource. Attribute-based access control can be implemented as either a mandatory or discretionary form of access control. When implemented with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Related Controls: None.

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

Provide [*Assignment: organization-defined mechanisms*] to enable individuals to have access to the following elements of their personally identifiable information: [*Assignment: organization-defined elements*].

Discussion: Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, [PRIVACT] processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the [PRIVACT]) or may require certain levels of authentication assurance. Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

Related Controls: IA-8, PM-22, PM-20, PM-21, PT-6.

(15) ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL

(a) Enforce [*Assignment: organization-defined mandatory access control policy*] over the set of covered subjects and objects specified in the policy; and

(b) Enforce [*Assignment: organization-defined discretionary access control policy*] over the set of covered subjects and objects specified in the policy.

Discussion: Simultaneously implementing a mandatory access control policy and a discretionary access control policy can provide additional protection against the unauthorized execution of code by users or processes acting on behalf of users. This helps prevent a single compromised user or process from compromising the entire system.

Related Controls: SC-2, SC-3, AC-4.

References: [PRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-162], [SP 800-178], [IR 7874].

AC-4 INFORMATION FLOW ENFORCEMENT

Control: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [*Assignment: organization-defined information flow control policies*].

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information

flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

Control Enhancements:

(1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY AND PRIVACY ATTRIBUTES

Use [*Assignment: organization-defined security and privacy attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Discussion: Information flow enforcement mechanisms compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled *Secret* would be allowed to flow to a destination object labeled *Secret*, but an information object labeled *Top Secret* would not be allowed to flow to a destination object labeled *Secret*. A dataset of personally identifiable information may be tagged with restrictions against combining with other types of datasets and, thus, would not be allowed to flow to the restricted dataset. Security and privacy attributes can also include source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security or privacy attributes can be used, for example, to control the release of certain types of information.

Related Controls: None.

(2) INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS

Use protected processing domains to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Discussion: Protected processing domains within systems are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains, information is identified by types, and information flows are controlled based on allowed information accesses (i.e., determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

Related Controls: SC-39.

(3) INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL

Enforce [*Assignment: organization-defined information flow control policies*].

Discussion: Organizational policies regarding dynamic information flow control include allowing or disallowing information flows based on changing conditions or mission or operational considerations. Changing conditions include changes in risk tolerance due to changes in the immediacy of mission or business needs, changes in the threat environment, and detection of potentially harmful or adverse events.

Related Controls: SI-4.

(4) INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION

Prevent encrypted information from bypassing [*Assignment: organization-defined information flow control mechanisms*] by [*Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information;* [*Assignment: organization-defined procedure or method*]].

Discussion: Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

Related Controls: SI-4.

(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES

Enforce [*Assignment: organization-defined limitations*] on embedding data types within other data types.

Discussion: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes inserting files as objects within other files and using compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

Related Controls: None.

(6) INFORMATION FLOW ENFORCEMENT | METADATA

Enforce information flow control based on [*Assignment: organization-defined metadata*].

Discussion: Metadata is information that describes the characteristics of data. Metadata can include structural metadata describing data structures or descriptive metadata describing data content. Enforcement of allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata regarding data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., employing sufficiently strong binding techniques with appropriate assurance).

Related Controls: AC-16, SI-7.

(7) INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS

Enforce one-way information flows through hardware-based flow control mechanisms.

Discussion: One-way flow mechanisms may also be referred to as a unidirectional network, unidirectional security gateway, or data diode. One-way flow mechanisms can be used to prevent data from being exported from a higher impact or classified domain or system while permitting data from a lower impact or unclassified domain or system to be imported.

Related Controls: None.

(8) INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS

(a) Enforce information flow control using [*Assignment: organization-defined security or privacy policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*]; and

(b) [*Selection (one or more): Block; Strip; Modify; Quarantine*] data after a filter processing failure in accordance with [*Assignment: organization-defined security or privacy policy*].

Discussion: Organization-defined security or privacy policy filters can address data structures and content. For example, security or privacy policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security or privacy policy filters for data content can check for specific words, enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data refers to digital information without a data structure or with a data structure that does not facilitate the development of rule sets to address the impact or classification level of the information conveyed by the data or the flow enforcement decisions. Unstructured data consists of bitmap objects that are inherently non-language-based (i.e., image, video, or audio files) and textual objects that are based on written or printed languages. Organizations can implement more than one security or privacy policy filter to meet information flow control objectives.

Related Controls: None.

(9) INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS

Enforce the use of human reviews for [*Assignment: organization-defined information flows*] under the following conditions: [*Assignment: organization-defined conditions*].

Discussion: Organizations define security or privacy policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of or as a complement to automated security or privacy policy filtering. Human reviews may also be employed as deemed necessary by organizations.

Related Controls: None.

(10) INFORMATION FLOW ENFORCEMENT | ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS

Provide the capability for privileged administrators to enable and disable [*Assignment: organization-defined security or privacy policy filters*] under the following conditions: [*Assignment: organization-defined conditions*].

Discussion: For example, as allowed by the system authorization, administrators can enable security or privacy policy filters to accommodate approved data types. Administrators also have the capability to select the filters that are executed on a specific data flow based on the type of data that is being transferred, the source and destination security domains, and other security or privacy relevant features, as needed.

Related Controls: None.

(11) INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS

Provide the capability for privileged administrators to configure [*Assignment: organization-defined security or privacy policy filters*] to support different security or privacy policies.

Discussion: Documentation contains detailed information for configuring security or privacy policy filters. For example, administrators can configure security or privacy policy filters to include the list of inappropriate words that security or privacy policy mechanisms check in accordance with the definitions provided by organizations.

Related Controls: None.

(12) INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS

When transferring information between different security domains, use [*Assignment: organization-defined data type identifiers*] to validate data essential for information flow decisions.

Discussion: Data type identifiers include filenames, file types, file signatures or tokens, and multiple internal file signatures or tokens. Systems only allow transfer of data that is compliant with data type format specifications. Identification and validation of data types is based on defined specifications associated with each allowed data format. The filename and number alone are not used for data type identification. Content is validated syntactically and semantically against its specification to ensure that it is the proper data type.

Related Controls: None.

(13) INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS

When transferring information between different security domains, decompose information into [*Assignment: organization-defined policy-relevant subcomponents*] for submission to policy enforcement mechanisms.

Discussion: Decomposing information into policy-relevant subcomponents prior to information transfer facilitates policy decisions on source, destination, certificates, classification, attachments, and other security- or privacy-related component differentiators. Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains.

Related Controls: None.

(14) INFORMATION FLOW ENFORCEMENT | SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS

When transferring information between different security domains, implement [*Assignment: organization-defined security or privacy policy filters*] requiring fully enumerated formats that restrict data structure and content.

Discussion: Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security or privacy policy filters that restrict data structures include restricting file sizes and field lengths. Data content policy filters include encoding formats for character sets, restricting character data fields to only contain alpha-numeric characters, prohibiting special characters, and validating schema structures.

Related Controls: None.

(15) INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION

When transferring information between different security domains, examine the information for the presence of [*Assignment: organization-defined unsanctioned information*] and prohibit the transfer of such information in accordance with the [*Assignment: organization-defined security or privacy policy*].

Discussion: Unsanctioned information includes malicious code, information that is inappropriate for release from the source network, or executable code that could disrupt or harm the services or systems on the destination network.

Related Controls: SI-3.

(16) INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS

[Withdrawn: Incorporated into AC-4.]

(17) INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION

Uniquely identify and authenticate source and destination points by [*Selection (one or more): organization; system; application; service; individual*] for information transfer.

Discussion: Attribution is a critical component of a security and privacy concept of operations. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals. Successful domain authentication requires that system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Attribution also allows organizations to better maintain the lineage of personally identifiable information processing as it flows through systems and can facilitate consent tracking, as well as correction, deletion, or access requests from individuals.

Related Controls: IA-2, IA-3, IA-9.

(18) INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING

[Withdrawn: Incorporated into AC-16.]

(19) INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA

When transferring information between different security domains, implement [*Assignment: organization-defined security or privacy policy filters*] on metadata.

Discussion: All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions and consider metadata and the data to which the metadata applies to be part of the payload.

Related Controls: None.

(20) INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS

Employ [*Assignment: organization-defined solutions in approved configurations*] to control the flow of [*Assignment: organization-defined information*] across security domains.

Discussion: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The National Security Agency (NSA) National Cross Domain Strategy and Management Office provides a listing of approved cross-domain solutions. Contact ncdsmo@nsa.gov for more information.

Related Controls: None.

(21) INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS

Separate information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Discussion: Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

Related Controls: SC-32.

(22) INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.

Discussion: The system provides a capability for users to access each connected security domain without providing any mechanisms to allow users to transfer data or information between the different security domains. An example of an access-only solution is a terminal that provides a user access to information with different security classifications while assuredly keeping the information separate.

Related Controls: None.

(23) INFORMATION FLOW ENFORCEMENT | MODIFY NON-RELEASABLE INFORMATION

When transferring information between different security domains, modify non-releasable information by implementing [*Assignment: organization-defined modification action*].

Discussion: Modifying non-releasable information can help prevent a data spill or attack when information is transferred across security domains. Modification actions include masking, permutation, alteration, removal, or redaction.

Related Controls: None.

(24) INFORMATION FLOW ENFORCEMENT | INTERNAL NORMALIZED FORMAT

When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

Discussion: Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.

Related Controls: None.

(25) INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION

When transferring information between different security domains, sanitize data to minimize [*Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information*] in accordance with [*Assignment: organization-defined policy*]].

Discussion: Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, and DVDs) or in hard copy form.

Related Controls: MP-6.

(26) INFORMATION FLOW ENFORCEMENT | AUDIT FILTERING ACTIONS

When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied. Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified and/or why it failed the filtering process. Audit events are defined in AU-2. Audit records are generated in AU-12.

Related Controls: AU-2, AU-3, AU-12.

(27) INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS

When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Redundant

and independent content filtering eliminates a single point of failure filtering system. Independence is defined as the implementation of a content filter that uses a different code base and supporting libraries (e.g., two JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

Related Controls: None.

(28) INFORMATION FLOW ENFORCEMENT | LINEAR FILTER PIPELINES

When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. The use of linear content filter pipelines ensures that filter processes are non-bypassable and always invoked. In general, the use of parallel filtering architectures for content filtering of a single data type introduces bypass and non-invocation issues.

Related Controls: None.

(29) INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES

When transferring information between different security domains, employ content filter orchestration engines to ensure that:

(a) Content filtering mechanisms successfully complete execution without errors; and

(b) Content filtering actions occur in the correct order and comply with [*Assignment: organization-defined policy*].

Discussion: Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined security policy. An orchestration engine coordinates the sequencing of activities (manual and automated) in a content filtering process. Errors are defined as either anomalous actions or unexpected termination of the content filter process. This is not the same as a filter failing content due to non-compliance with policy. Content filter reports are a commonly used mechanism to ensure that expected filtering actions are completed successfully.

Related Controls: None.

(30) INFORMATION FLOW ENFORCEMENT | FILTER MECHANISMS USING MULTIPLE PROCESSES

When transferring information between different security domains, implement content filtering mechanisms using multiple processes.

Discussion: The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.

Related Controls: None.

(31) INFORMATION FLOW ENFORCEMENT | FAILED CONTENT TRANSFER PREVENTION

When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.

Discussion: Content that failed filtering checks can corrupt the system if transferred to the receiving domain.

Related Controls: None.

(32) INFORMATION FLOW ENFORCEMENT | PROCESS REQUIREMENTS FOR INFORMATION TRANSFER

When transferring information between different security domains, the process that transfers information between filter pipelines:

(a) Does not filter message content;

(b) Validates filtering metadata;

(c) Ensures the content associated with the filtering metadata has successfully completed filtering; and

(d) Transfers the content to the destination filter pipeline.

Discussion: The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.

Related Controls: None.

References: [SP-800-160-1], [SP 800-162], [SP 800-178], [IR 8112].

AC-5 SEPARATION OF DUTIES

Control:

a. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and

b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

Control Enhancements: None.

References: None.

AC-6 LEAST PRIVILEGE

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Authorize access for [*Assignment: organization-defined individuals or roles*] to:

(a) [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware)*]; and

(b) [*Assignment: organization-defined security-relevant information*].

Discussion: Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Require that users of system accounts (or roles) with access to [*Assignment: organization-defined security functions or security-relevant information*] use non-privileged accounts or roles, when accessing nonsecurity functions.

Discussion: Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related Controls: AC-17, AC-18, AC-19, PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

Authorize network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and document the rationale for such access in the security plan for the system.

Discussion: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Related Controls: AC-17, AC-18, AC-19.

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

Provide separate processing domains to enable finer-grained allocation of user privileges.

Discussion: Providing separate processing domains for finer-grained allocation of user privileges includes using virtualization techniques to permit additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying physical machine, implementing separate physical domains, and employing hardware or software domain separation mechanisms.

Related Controls: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*].

Discussion: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls: IA-2, MA-3, MA-4.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

Prohibit privileged access to the system by non-organizational users.

Discussion: An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

Related Controls: AC-18, AC-19, IA-2, IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

(a) Review [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls: CA-7.

(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

Prevent the following software from executing at higher privilege levels than users executing the software: [*Assignment: organization-defined software*].

Discussion: In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

Related Controls: None.

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

Log the execution of privileged functions.

Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls: AU-2, AU-3, AU-12.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and

prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Related Controls: None.

References: None.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection (one or more): lock the account or node for an* [*Assignment: organization-defined time period*]; *lock the account or node until released by an administrator; delay next logon prompt per* [*Assignment: organization-defined delay algorithm*]; *notify system administrator; take other* [*Assignment: organization-defined action*]] when the maximum number of unsuccessful attempts is exceeded.

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.

Control Enhancements:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK

[Withdrawn: Incorporated into AC-7.]

(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE OR WIPE MOBILE DEVICE

Purge or wipe information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging or wiping requirements and techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.

Discussion: A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile

device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Related Controls: AC-19, MP-5, MP-6.

(3) UNSUCCESSFUL LOGON ATTEMPTS | BIOMETRIC ATTEMPT LIMITING

Limit the number of unsuccessful biometric logon attempts to [*Assignment: organization-defined number*].

Discussion: Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts for users based on organizationally-defined factors.

Related Controls: IA-3.

(4) UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR

(a) Allow the use of [*Assignment: organization-defined authentication factors*] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; and

(b) Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts through use of the alternative factors by a user during a [*Assignment: organization-defined time period*].

Discussion: The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related Controls: IA-3.

References: [SP 800-63-3], [SP 800-124].

AC-8 SYSTEM USE NOTIFICATION

Control:

a. Display [*Assignment: organization-defined system use notification message or banner*] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

   1. Users are accessing a U.S. Government system;
   2. System usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
   4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

   1. Display system use information [*Assignment: organization-defined conditions*], before granting further access to the publicly accessible system;
   2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls: AC-14, PL-4, SI-4.

Control Enhancements: None.

References: None.

AC-9 PREVIOUS LOGON NOTIFICATION

Control: Notify the user, upon successful logon to the system, of the date and time of the last logon.

Discussion: Previous logon notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user's last access.

Related Controls: AC-7, PL-4.

Control Enhancements:

(1) PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS

Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

Discussion: Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts.

Related Controls: None.

(2) PREVIOUS LOGON NOTIFICATION | SUCCESSFUL AND UNSUCCESSFUL LOGONS

Notify the user, upon successful logon, of the number of [*Selection: successful logons; unsuccessful logon attempts; both*] during [*Assignment: organization-defined time period*].

Discussion: Information about the number of successful and unsuccessful logon attempts within a specified time period allows the user to recognize if the number and type of logon attempts are consistent with the user's actual logon attempts.

Related Controls: None.

(3) PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES

Notify the user, upon successful logon, of changes to [*Assignment: organization-defined security-related characteristics or parameters of the user's account*] during [*Assignment: organization-defined time period*].

Discussion: Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.

Related Controls: None.

(4) PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION

Notify the user, upon successful logon, of the following additional information: [*Assignment: organization-defined additional information*].

Discussion: Organizations can specify additional information to be provided to users upon logon, including the location of the last logon. User location is defined as information that can be determined by systems, such as Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

Related Controls: None.

References: None.

AC-10 CONCURRENT SESSION CONTROL

Control: Limit the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

Discussion: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Related Controls: SC-23.

Control Enhancements: None.

References: None.

AC-11 DEVICE LOCK

Control:

a. Prevent further access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls: AC-2, AC-7, IA-11, PL-4.

Control Enhancements:

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls: None.

References: None.

AC-12 SESSION TERMINATION

Control: Automatically terminate a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls: MA-4, SC-10, SC-23.

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*].

Discussion: Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Related Controls: None.

(2) SESSION TERMINATION | TERMINATION MESSAGE

Display an explicit logout message to users indicating the termination of authenticated communications sessions.

Discussion: Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Related Controls: None.

(3) SESSION TERMINATION | TIMEOUT WARNING MESSAGE

Display an explicit message to users indicating that the session will end in [*Assignment: organization-defined time until end of session*].

Discussion: To increase usability, notify users of pending session termination and prompt users to continue the session. The pending session termination time period is based on the parameters defined in the AC-12 base control.

Related Controls: None.

References: None.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6.]

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control:

a. Identify [*Assignment: organization-defined user actions*] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

Related Controls: AC-8, IA-2, PL-2.

Control Enhancements: None.

(1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES

[Withdrawn: Incorporated into AC-14.]

References: None.

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3.]

AC-16 SECURITY AND PRIVACY ATTRIBUTES

Control:

a. Provide the means to associate [*Assignment: organization-defined types of security and privacy attributes*] with [*Assignment: organization-defined security and privacy attribute values*] for information in storage, in process, and/or in transmission;

b. Ensure that the attribute associations are made and retained with the information;

c. Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [*Assignment: organization-defined systems*]: [*Assignment: organization-defined security and privacy attributes*];

d. Determine the following permitted attribute values or ranges for each of the established attributes: [*Assignment: organization-defined attribute values or ranges for established attributes*];

e. Audit changes to attributes; and

f. Review [*Assignment: organization-defined security and privacy attributes*] for applicability [*Assignment: organization-defined frequency*].

Discussion: Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as *subjects*, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as *objects*, are typically associated with data structures, such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions that represent the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently or in conjunction with security attributes, represent the basic properties or characteristics of active or passive entities with respect to the management of personally identifiable information. Attributes can be either explicitly or implicitly associated with the information contained in organizational systems or system components.

Attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, cause information to flow among objects, or change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of attributes to subjects and objects by a system is referred to as binding and is inclusive of setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects. Such enforcement occurs through organizational processes or system functions or mechanisms. The binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play important parts in the trust that organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for systems to support missions or business functions. There are many values that can be assigned to a security attribute. By specifying the permitted attribute ranges and values, organizations ensure that attribute values are meaningful and relevant. Labeling refers to the association of attributes with the subjects and objects represented by the internal data structures within systems. This facilitates system-based enforcement of information security and privacy policies. Labels include classification of information in accordance with legal and compliance requirements (e.g., top secret, secret, confidential, controlled unclassified), information impact level; high value asset information, access authorizations, nationality; data life cycle protection (i.e., encryption and data expiration), personally identifiable information processing permissions, including individual consent to personally identifiable information processing, and contractor affiliation. A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form and displayed on system media. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. Security and privacy labels may have the same value as media markings (e.g., top secret, secret, confidential). See MP-3 (Media Marking).

Related Controls: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18.

Control Enhancements:

(1) SECURITY AND PRIVACY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION

Dynamically associate security and privacy attributes with [*Assignment: organization-defined subjects and objects*] in accordance with the following security and privacy policies as information is created and combined: [*Assignment: organization-defined security and privacy policies*].

Discussion: Dynamic association of attributes is appropriate whenever the security or privacy characteristics of information change over time. Attributes may change due to information aggregation issues (i.e., characteristics of individual data elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), changes in the security category of information, or changes in security or privacy policies. Attributes may also change situationally.

Related Controls: None.

(2) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS

Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.

Discussion: The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.

Related Controls: None.

(3) SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM

Maintain the association and integrity of [*Assignment: organization-defined security and privacy attributes*] to [*Assignment: organization-defined subjects and objects*].

Discussion: Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. The integrity of specific items, such as security configuration files, may be maintained through the use of an integrity monitoring mechanism that detects anomalies and changes that deviate from "known good" baselines. Automated policy actions include retention date expirations, access control decisions, information flow control decisions, and information disclosure decisions.

Related Controls: None.

(4) SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS

Provide the capability to associate [*Assignment: organization-defined security and privacy attributes*] with [*Assignment: organization-defined subjects and objects*] by authorized individuals (or processes acting on behalf of individuals).

Discussion: Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports). Some systems provide additional capability for general users to assign security and privacy attributes to additional objects (e.g., files, emails). The association of attributes by authorized individuals is described in the design documentation. The support provided by systems can include prompting users to select security and privacy attributes to be associated with information objects, employing automated mechanisms to categorize information with attributes based on defined policies, or ensuring that the combination of the security or privacy attributes selected is valid. Organizations consider the creation, deletion, or modification of attributes when defining auditable events.

Related Controls: None.

(5) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT

Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [*Assignment: organization-defined special dissemination, handling, or distribution instructions*] using [*Assignment: organization-defined human-readable, standard naming conventions*].

Discussion: System outputs include printed pages, screens, or equivalent items. System output devices include printers, notebook computers, video displays, smart phones, and tablets. To mitigate the risk of unauthorized exposure of information (e.g., shoulder surfing), the outputs display full attribute values when unmasked by the subscriber.

Related Controls: None.

(6) SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION

Require personnel to associate and maintain the association of [*Assignment: organization-defined security and privacy attributes*] with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security and privacy policies*].

Discussion: Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined security and privacy attributes with subjects and objects.

Related Controls: None.

(7) SECURITY AND PRIVACY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION

Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.

Discussion: To enforce security and privacy policies across multiple system components in distributed systems, organizations provide a consistent interpretation of security and privacy attributes employed in access enforcement and flow enforcement decisions. Organizations can establish agreements and processes to help ensure that distributed system components implement attributes with consistent interpretations in automated access enforcement and flow enforcement actions.

Related Controls: None.

(8) SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION TECHNIQUES AND TECHNOLOGIES

Implement [*Assignment: organization-defined techniques and technologies*] in associating security and privacy attributes to information.

Discussion: The association of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes to information (i.e., binding) can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

Related Controls: SC-12, SC-13.

(9) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE REASSIGNMENT — REGRADING MECHANISMS

Change security and privacy attributes associated with information only via regrading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].

Discussion: A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception. Validated regrading mechanisms are

used by organizations to provide the requisite levels of assurance for attribute reassignment activities. The validation is facilitated by ensuring that regrading mechanisms are single purpose and of limited function. Since security and privacy attribute changes can directly affect policy enforcement actions, implementing trustworthy regrading mechanisms is necessary to help ensure that such mechanisms perform in a consistent and correct mode of operation.

Related Controls: None.

(10) SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS

Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.

Discussion: The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Thus, it is important for systems to be able to limit the ability to create or modify the type and value of attributes available for association with subjects and objects to authorized individuals only.

Related Controls: None.

References: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-162], [SP 800-178].

AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers,

notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-2, AU-6, AU-12, AU-14.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls: SC-8, SC-12, SC-13.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Route remote accesses through authorized and managed network access control points.

Discussion: Organizations consider the Trusted Internet Connections (TIC) initiative [DHS TIC] requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Related Controls: SC-7.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [*Assignment: organization-defined needs*]; and

(b) Document the rationale for remote access in the security plan for the system.

Discussion: Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls: AC-6, SC-12, SC-13.

(5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4.]

(6) REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION

Protect information about remote access mechanisms from unauthorized use and disclosure.

Discussion: Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior (see PL-4) and access agreements (see PS-6).

Related Controls: AT-2, AT-3, PS-6.

(7) REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS

[Withdrawn: Incorporated into AC-3(10).]

(8) REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS

[Withdrawn: Incorporated into CM-7.]

(9) REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS

Provide the capability to disconnect or disable remote access to the system within [*Assignment: organization-defined time period*].

Discussion: The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Related Controls: None.

(10) REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS

Implement [*Assignment: organization-defined mechanisms*] to authenticate [*Assignment: organization-defined remote commands*].

Discussion: Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Related Controls: SC-12, SC-13, SC-23.

References: [SP 800-46], [SP 800-77], [SP 800-113], [SP 800-114], [SP 800-121], [IR 7966].

AC-18 WIRELESS ACCESS

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

Discussion: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Protect wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, SC-13.

(2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS

[Withdrawn: Incorporated into SI-4.]

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

(4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Discussion: Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Related Controls: SC-7, SC-15.

(5) WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Discussion: Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related Controls: PE-19.

References: [SP 800-94], [SP 800-97].

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control:

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Control Enhancements:

(1) ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE AND PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(2) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(3) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER

[Withdrawn: Incorporated into MP-7.]

(4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION

(a) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

(b) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information:

(1) Connection of unclassified mobile devices to classified systems is prohibited;

(2) Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;

(3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and

(4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.

(c) Restrict the connection of classified mobile devices to classified systems in accordance with [*Assignment: organization-defined security policies*].

Discussion: None.

Related Controls: CM-8, IR-4.

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

Employ [*Selection: full-device encryption; container-based encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].

Discussion: Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls: SC-12, SC-13, SC-28.

References: [SP 800-114], [SP 800-124].

AC-20 USE OF EXTERNAL SYSTEMS

Control:

a. [*Selection (one or more): Establish* [*Assignment: organization-defined terms and conditions*]*; Identify* [*Assignment: organization-defined controls asserted to be implemented on external systems*]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   1. Access the system from external systems; and

   2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [*Assignment: organizationally-defined types of external systems*].

Discussion: External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational

systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Control Enhancements:

(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls: CA-2.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [*Assignment: organization-defined restrictions*].

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls: MP-7, SC-41.

(3) USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE

Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [*Assignment: organization-defined restrictions*].

Discussion: Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20 b.). In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. Organizations consult with the Office of the General Counsel regarding legal issues associated with using personally owned devices, including requirements for conducting forensic analyses during investigations after an incident.

Related Controls: None.

(4) USE OF EXTERNAL SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE

Prohibit the use of [*Assignment: organization-defined network accessible storage devices*] in external systems.

Discussion: Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Related Controls: None.

(5) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — PROHIBITED USE

Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Related Controls: MP-7, PL-4, PS-6, SC-41.

References: [FIPS 199], [SP 800-171], [SP 800-172].

AC-21 INFORMATION SHARING

Control:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employ [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing and collaboration decisions.

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Control Enhancements:

(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT

Employ [*Assignment: organization-defined automated mechanisms]* to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Discussion: Automated mechanisms are used to enforce information sharing decisions.

Related Controls: None.

(2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL

Implement information search and retrieval services that enforce [*Assignment: organization-defined information sharing restrictions*].

Discussion: Information search and retrieval services identify information system resources relevant to an information need.

Related Controls: None.

References: [OMB A-130], [SP 800-150], [IR 8062].

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [*Assignment: organization-defined frequency*] and remove such information, if discovered.

Discussion: In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the [PRIVACT] and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related Controls: AC-3, AT-2, AT-3, AU-13.

Control Enhancements: None.

References: [PRIVACT].

AC-23 DATA MINING PROTECTION

Control: Employ [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to detect and protect against unauthorized data mining.

Discussion: Data mining is an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. Data storage objects include database records and database fields. Sensitive information can be extracted from data mining operations. When information is personally identifiable information, it may lead to unanticipated revelations about individuals and give rise to privacy risks. Prior to performing data mining activities, organizations determine whether such activities are authorized. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that address data mining requirements. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores

and is available as open-source information residing on external sites, such as social networking or social media websites.

[EO 13587] requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of sensitive information from exploitation, compromise, or other unauthorized disclosure. Data mining protection requires organizations to identify appropriate techniques to prevent and detect unnecessary or unauthorized data mining. Data mining can be used by an insider to collect organizational information for the purpose of exfiltration.

Related Controls: PM-12, PT-2.

Control Enhancements: None.

References: [EO 13587].

AC-24 ACCESS CONTROL DECISIONS

Control: [*Selection: Establish procedures; Implement mechanisms*] to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

Discussion: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions. While it is common to have access control decisions and access enforcement implemented by the same entity, it is not required, and it is not always an optimal implementation choice. For some architectures and distributed systems, different entities may make access control decisions and enforce access.

Related Controls: AC-2, AC-3.

Control Enhancements:

(1) ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION

Transmit [*Assignment: organization-defined access authorization information*] using [*Assignment: organization-defined controls*] to [*Assignment: organization-defined systems*] that enforce access control decisions.

Discussion: Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information supporting security and privacy attributes. This is because in distributed systems, there are various access control decisions that need to be made, and different entities make these decisions in a serial fashion, each requiring those attributes to make the decisions. Protecting access authorization information ensures that such information cannot be altered, spoofed, or compromised during transmission.

Related Controls: AU-10.

(2) ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY

Enforce access control decisions based on [*Assignment: organization-defined security or privacy attributes*] that do not include the identity of the user or process acting on behalf of the user.

Discussion: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other

situations, user identification information is simply not needed for access control decisions, and especially in the case of distributed systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish. MAC, RBAC, ABAC, and label-based control policies, for example, might not include user identity as an attribute.

Related Controls: None.

References: [SP 800-162], [SP 800-178].

AC-25 REFERENCE MONITOR

Control: Implement a reference monitor for [*Assignment: organization-defined access control policies*] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Discussion: A reference monitor is a set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked, tamper-proof, and small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable). Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are associated with data structures, such as records, buffers, communications ports, tables, files, and inter-process pipes. Reference monitors enforce access control policies that restrict access to objects based on the identity of subjects or groups to which the subjects belong. The system enforces the access control policy based on the rule set established by the policy. The tamper-proof property of the reference monitor prevents determined adversaries from compromising the functioning of the reference validation mechanism. The always invoked property prevents adversaries from bypassing the mechanism and violating the security policy. The smallness property helps to ensure completeness in the analysis and testing of the mechanism to detect any weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

Related Controls: AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.

Control Enhancements: None.

References: None.

3.2 AWARENESS AND TRAINING

Quick link to Awareness and Training Summary Table

AT-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] awareness and training policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-100].

AT-2 LITERACY TRAINING AND AWARENESS

Control:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

   1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and

   2. When required by system changes or following [*Assignment: organization-defined events*];

b. Employ the following techniques to increase the security and privacy awareness of system users [*Assignment: organization-defined awareness techniques*];

c. Update literacy training and awareness content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

Control Enhancements:

(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related Controls: CA-2, CA-7, CP-4, IR-3.

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

Related Controls: PM-12.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Related Controls: None.

(4) LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [*Assignment: organization-defined indicators of malicious code*].

Discussion: A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Related Controls: None.

(5) LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT

Provide literacy training on the advanced persistent threat.

Discussion: An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social

engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

Related Controls: None.

(6) LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT

(a) Provide literacy training on the cyber threat environment; and

(b) Reflect current cyber threat information in system operations.

Discussion: Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Related Controls: RA-3.

References: [OMB A-130], [SP 800-50], [SP 800-160-2], [SP 800-181], [ODNI CTF].

AT-3 ROLE-BASED TRAINING

Control:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [*Assignment: organization-defined roles and responsibilities*]:

   1. Before authorizing access to the system, information, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and

   2. When required by system changes;

b. Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based

training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

Control Enhancements:

(1) ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Discussion: Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Related Controls: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Discussion: Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Related Controls: PE-2, PE-3, PE-4.

(3) ROLE-BASED TRAINING | PRACTICAL EXERCISES

Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion: Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Related Controls: None.

(4) ROLE-BASED TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

[Withdrawn: Moved to AT-2(4)].

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and

notices, privacy impact assessments, [PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Related Controls: PT-2, PT-3, PT-5, PT-6.

References: [OMB A-130], [SP 800-50], [SP 800-181].

AT-4 TRAINING RECORDS

Control:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [*Assignment: organization-defined time period*].

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

Related Controls: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Control Enhancements: None.

References: [OMB A-130].

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15.]

AT-6 TRAINING FEEDBACK

Control: Provide feedback on organizational training results to the following personnel [*Assignment: organization-defined frequency*]: [*Assignment: organization-defined personnel*].

Discussion: Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the evaluation and update of organizational training described in AT-2b and AT-3b.

Related Controls: None.

Control Enhancements: None.

References: None.

3.3 AUDIT AND ACCOUNTABILITY

Quick link to Audit and Accountability Summary Table

AU-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] audit and accountability policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

AU-2 EVENT LOGGING

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: [*Assignment: organization-defined event types that the system is capable of logging*];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [*Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type*];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Control Enhancements:

(1) EVENT LOGGING | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12.]

(2) EVENT LOGGING | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12.]

(3) EVENT LOGGING | REVIEWS AND UPDATES

[Withdrawn: Incorporated into AU-2.]

(4) EVENT LOGGING | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6(9).]

References: [OMB A-130], [SP 800-92].

AU-3 CONTENT OF AUDIT RECORDS

Control: Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Generate audit records containing the following additional information: [*Assignment: organization-defined additional information*].

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related Controls: None.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

[Withdrawn: Incorporated into PL-9.]

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*Assignment: organization-defined elements*].

Discussion: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3.

References: [OMB A-130], [IR 8062].

AU-4 AUDIT LOG STORAGE CAPACITY

Control: Allocate audit log storage capacity to accommodate [*Assignment: organization-defined audit log retention requirements*].

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Transfer audit logs [*Assignment: organization-defined frequency*] to a different system, system component, or media other than the system or system component conducting the logging.

Discussion: Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Related Controls: None.

References: None.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control:

a. Alert [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] in the event of an audit logging process failure; and

b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping

the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Control Enhancements:

(1) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | STORAGE CAPACITY WARNING

Provide a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit log storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit log storage capacity.

Discussion: Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Related Controls: None.

(2) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS

Provide an alert within [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit logging failure events requiring real-time alerts*].

Discussion: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Related Controls: None.

(3) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [*Selection: reject; delay*] network traffic above those thresholds.

Discussion: Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Related Controls: None.

(4) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE

Invoke a [*Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available*] in the event of [*Assignment: organization-defined audit logging failures*], unless an alternate audit logging capability exists.

Discussion: Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system

supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Related Controls: AU-15.

(5) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | ALTERNATE AUDIT LOGGING CAPABILITY

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [*Assignment: organization-defined alternate audit logging functionality*].

Discussion: Since an alternate audit logging capability may be a short-term protection solution employed until the failure in the primary audit logging capability is corrected, organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Related Controls: AU-9.

References: None.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control:

a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [*Assignment: organization-defined personnel or roles*]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion: Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

Integrate audit record review, analysis, and reporting processes using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

Related Controls: PM-7.

(2) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS

[Withdrawn: Incorporated into SI-4.]

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls: AU-12, IR-4.

(4) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Discussion: Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

Related Controls: AU-2, AU-12.

(5) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS

Integrate analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

Discussion: Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related Controls: AU-12, IR-4.

(6) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Discussion: The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Related Controls: None.

(7) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS

Specify the permitted actions for each [*Selection (one or more): system process; role; user*] associated with the review, analysis, and reporting of audit record information.

Discussion: Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Related Controls: None.

(8) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Discussion: Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Related Controls: AU-3, AU-9, AU-11, AU-12.

(9) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls: PM-12.

(10) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

[Withdrawn: Incorporated into AU-6.]

References: [SP 800-86], [SP 800-101].

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

Control: Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Discussion: Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record

reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Related Controls: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.

Control Enhancements:

(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Assignment: organization-defined fields within audit records*].

Discussion: Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

Related Controls: None.

(2) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH

[Withdrawn: Incorporated into AU-7(1).]

References: None.

AU-8 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity of time measurement*] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12, AU-14, SC-45.

Control Enhancements:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

[Withdrawn: Moved to SC-45(1).]

(2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE

[Withdrawn: Moved to SC-45(2).]

References: None.

AU-9 PROTECTION OF AUDIT INFORMATION

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [*Assignment: organization-defined personnel or roles*] upon detection of unauthorized access, modification, or deletion of audit information.

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

Write audit trails to hardware-enforced, write-once media.

Discussion: Writing audit trails to hardware-enforced, write-once media applies to the initial generation of audit trails (i.e., the collection of audit records that represents the information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. Writing audit trails to hardware-enforced, write-once media does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes Compact Disc-Recordable (CD-R), Blu-Ray Disc Recordable (BD-R), and Digital Versatile Disc-Recordable (DVD-R). In contrast, the use of switchable write-protection media, such as tape cartridges, Universal Serial Bus (USB) drives, Compact Disc Re-Writeable (CD-RW), and Digital Versatile Disc-Read Write (DVD-RW) results in write-protected but not write-once media.

Related Controls: AU-4, AU-5.

(2) PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

Store audit records [*Assignment: organization-defined frequency*] in a repository that is part of a physically different system or system component than the system or component being audited.

Discussion: Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related Controls: AU-4, AU-5.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Discussion: Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related Controls: AU-10, SC-12, SC-13.

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Authorize access to management of audit logging functionality to only [*Assignment: organization-defined subset of privileged users or roles*].

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls: AC-5.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

Enforce dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].

Discussion: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of two authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related Controls: AC-3.

(6) PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS

Authorize read-only access to audit information to [*Assignment: organization-defined subset of privileged users or roles*].

Discussion: Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.

Related Controls: None.

(7) PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM

Store audit information on a component running a different operating system than the system or component being audited.

Discussion: Storing auditing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system, resulting in a compromise of the audit records.

Related controls: AU-4, AU-5, AU-11, SC-29.

References: [FIPS 140-3], [FIPS 180-4], [FIPS 202].

AU-10 NON-REPUDIATION

Control: Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [*Assignment: organization-defined actions to be covered by non-repudiation*].

Discussion: Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

Related Controls: AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Control Enhancements:

(1) NON-REPUDIATION | ASSOCIATION OF IDENTITIES

(a) Bind the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and

(b) Provide the means for authorized individuals to determine the identity of the producer of the information.

Discussion: Binding identities to the information supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of attribute binding between the information producer and the information based on the security category of the information and other relevant risk factors.

Related Controls: AC-4, AC-16.

(2) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY

(a) Validate the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and

(b) Perform [*Assignment: organization-defined actions*] in the event of a validation error.

Discussion: Validating the binding of the information producer identity to the information prevents the modification of information between production and review. The validation of bindings can be achieved by, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls: AC-3, AC-4, AC-16.

(3) NON-REPUDIATION | CHAIN OF CUSTODY

Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.

Discussion: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release or transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, maintaining the credentials of reviewers or releasers provides

the organization with the means to identify who reviewed and released the information. In the case of automated reviews, it ensures that only approved review functions are used.

Related Controls: AC-4, AC-16.

(4) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY

(a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [*Assignment: organization-defined security domains*]; and

(b) Perform [*Assignment: organization-defined actions*] in the event of a validation error.

Discussion: Validating the binding of the information reviewer identity to the information at transfer or release points prevents the unauthorized modification of information between review and the transfer or release. The validation of bindings can be achieved by using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls: AC-4, AC-16.

(5) NON-REPUDIATION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SI-7.]

References: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-177].

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Control Enhancements:

(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

Employ [*Assignment: organization-defined measures*] to ensure that long-term audit records generated by the system can be retrieved.

Discussion: Organizations need to access and read audit records requiring long-term storage (on the order of years). Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

Related Controls: None.

References: [OMB A-130].

AU-12 AUDIT RECORD GENERATION

Control:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [*Assignment: organization-defined system components*];

b. Allow [*Assignment: organization-defined personnel or roles*] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion: Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

Control Enhancements:

(1) AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from [*Assignment: organization-defined system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail*].

Discussion: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related Controls: AU-8, SC-45.

(2) AUDIT RECORD GENERATION | STANDARDIZED FORMATS

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Discussion: Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Related Controls: None.

(3) AUDIT RECORD GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Provide and implement the capability for [*Assignment: organization-defined individuals or roles*] to change the logging to be performed on [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].

Discussion: Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Related Controls: AC-3.

(4) AUDIT RECORD GENERATION | QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION

Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.

Discussion: Query parameters are explicit criteria that an individual or automated system submits to a system to retrieve data. Auditing of query parameters for datasets that contain personally identifiable information augments the capability of an organization to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.

Related Controls: None.

References: None.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control:

a. Monitor [*Assignment: organization-defined open-source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information; and

b. If an information disclosure is discovered:

   1. Notify [*Assignment: organization-defined personnel or roles*]; and

   2. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Related Controls: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Control Enhancements:

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

Monitor open-source information and information sites using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

Related Controls: None.

(2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES

Review the list of open-source information sites being monitored [*Assignment: organization-defined frequency*].

Discussion: Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Related Controls: None.

(3) MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED REPLICATION OF INFORMATION

Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

Discussion: The unauthorized use or replication of organizational information by external entities can cause adverse impacts on organizational operations and assets, including damage to reputation. Such activity can include the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-hosting organization. Discovery tools, techniques, and processes used to determine if external entities are replicating organizational information in an unauthorized manner include scanning external websites, monitoring social media, and training staff to recognize the unauthorized use of organizational information.

Related Controls: None.

References: None.

AU-14 SESSION AUDIT

Control:

a. Provide and implement the capability for [*Assignment: organization-defined users or roles*] to [*Selection (one or more): record; view; hear; log*] the content of a user session under [*Assignment: organization-defined circumstances*]; and

b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the organization is suspicious of a specific individual). Organizations consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of personally identifiable information, are appropriately addressed.

Related Controls: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Control Enhancements:

(1) SESSION AUDIT | SYSTEM START-UP

Initiate session audits automatically at system start-up.

Discussion: The automatic initiation of session audits at startup helps to ensure that the information being captured on selected individuals is complete and not subject to compromise through tampering by malicious threat actors.

Related Controls: None.

(2) SESSION AUDIT | CAPTURE AND RECORD CONTENT

[Withdrawn: Incorporated into AU-14.]

(3) SESSION AUDIT | REMOTE VIEWING AND LISTENING

Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

Discussion: None.

Related Controls: AC-17.

References: None.

AU-15 ALTERNATE AUDIT LOGGING CAPABILITY

[Withdrawn: Moved to AU-5(5).]

AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING

Control: Employ [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

Discussion: When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational audit logging simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.

Related Controls: AU-3, AU-6, AU-7, CA-3, PT-7.

Control Enhancements:

(1) CROSS-ORGANIZATIONAL AUDIT LOGGING | IDENTITY PRESERVATION

Preserve the identity of individuals in cross-organizational audit trails.

Discussion: Identity preservation is applied when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Related Controls: IA-2, IA-4, IA-5, IA-8.

(2) CROSS-ORGANIZATIONAL AUDIT LOGGING | SHARING OF AUDIT INFORMATION

Provide cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].

Discussion: Due to the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only individuals' home organizations have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Related Controls: IR-4, SI-4.

(3) CROSS-ORGANIZATIONAL AUDITING | DISASSOCIABILITY

Implement [*Assignment: organization-defined measures*] to disassociate individuals from audit information transmitted across organizational boundaries.

Discussion: Preserving identities in audit trails could have privacy ramifications, such as enabling the tracking and profiling of individuals, but may not be operationally necessary. These risks could be further amplified when transmitting information across organizational boundaries. Implementing privacy-enhancing cryptographic techniques can disassociate individuals from audit information and reduce privacy risk while maintaining accountability.

Related Controls: None.

References: None.

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

Quick link to Assessment, Authorization, and Monitoring Summary Table

CA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] assessment, authorization, and monitoring policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-100], [SP 800-137], [SP 800-137A], [IR 8062].

CA-2 CONTROL ASSESSMENTS

Control:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

   1. Controls and control enhancements under assessment;

   2. Assessment procedures to be used to determine control effectiveness; and

   3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to [*Assignment: organization-defined individuals or roles*].

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system

life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Related Controls: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

Control Enhancements:

(1) CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support

authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls: None.

(2) CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS

Include as part of control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment*]].

Discussion: Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle (e.g., during initial design, development, and unit testing).

Related Controls: PE-3, SI-2.

(3) CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS

Leverage the results of control assessments performed by [*Assignment: organization-defined external organization*] on [*Assignment: organization-defined system*] when the assessment meets [*Assignment: organization-defined requirements*].

Discussion: Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories that support the Common Criteria Program [ISO 15408-1], the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

Related Controls: SA-4.

References: [OMB A-130], [FIPS 199], [SP 800-18], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137], [IR 8011-1], [IR 8062].

CA-3 INFORMATION EXCHANGE

Control:

a. Approve and manage the exchange of information between the system and other systems using [*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements;*

user agreements; nondisclosure agreements; [*Assignment: organization-defined type of agreement*]];

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [*Assignment: organization-defined frequency*].

Discussion: System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-6(1) or CA-6(2), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

Control Enhancements:

(1) SYSTEM CONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(25).]

(2) SYSTEM CONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(26).]

(3) SYSTEM CONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(27).]

(4) SYSTEM CONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS

[Withdrawn: Moved to SC-7(28).]

(5) SYSTEM CONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

[Withdrawn: Moved to SC-7(5).]

(6) INFORMATION EXCHANGE | TRANSFER AUTHORIZATIONS

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

Discussion: To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means—whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

Related Controls: AC-2, AC-3, AC-4.

(7) INFORMATION EXCHANGE | TRANSITIVE INFORMATION EXCHANGES

(a) Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and

(b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.

Discussion: Transitive or "downstream" information exchanges are information exchanges between the system or systems with which the organizational system exchanges information and other systems. For mission-essential systems, services, and applications, including high value assets, it is necessary to identify such information exchanges. The transparency of the controls or protection measures in place in such downstream systems connected directly or indirectly to organizational systems is essential to understanding the security and privacy risks resulting from those information exchanges. Organizational systems can inherit risk from downstream systems through transitive connections and information exchanges, which can make the organizational systems more susceptible to threats, hazards, and adverse impacts.

Related Controls: SC-7.

References: [OMB A-130], [FIPS 199], [SP 800-47].

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2.]

CA-5 PLAN OF ACTION AND MILESTONES

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Control Enhancements:

(1) PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [*Assignment: organization-defined automated mechanisms*].

Discussion: Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy information throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Related Controls: None.

References: [OMB A-130], [SP 800-37].

CA-6 AUTHORIZATION

Control:

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

   1. Accepts the use of common controls inherited by the system; and

   2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations [*Assignment: organization-defined frequency*].

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a federal responsibility, and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls: CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

Control Enhancements:

(1) AUTHORIZATION | JOINT AUTHORIZATION — INTRA-ORGANIZATION

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

Discussion: Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners.

Related Controls: AC-6.

(2) AUTHORIZATION | JOINT AUTHORIZATION — INTER-ORGANIZATION

Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.

Discussion: Assigning multiple authorizing officials, at least one of whom comes from an external organization, to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It implements the concepts of separation of duties and dual authorization as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorizing official from the organization that owns or hosts the system may be necessary when the external organizations have a vested interest or equities in the outcome of the authorization decision. The inter-organization joint authorization process is relevant and appropriate for connected systems, shared systems or services, and systems with multiple information owners. The authorizing officials from the external organizations are key stakeholders of the system undergoing authorization.

Related Controls: AC-6.

References: [OMB A-130], [SP 800-37], [SP 800-137].

CA-7 CONTINUOUS MONITORING

Control: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [*Assignment: organization-defined system-level metrics*];

b. Establishing [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, and SI-4.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Discussion: Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related Controls: None.

(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2.]

(3) CONTINUOUS MONITORING | TREND ANALYSES

Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Discussion: Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization or the Federal Government, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors.

Related Controls: None.

(4) CONTINUOUS MONITORING | RISK MONITORING

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls: None.

(5) CONTINUOUS MONITORING | CONSISTENCY ANALYSIS

Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [*Assignment: organization-defined actions*].

Discussion: Security and privacy controls are often added incrementally to a system. As a result, policies for selecting and implementing controls may be inconsistent, and the controls could fail to work together in a consistent or coordinated manner. At a minimum, the lack of consistency and coordination could mean that there are unacceptable security and privacy gaps in the system. At worst, it could mean that some of the controls implemented in one location or by one component are actually impeding the functionality of other controls (e.g., encrypting internal network traffic can impede monitoring). In other situations, failing to consistently monitor all implemented network protocols (e.g., a dual stack of IPv4 and IPv6) may create unintended vulnerabilities in the system that could be exploited by adversaries. It is important to validate—through testing, monitoring, and analysis—that the implemented controls are operating in a consistent, coordinated, non-interfering manner.

Related Controls: None.

(6) CONTINUOUS MONITORING | AUTOMATION SUPPORT FOR MONITORING

Ensure the accuracy, currency, and availability of monitoring results for the system using [*Assignment: organization-defined automated mechanisms*].

Discussion: Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

Related Controls: None.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115],[SP 800-137], [IR 8011-1], [IR 8062].

CA-8 PENETRATION TESTING

Control: Conduct penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined systems or system components*].

Discussion: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Related Controls: RA-5, RA-10, SA-11, SR-5, SR-6.

Control Enhancements:

(1) PENETRATION TESTING | INDEPENDENT PENETRATION TESTING AGENT OR TEAM

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Discussion: Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.

Related Controls: CA-2.

(2) PENETRATION TESTING | RED TEAM EXERCISES

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [*Assignment: organization-defined red team exercises*].

Discussion: Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and

privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Related Controls: None.

(3) PENETRATION TESTING | FACILITY PENETRATION TESTING

Employ a penetration testing process that includes [*Assignment: organization-defined frequency*] [*Selection: announced; unannounced*] attempts to bypass or circumvent controls associated with physical access points to the facility.

Discussion: Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.

Related Controls: CA-2, PE-3.

References: None.

CA-9 INTERNAL SYSTEM CONNECTIONS

Control:

a. Authorize internal connections of [*Assignment: organization-defined system components or classes of components*] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [*Assignment: organization-defined conditions*]; and

d. Review [*Assignment: organization-defined frequency*] the continued need for each internal connection.

Discussion: Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

Control Enhancements:

(1) INTERNAL SYSTEM CONNECTIONS | COMPLIANCE CHECKS

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Discussion: Compliance checks include verification of the relevant baseline configuration.

Related Controls: CM-6.

References: [SP 800-124], [IR 8023].

3.5 CONFIGURATION MANAGEMENT

Quick link to Configuration Management Summary Table

CM-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] configuration management policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

CM-2 BASELINE CONFIGURATION

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [*Assignment: organization-defined frequency*];

2. When required due to [*Assignment: organization-defined circumstances*]; and

3. When system components are installed or upgraded.

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

Related Controls: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

Control Enhancements:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

[Withdrawn: Incorporated into CM-2.]

(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls: CM-7, IA-3, RA-5.

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

Retain [*Assignment: organization-defined number*] of previous versions of baseline configurations of the system to support rollback.

Discussion: Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related Controls: None.

(4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(4).]

(5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE

[Withdrawn: Incorporated into CM-7(5).]

(6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS

Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

Discussion: Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations do not necessarily require separate physical environments.

Related Controls: CM-4, SC-3, SC-7.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS

(a) Issue [*Assignment: organization-defined systems or system components*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [*Assignment: organization-defined controls*].

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls: MP-4, MP-5.

References: [SP 800-124], [SP 800-128].

CM-3 CONFIGURATION CHANGE CONTROL

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time period*];

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; when [*Assignment: organization-defined configuration change conditions*]].

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Control Enhancements:

(1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES

Use [*Assignment: organization-defined automated mechanisms*] to:

(a) Document proposed changes to the system;

(b) Notify [*Assignment: organization-defined approval authorities*] of proposed changes to the system and request change approval;

(c) Highlight proposed changes to the system that have not been approved or disapproved within [*Assignment: organization-defined time period*];

(d) Prohibit changes to the system until designated approvals are received;

(e) Document all changes to the system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the system are completed.

Discussion: None.

Related Controls: None.

(2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems

may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related Controls: None.

(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION

Implement changes to the current system baseline and deploy the updated baseline across the installed base using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated tools can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls: None.

(4) CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES

Require [*Assignment: organization-defined* security and privacy representatives] to be members of the [*Assignment: organization-defined configuration change control element*].

Discussion: Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3*g*.

Related Controls: None.

(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [*Assignment: organization-defined security responses*].

Discussion: Automated security responses include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Related Controls: None.

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [*Assignment: organization-defined controls*].

Discussion: The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Related Controls: SC-12.

(7) CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES

Review changes to the system [*Assignment: organization-defined frequency*] or when [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

Discussion: Indications that warrant a review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.

Related Controls: AU-6, AU-7, CM-3.

(8) CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES

Prevent or restrict changes to the configuration of the system under the following circumstances: [*Assignment: organization-defined circumstances*].

Discussion: System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.

Related Controls: None.

References: [SP 800-124], [SP 800-128], [IR 8062].

CM-4 IMPACT ANALYSES

Control: Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.

Related Controls: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.

Control Enhancements:

(1) IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Discussion: A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls: SA-11, SC-7.

(2) IMPACT ANALYSES | VERIFICATION OF CONTROLS

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls: SA-11, SC-3, SI-6.

References: [SP 800-128].

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

Control Enhancements:

(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS

(a) Enforce access restrictions using [*Assignment: organization-defined automated mechanisms*]; and

(b) Automatically generate audit records of the enforcement actions.

Discussion: Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related Controls: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

[Withdrawn: Incorporated into CM-3(7).]

(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

[Withdrawn: Moved to CM-14.]

(4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION

Enforce dual authorization for implementing changes to [*Assignment: organization-defined system components and system-level information*].

Discussion: Organizations employ dual authorization to help ensure that any changes to selected system components and information cannot occur unless two qualified individuals approve and implement such changes. The two individuals possess the skills and expertise to determine if the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. System-level information includes operational procedures.

Related Controls: AC-2, AC-5, CM-3.

(5) ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges [*Assignment: organization-defined frequency*].

Discussion: In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Related Controls: AC-2.

(6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES

Limit privileges to change software resident within software libraries.

Discussion: Software libraries include privileged programs.

Related Controls: AC-2.

(7) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS

[Withdrawn: Incorporated into SI-7.]

References: [FIPS 140-3]; [FIPS 186-4].

CM-6 CONFIGURATION SETTINGS

Control:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [*Assignment: organization-defined common secure configurations*];

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology

products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline [USGCB] and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Control Enhancements:

(1) CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION

Manage, apply, and verify configuration settings for [*Assignment: organization-defined system components*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls: CA-7.

(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

Take the following actions in response to unauthorized changes to [*Assignment: organization-defined configuration settings*]: [*Assignment: organization-defined actions*].

Discussion: Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

Related Controls: IR-4, IR-6, SI-7.

(3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION

[Withdrawn: Incorporated into SI-7.]

(4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION

[Withdrawn: Incorporated into CM-4.]

References: [SP 800-70], [SP 800-126], [SP 800-128], [USGCB], [NCPR], [DOD STIG].

CM-7 LEAST FUNCTIONALITY

Control:

a. Configure the system to provide only [*Assignment: organization-defined mission essential capabilities*]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [*Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services*].

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3).

Related Controls: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4.

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

(a) Review the system [*Assignment: organization-defined frequency*] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove [*Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure*].

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls: AC-18.

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

Prevent program execution in accordance with [*Selection (one or more):* [*Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions*]*; rules authorizing the terms and conditions of software program usage*].

Discussion: Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related Controls: CM-8, PL-4, PL-9, PM-5, PS-6.

(3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE

Ensure compliance with [*Assignment: organization-defined registration requirements for functions, ports, protocols, and services*].

Discussion: Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.

Related Controls: None.

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION

(a) Identify [*Assignment: organization-defined software programs not authorized to execute on the system*];

(b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

(c) Review and update the list of unauthorized software programs [*Assignment: organization-defined frequency*].

Discussion: Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Related Controls: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION

(a) Identify [*Assignment: organization-defined software programs authorized to execute on the system*];

(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

(c) Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Related Controls: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

(6) LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [*Assignment: organization-defined user-installed software*].

Discussion: Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related Controls: CM-11, SC-44.

(7) LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*] when such code is:

(a) Obtained from sources with limited or no warranty; and/or

(b) Without the provision of source code.

Discussion: Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Related Controls: CM-10, SC-44.

(8) LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE

(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and

(b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.

Discussion: Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

Related Controls: SA-5, SA-22.

(9) LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE

(a) Identify [*Assignment: organization-defined hardware components authorized for system use*];

(b) Prohibit the use or connection of unauthorized hardware components;

(c) Review and update the list of authorized hardware components [*Assignment: organization-defined frequency*].

Discussion: Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.

Related Controls: None.

References: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-167].

CM-8 SYSTEM COMPONENT INVENTORY

Control:

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: [*Assignment: organization-defined information deemed necessary to achieve effective system component accountability*]; and

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

Related Controls: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.

Control Enhancements:

(1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL

Update the inventory of system components as part of component installations, removals, and system updates.

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related Controls: PM-16.

(2) SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and

accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls: None.

(3) SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [*Assignment: organization-defined automated mechanisms*] [*Assignment: organization-defined frequency*]; and

(b) Take the following actions when unauthorized components are detected: [*Selection (one or more): disable network access by such components; isolate the components; notify* [*Assignment: organization-defined personnel or roles*]].

Discussion: Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-7(9)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved , for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing."

Related Controls: AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

(4) SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

Include in the system component inventory information, a means for identifying by [*Selection (one or more): name; position; role*], individuals responsible and accountable for administering those components.

Discussion: Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related Controls: AC-3.

(5) SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

[Withdrawn: Incorporated into CM-8.]

(6) SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

Discussion: Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

Related Controls: None.

(7) SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY

Provide a centralized repository for the inventory of system components.

Discussion: Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.

Related Controls: None.

(8) SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING

Support the tracking of system components by geographic location using [*Assignment: organization-defined automated mechanisms*].

Discussion: The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms can be coordinated with senior agency officials for privacy if there are implications that affect individual privacy.

Related Controls: None.

(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS

(a) Assign system components to a system; and

(b) Receive an acknowledgement from [*Assignment: organization-defined personnel or roles*] of this assignment.

Discussion: System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Related Controls: None.

References: [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-128], [IR 8011-2], [IR 8011-3].

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Discussion: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to

individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

Control Enhancements:

(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Discussion: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Related Controls: None.

References: [SP 800-128].

CM-10 SOFTWARE USAGE RESTRICTIONS

Control:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

Control Enhancements:

(1) SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE

Establish the following restrictions on the use of open-source software: [*Assignment: organization-defined restrictions*].

Discussion: Open-source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open-source software is that it provides organizations with the ability to examine the source code. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software. Open-source software that is available only in binary form may increase the level of risk in using such software.

Related Controls: SI-7.

References: None.

CM-11 USER-INSTALLED SOFTWARE

Control:

a. Establish [*Assignment: organization-defined policies*] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [*Assignment: organization-defined methods*]; and

c. Monitor policy compliance [*Assignment: organization-defined frequency*].

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related Controls: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

Control Enhancements:

(1) USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS

[Withdrawn: Incorporated into CM-8(3).]

(2) USER-INSTALLED SOFTWARE | SOFTWARE INSTALLATION WITH PRIVILEGED STATUS

Allow user installation of software only with explicit privileged status.

Discussion: Privileged status can be obtained, for example, by serving in the role of system administrator.

Related Controls: AC-5, AC-6.

(3) USER-INSTALLED SOFTWARE | AUTOMATED ENFORCEMENT AND MONITORING

Enforce and monitor compliance with software installation policies using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations enforce and monitor compliance with software installation policies using automated mechanisms to more quickly detect and respond to unauthorized software installation which can be an indicator of an internal or external hostile attack.

Related Controls: None.

References: None.

CM-12 INFORMATION LOCATION

Control:

a. Identify and document the location of [*Assignment: organization-defined information*] and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Discussion: Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).

Related Controls: AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

Control Enhancements:

(1) INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

Use automated tools to identify [*Assignment: organization-defined information by information type*] on [*Assignment: organization-defined system components*] to ensure controls are in place to protect organizational information and individual privacy.

Discussion: The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Related Controls: None.

References: [FIPS 199], [SP 800-60-1], [SP 800-60-2].

CM-13 DATA ACTION MAPPING

Control: Develop and document a map of system data actions.

Discussion: Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. A map of system

data actions includes discrete data actions, elements of personally identifiable information being processed in the data actions, system components involved in the data actions, and the owners or operators of the system components. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed in another part of the system), and by whom (e.g., individuals may have different privacy perceptions based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the organization is using. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system.

Related Controls: AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.

CM-14 SIGNED COMPONENTS

Control: Prevent the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related Controls: CM-7, SC-12, SC-13, SI-7.

References: [IR 8062].

3.6 CONTINGENCY PLANNING

Quick link to Contingency Planning Summary Table

CP-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] contingency planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-34], [SP 800-39], [SP 800-50], [SP 800-100].

CP-2 CONTINGENCY PLAN

Control:

a. Develop a contingency plan for the system that:

   1. Identifies essential mission and business functions and associated contingency requirements;

   2. Provides recovery objectives, restoration priorities, and metrics;

   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

   6. Addresses the sharing of contingency information; and

   7. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distribute copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [*Assignment: organization-defined frequency*];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Related Controls: None.

(2) CONTINGENCY PLAN | CAPACITY PLANNING

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Discussion: Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

Plan for the resumption of [*Selection: all; essential*] mission and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(4) CONTINGENCY PLAN | RESUME ALL MISSION AND BUSINESS FUNCTIONS

[Withdrawn: Incorporated into CP-2(3).]

(5) CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS

Plan for the continuance of [*Selection: all; essential*] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Discussion: Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(6) CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITES

Plan for the transfer of [*Selection: all; essential*] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Discussion: When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls: SA-9.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

Identify critical system assets supporting [*Selection: all; essential*] mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Related Controls: CM-8, RA-9.

References: [SP 800-34], [IR 8179].

CP-3 CONTINGENCY TRAINING

Control:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

   1. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;

   2. When required by system changes; and

3. [*Assignment: organization-defined frequency*] thereafter; and

b. Review and update contingency training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Control Enhancements:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Discussion: The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Related Controls: None.

(2) CONTINGENCY TRAINING | MECHANISMS USED IN TRAINING ENVIRONMENTS

Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.

Discussion: Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.

Related Controls: None.

References: [SP 800-50].

CP-4 CONTINGENCY PLAN TESTING

Control:

a. Test the contingency plan for the system [*Assignment: organization-defined frequency*] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [*Assignment: organization-defined tests*].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls: IR-8, PM-8.

(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

Test the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Discussion: Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Related Controls: CP-7.

(3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING

Test the contingency plan using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission and business functions.

Related Controls: None.

(4) CONTINGENCY PLAN TESTING | FULL RECOVERY AND RECONSTITUTION

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes

activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related Controls: CP-10, SC-24.

(5) CONTINGENCY PLAN TESTING | SELF-CHALLENGE

Employ [*Assignment: organization-defined mechanisms*] to [*Assignment: organization-defined system or system component*] to disrupt and adversely affect the system or system component.

Discussion: Often, the best method of assessing system resilience is to disrupt the system in some manner. The mechanisms used by the organization could disrupt system functions or system services in many ways, including terminating or disabling critical system components, changing the configuration of system components, degrading critical functionality (e.g., restricting network bandwidth), or altering privileges. Automated, on-going, and simulated cyber-attacks and service disruptions can reveal unexpected functional dependencies and help the organization determine its ability to ensure resilience in the face of an actual cyber-attack.

Related Controls: None.

References: [FIPS 199], [SP 800-34], [SP 800-84], [SP 800-160-2].

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2.]

CP-6 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of

omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE STORAGE SITE | RECOVERY TIME AND RECOVERY POINT OBJECTIVES

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Discussion: Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related Controls: None.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

References: [SP 800-34].

CP-7 ALTERNATE PROCESSING SITE

Control:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined system operations*] for essential mission and business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites

that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls: None.

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Discussion: Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related Controls: CM-2, CM-6, CP-4.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into CP-7.]

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

Plan and prepare for circumstances that preclude returning to the primary processing site.

Discussion: There may be situations that preclude an organization from returning to the primary processing site such as if a natural disaster (e.g., flood or a hurricane) damaged or

destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Related Controls: None.

References: [SP 800-34].

CP-8 TELECOMMUNICATIONS SERVICES

Control: Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*Assignment: organization-defined system operations*] for essential mission and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, CP-11, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion: Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Related Controls: None.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls: None.

(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Discussion: Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Related Controls: None.

(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

(a) Require primary and alternate telecommunications service providers to have contingency plans;

(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtain evidence of contingency testing and training by providers [*Assignment: organization-defined frequency*].

Discussion: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls: CP-3, CP-4.

(5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING

Test alternate telecommunication services [*Assignment: organization-defined frequency*].

Discussion: Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.

Related Controls: CP-3.

References: [SP 800-34].

CP-9 SYSTEM BACKUP

Control:

a. Conduct backups of user-level information contained in [*Assignment: organization-defined system components*] [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

b. Conduct backups of system-level information contained in the system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

c. Conduct backups of system documentation, including security- and privacy-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Test backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

(2) SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Discussion: Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related Controls: CP-4.

(3) SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

Store backup copies of [*Assignment: organization-defined critical system software and other security-related information*] in a separate facility or in a fire rated container that is not collocated with the operational system.

Discussion: Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may

provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

Related Controls: CM-2, CM-6, CM-8.

(4) SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9.]

(5) SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE

Transfer system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

Discussion: System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

Related Controls: CP-7, MP-3, MP-4, MP-5.

(6) SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Discussion: The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the two systems, the secondary system can also serve as the alternate processing site.

Related Controls: CP-7.

(7) SYSTEM BACKUP | DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION

Enforce dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Discussion: Dual authorization ensures that deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting or destroying backup information possess the skills or expertise to determine if the proposed deletion or destruction of information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls: AC-3, AC-5, MP-2.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined backup information*].

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

References: [FIPS 140-3], [FIPS 186-4], [SP 800-34], [SP 800-130], [SP 800-152].

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Control Enhancements:

(1) SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4.]

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls: None.

(3) SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring.]

(4) SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD

Provide the capability to restore system components within [*Assignment: organization-defined restoration time periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Discussion: Restoration of system components includes reimaging, which restores the components to known, operational states.

Related Controls: CM-2, CM-6.

(5) SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13.]

(6) SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION

Protect system components used for recovery and reconstitution.

Discussion: Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related Controls: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

References: [SP 800-34].

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: Provide the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.

Discussion: Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Related Controls: CP-2, CP-8, CP-13.

Control Enhancements: None.

References: None.

CP-12 SAFE MODE

Control: When [*Assignment: organization-defined conditions*] are detected, enter a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Discussion: For systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Related Controls: CM-2, SA-8, SC-24, SI-13, SI-17.

Control Enhancements: None.

References: None.

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: Employ [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Discussion: Use of alternative security mechanisms supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens—the standard means for achieving secure authentication—are compromised.

Related Controls: CP-2, CP-11, SI-13.

Control Enhancements: None

References: None.

3.7 IDENTIFICATION AND AUTHENTICATION

Quick link to Identification and Authentication Summary Table

IA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] identification and authentication policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AC-1, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [FIPS 201-2], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-100], [IR 7874].

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [HSPD 12]. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5, AC-6.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to non-privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls: AC-5.

(3) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

[Withdrawn: Incorporated into IA-2(1).]

(4) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

[Withdrawn: Incorporated into IA-2(2).]

(5) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Discussion: Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Related Controls: None.

(6) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — SEPARATE DEVICE

Implement multi-factor authentication for [*Selection (one or more): local; network; remote*] access to [*Selection (one or more): privileged accounts; non-privileged accounts*] such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets [*Assignment: organization-defined strength of mechanism requirements*].

Discussion: The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

Related Controls: AC-6.

(7) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE

[Withdrawn: Incorporated into IA-2(6).]

(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT

Implement replay-resistant authentication mechanisms for access to [*Selection (one or more): privileged accounts; non-privileged accounts*].

Discussion: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Related Controls: None.

(9) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT

[Withdrawn: Incorporated into IA-2(8).]

(10) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON

Provide a single sign-on capability for [*Assignment: organization-defined system accounts and services*].

Discussion: Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add multi-factor authentication for applications and systems (existing and new) that may not be able to natively support multi-factor authentication.

Related Controls: None.

(11) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS — SEPARATE DEVICE

[Withdrawn: Incorporated into IA-2(6).]

(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

Accept and electronically verify Personal Identity Verification-compliant credentials.

Discussion: Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using [SP 800-79-2]. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in [SP 800-166]. The DOD Common Access Card (CAC) is an example of a PIV credential.

Related Controls: None.

(13) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | OUT-OF-BAND AUTHENTICATION

Implement the following out-of-band authentication mechanisms under [*Assignment: organization-defined conditions*]: [*Assignment: organization-defined out-of-band authentication*].

Discussion: Out-of-band authentication refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path) is used to identify and authenticate users or devices and is generally the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. Out-of-band authentication can be used to mitigate actual or suspected "man-in the-middle" attacks. The conditions or criteria for activation include suspicious activities, new threat indicators, elevated threat levels, or the impact or classification level of information in requested transactions.

Related Controls: IA-10, IA-11, SC-37.

References: [FIPS 140-3], [FIPS 201-2], [FIPS 202], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-79-2], [SP 800-156], [SP 800-166], [IR 7539], [IR 7676], [IR 7817], [IR 7849], [IR 7870], [IR 7874], [IR 7966].

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Discussion: Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related Controls: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

Control Enhancements:

(1) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Discussion: A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

Related Controls: SC-8, SC-12, SC-13.

(2) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION

[Withdrawn: Incorporated into IA-3(1).]

(3) DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION

(a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and

(b) Audit lease information when assigned to a device.

Discussion: The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dynamically receive network address assignments.

Related Controls: AU-2.

(4) DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION

Handle device identification and authentication based on attestation by [*Assignment: organization-defined configuration management process*].

Discussion: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

Related Controls: CM-2, CM-3, CM-6.

References: None.

IA-4 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*].

Discussion: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

Control Enhancements:

(1) IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS

Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.

Discussion: Prohibiting account identifiers as public identifiers applies to any publicly disclosed account identifier used for communication such as, electronic mail and instant

messaging. Prohibiting the use of systems account identifiers that are the same as some public identifier, such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers. Prohibiting account identifiers as public identifiers without the implementation of other supporting controls only complicates guessing of identifiers. Additional protections are required for authenticators and credentials to protect the account.

Related Controls: AT-2, PT-7.

(2) IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION

[Withdrawn: Incorporated into IA-12(1).]

(3) IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION

[Withdrawn: Incorporated into IA-12(2).]

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

Manage individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

Discussion: Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Related Controls: None.

(5) IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT

Manage individual identifiers dynamically in accordance with [*Assignment: organization-defined dynamic identifier policy*].

Discussion: In contrast to conventional approaches to identification that presume static accounts for preregistered users, many distributed systems establish identifiers at runtime for entities that were previously unknown. When identifiers are established at runtime for previously unknown entities, organizations can anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate credentials and related identifiers are essential.

Related Controls: AC-16.

(6) IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT

Coordinate with the following external organizations for cross-organization management of identifiers: [*Assignment: organization-defined external organizations*].

Discussion: Cross-organization identifier management provides the capability to identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

Related Controls: AU-16, IA-2, IA-5.

(7) IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION

[Withdrawn: Incorporated into IA-12(4).]

(8) IDENTIFIER MANAGEMENT | PAIRWISE PSEUDONYMOUS IDENTIFIERS

Generate pairwise pseudonymous identifiers.

Discussion: A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by an identity provider for use at a specific individual relying party. Generating distinct pairwise pseudonymous identifiers with no identifying information about a subscriber discourages subscriber activity tracking and profiling beyond the operational

requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party except in situations where relying parties can show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

Related Controls: IA-5.

(9) IDENTIFIER MANAGEMENT | ATTRIBUTE MAINTENANCE AND PROTECTION

Maintain the attributes for each uniquely identified individual, device, or service in [*Assignment: organization-defined protected central storage*].

Discussion: For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Related Controls: None.

References: [FIPS 201-2], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for

time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*].

Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Related Controls: IA-6.

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

Discussion: Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

Related Controls: IA-3, SC-17.

(3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION

[Withdrawn: Incorporated into IA-12(4).]

(4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

[Withdrawn: Incorporated into IA-5(1).]

(5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Discussion: Changing authenticators prior to the delivery and installation of system components extends the requirement for organizations to change default authenticators upon system installation by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to developers of commercial off-the-shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

Related Controls: None.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Discussion: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls: RA-2.

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Discussion: In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators.

Related Controls: None.

(8) AUTHENTICATOR MANAGEMENT | MULTIPLE SYSTEM ACCOUNTS

Implement [*Assignment: organization-defined security controls*] to manage the risk of compromise due to individuals having accounts on multiple systems.

Discussion: When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behavior (see PL-4) and access agreements (see PS-6) to mitigate the risk of multiple system accounts.

Related Controls: PS-6.

(9) AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT

Use the following external organizations to federate credentials: [*Assignment: organization-defined external organizations*].

Discussion: Federation provides organizations with the capability to authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information. Using a specific list of approved external organizations for authentication helps to ensure that those organizations are vetted and trusted.

Related Controls: AU-7, AU-16.

(10) AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL BINDING

Bind identities and authenticators dynamically using the following rules: [*Assignment: organization-defined binding rules*].

Discussion: Authentication requires some form of binding between an identity and the authenticator that is used to confirm the identity. In conventional approaches, binding is established by pre-provisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system. New authentication techniques allow the binding between the identity and the authenticator to be implemented external to a system. For example, with smartcard credentials, the identity and authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Related Controls: AU-16, IA-5.

(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

[Withdrawn: Incorporated into IA-2(1) and IA-2(2).]

(12) AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION PERFORMANCE

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [*Assignment: organization-defined biometric quality requirements*].

Discussion: Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.

Related Controls: AC-7.

(13) AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS

Prohibit the use of cached authenticators after [*Assignment: organization-defined time period*].

Discussion: Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

Related Controls: None.

(14) AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES

For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.

Discussion: An organization-wide methodology for managing the content of PKI trust stores helps improve the accuracy and currency of PKI-based authentication credentials across the organization.

Related Controls: None.

(15) AUTHENTICATOR MANAGEMENT | GSA-APPROVED PRODUCTS AND SERVICES

Use only General Services Administration-approved products and services for identity, credential, and access management.

Discussion: General Services Administration (GSA)-approved products and services are products and services that have been approved through the GSA conformance program, where applicable, and posted to the GSA Approved Products List. GSA provides guidance for teams to design and build functional and secure systems that comply with Federal Identity, Credential, and Access Management (FICAM) policies, technologies, and implementation patterns.

Related Controls: None.

(16) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE

Require that the issuance of [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted external party*] before [*Assignment: organization-defined registration authority*] with authorization by *[Assignment: organization-defined personnel or roles*].

Discussion: Issuing authenticators in person or by a trusted external party enhances and reinforces the trustworthiness of the identity proofing process.

Related Controls: IA-12.

(17) AUTHENTICATOR MANAGEMENT | PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS

Employ presentation attack detection mechanisms for biometric-based authentication.

Discussion: Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online web accesses, taking a picture of someone with a camera phone to obtain facial images with or without their knowledge, lifting from objects that someone has touched (e.g., a latent fingerprint), or capturing a high-resolution image (e.g., an iris pattern). Presentation attack detection technologies including liveness detection, can mitigate the risk of these types of attacks by making it difficult to produce artifacts intended to defeat the biometric sensor.

Related Controls: AC-7.

(18) AUTHENTICATOR MANAGEMENT | PASSWORD MANAGERS

(a) Employ [*Assignment: organization-defined password managers*] to generate and manage passwords; and

(b) Protect the passwords using [*Assignment: organization-defined controls*].

Discussion: For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see IA-5(1)(d)) and storing the collection offline in a token.

Related Controls: None.

References: [FIPS 140-3], [FIPS 180-4], [FIPS 201-2], [FIPS 202], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [IR 7539], [IR 7817], [IR 7849], [IR 7870], [IR 8040].

IA-6 AUTHENTICATION FEEDBACK

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Discussion: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related Controls: AC-3.

Control Enhancements: None.

References: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Discussion: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13.

Control Enhancements: None.

References: [FIPS 140-3].

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Discussion: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

Discussion: Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using [SP 800-79-2].

Related Controls: PE-3.

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

Discussion: Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with [SP 800-63B]. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Related Controls: None.

(3) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS

[Withdrawn: Incorporated into IA-8(2).]

(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES

Conform to the following profiles for identity management [*Assignment: organization-defined identity management profiles*].

Discussion: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: None.

(5) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS

Accept and verify federated or PKI credentials that meet [*Assignment: organization-defined policy*].

Discussion: Acceptance of PIV-I credentials can be implemented by PIV, PIV-I, and other commercial or external identity providers. The acceptance and verification of PIV-I-compliant credentials apply to both logical and physical access control systems. The acceptance and verification of PIV-I credentials address nonfederal issuers of identity cards that desire to interoperate with United States Government PIV systems and that can be trusted by Federal Government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is commensurate with the PIV credentials as defined in cited references. PIV-I credentials are the credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified with the FBCA (directly or through another PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy.

Related Controls: None.

(6) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | DISASSOCIABILITY

Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [*Assignment: organization-defined measures*].

Discussion: Federated identity solutions can create increased privacy risks due to the tracking and profiling of individuals. Using identifier mapping tables or cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties can reduce these privacy risks.

Related Controls: None.

References: [OMB A-130], [FED PKI], [FIPS 201-2], [SP 800-63-3], [SP 800-79-2], [SP 800-116], [IR 8062].

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate [*Assignment: organization-defined system services and applications*] before establishing communications with devices, users, or other services or applications.

Discussion: Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Related Controls: IA-3, IA-4, IA-5, SC-8.

Control Enhancements:

(1) SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE

[Withdrawn: Incorporated into IA-9.]

(2) SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS

[Withdrawn: Incorporated into IA-9.]

References: None.

IA-10 ADAPTIVE AUTHENTICATION

Control: Require individuals accessing the system to employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].

Discussion: Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Suspicious behavior may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than individuals would routinely access; or attempting to access information from suspicious network addresses. When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number or types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of multi-factor authentication mechanisms but can augment implementations of multi-factor authentication.

Related Controls: IA-2, IA-8.

Control Enhancements: None.

References: [SP 800-63-3].

IA-11 RE-AUTHENTICATION

Control: Require users to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

Discussion: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

Control Enhancements: None.

References: None.

IA-12 IDENTITY PROOFING

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Discussion: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of

their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include [SP 800-63-3] and [SP 800-63A]. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Control Enhancements:

(1) IDENTITY PROOFING | SUPERVISOR AUTHORIZATION

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Discussion: Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the organization.

Related Controls: None.

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

Require evidence of individual identification be presented to the registration authority.

Discussion: Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Related Controls: None.

(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION

Require that the presented identity evidence be validated and verified through [*Assignment: organizational defined methods of validation and verification*].

Discussion: Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

Related Controls: None.

(4) IDENTITY PROOFING | IN-PERSON VALIDATION AND VERIFICATION

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Discussion: In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

Related Controls: None.

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

Require that a [*Selection: registration code; notice of proofing*] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Discussion: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

Related Controls: IA-12.

(6) IDENTITY PROOFING | ACCEPT EXTERNALLY-PROOFED IDENTITIES

Accept externally-proofed identities at [*Assignment: organization-defined identity assurance level*].

Discussion: To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and the identity assurance level appropriate for the system, application, or information accessed. Accepting externally-proofed identities is a fundamental component of managing federated identities across agencies and organizations.

Related Controls: IA-3, IA-4, IA-5, IA-8.

References: [FIPS 201-2], [SP 800-63-3], [SP 800-63A], [SP 800-79-2].

3.8 INCIDENT RESPONSE

Quick link to Incident Response Summary Table

IR-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] incident response policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-61], [SP 800-83], [SP 800-100].

IR-2 INCIDENT RESPONSE TRAINING

Control:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

   1. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility or acquiring system access;

   2. When required by system changes; and

   3. [*Assignment: organization-defined frequency*] thereafter; and

b. Review and update incident response training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Discussion: Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

Related Controls: None.

(2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

Provide an incident response training environment using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

Related Controls: None.

(3) INCIDENT RESPONSE TRAINING | BREACH

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Discussion: For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-2(1).

Related Controls: None.

References: [OMB M-17-12], [SP 800-50].

IR-3 INCIDENT RESPONSE TESTING

Control: Test the effectiveness of the incident response capability for the system [*Assignment: organization-defined frequency*] using the following tests: [*Assignment: organization-defined tests*].

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Control Enhancements:

(1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING

Test the incident response capability using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished by providing more complete coverage of incident response issues, selecting realistic test scenarios and environments, and stressing the response capability.

Related Controls: None.

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Related Controls: None.

(3) INCIDENT RESPONSE TESTING | CONTINUOUS IMPROVEMENT

Use qualitative and quantitative data from testing to:

(a) Determine the effectiveness of incident response processes;

(b) Continuously improve incident response processes; and

(c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Discussion: To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Related Controls: None.

References: [OMB A-130], [SP 800-84], [SP 800-115].

IR-4 INCIDENT HANDLING

Control:

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Support the incident handling process using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Related Controls: None.

(2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION

Include the following types of dynamic reconfiguration for [*Assignment: organization-defined system components*] as part of the incident response capability: [*Assignment: organization-defined types of dynamic reconfiguration*].

Discussion: Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

Related Controls: AC-2, AC-4, CM-2.

(3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Identify [*Assignment: organization-defined classes of incidents*] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [*Assignment: organization-defined actions to take in response to classes of incidents*].

Discussion: Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack. Organizations consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified as part of IR-4(5).

Related Controls: None.

(4) INCIDENT HANDLING | INFORMATION CORRELATION

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Discussion: Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Related Controls: None.

(5) INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM

Implement a configurable capability to automatically disable the system if [*Assignment: organization-defined security violations*] are detected.

Discussion: Organizations consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-2 or IR-4(3). Security violations include cyber-attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals.

Related Controls: None.

(6) INCIDENT HANDLING | INSIDER THREATS

Implement an incident handling capability for incidents involving insider threats.

Discussion: Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

Related Controls: None.

(7) INCIDENT HANDLING | INSIDER THREATS — INTRA-ORGANIZATION COORDINATION

Coordinate an incident handling capability for insider threats that includes the following organizational entities [*Assignment: organization-defined entities*].

Discussion: Incident handling for insider threat incidents (e.g., preparation, detection and analysis, containment, eradication, and recovery) requires coordination among many organizational entities, including mission or business owners, system owners, human resources offices, procurement offices, personnel offices, physical security offices, senior agency information security officer, operations personnel, risk executive (function), senior agency official for privacy, and legal counsel. In addition, organizations may require external support from federal, state, and local law enforcement agencies.

Related Controls: None.

(8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS

Coordinate with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Discussion: The coordination of incident information with external organizations—including mission or business partners, military or coalition partners, customers, and developers—can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization's operations, assets, and individuals.

Related Controls: AU-16, PM-16.

(9) INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY

Employ [*Assignment: organization-defined dynamic response capabilities*] to respond to incidents.

Discussion: The dynamic response capability addresses the timely deployment of new or replacement organizational capabilities in response to incidents. This includes capabilities implemented at the mission and business process level and at the system level.

Related Controls: None.

(10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION

Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents can occur anywhere through or to the supply chain and include compromises or breaches that involve primary or sub-tier providers, information technology products, system components, development processes or personnel, and distribution processes or warehousing facilities. Organizations consider including processes for protecting and sharing incident information in information exchange agreements and their obligations for reporting incidents to government oversight bodies (e.g., Federal Acquisition Security Council).

Related Controls: CA-3, MA-2, SA-9, SR-8.

(11) INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [*Assignment: organization-defined time period*].

Discussion: An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Related Controls: AT-3.

(12) INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS

Analyze malicious code and/or other residual artifacts remaining in the system after the incident.

Discussion: When conducted carefully in an isolated environment, analysis of malicious code and other residual artifacts of a security incident or breach can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. In addition, malicious code analysis can help the organization develop responses to future incidents.

Related Controls: None.

(13) INCIDENT HANDLING | BEHAVIOR ANALYSIS

Analyze anomalous or suspected adversarial behavior in or related to [*Assignment: organization-defined environments or resources*].

Discussion: If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures. External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

Related Controls: None.

(14) INCIDENT HANDLING | SECURITY OPERATIONS CENTER

Establish and maintain a security operations center.

Discussion: A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and

operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

Related Controls: None.

(15) INCIDENT HANDLING | PUBLIC RELATIONS AND REPUTATION REPAIR

(a) Manage public relations associated with an incident; and

(b) Employ measures to repair the reputation of the organization.

Discussion: It is important for an organization to have a strategy in place for addressing incidents that have been brought to the attention of the general public, have cast the organization in a negative light, or have affected the organization's constituents (e.g., partners, customers). Such publicity can be extremely harmful to the organization and affect its ability to carry out its mission and business functions. Taking proactive steps to repair the organization's reputation is an essential aspect of reestablishing the trust and confidence of its constituents.

Related Controls: None.

References: [FASC18], [41 CFR 201], [OMB M-17-12], [SP 800-61], [SP 800-86], [SP 800-101], [SP 800-150], [SP 800-160-2], [SP 800-184], [IR 7559].

IR-5 INCIDENT MONITORING

Control: Track and document incidents.

Discussion: Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Related Controls: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) INCIDENT MONITORING | AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS

Track incidents and collect and analyze incident information using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Related Controls: None.

References: [SP 800-61].

IR-6 INCIDENT REPORTING

Control:

a. Require personnel to report suspected incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and

b. Report incident information to [*Assignment: organization-defined authorities*].

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Related Controls: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

Report incidents using [*Assignment: organization-defined automated mechanisms*].

Discussion: The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related Controls: IR-7.

(2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS

Report system vulnerabilities associated with reported incidents to [*Assignment: organization-defined personnel or roles*].

Discussion: Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

Related Controls: None.

(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls: SR-8.

References: [FASC18], [41 CFR 201], [USCERT IR], [SP 800-61].

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Discussion: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

Increase the availability of incident response information and support using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Related Controls: None.

(2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS

(a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and

(b) Identify organizational incident response team members to the external providers.

Discussion: External providers of a system protection capability include the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks. It may be beneficial to have agreements in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

Related Controls: None.

References: [OMB A-130], [IR 7559].

IR-8 INCIDENT RESPONSE PLAN

Control:

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]; and
10. Explicitly designates responsibility for incident response to [*Assignment: organization-defined entities, personnel, or roles*].

b. Distribute copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

Control Enhancements:

(1) INCIDENT RESPONSE PLAN | BREACHES

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;

(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

(c) Identification of applicable privacy requirements.

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Related Controls: PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

References: [OMB A-130], [SP 800-61], [OMB M-17-12].

IR-9 INFORMATION SPILLAGE RESPONSE

Control: Respond to information spills by:

a. Assigning [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: [*Assignment: organization-defined actions*].

Discussion: Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Related Controls: CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

Control Enhancements:

(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL

[Withdrawn: Incorporated into IR-9.]

(2) INFORMATION SPILLAGE RESPONSE | TRAINING

Provide information spillage response training [*Assignment: organization-defined frequency*].

Discussion: Organizations establish requirements for responding to information spillage incidents in incident response plans. Incident response training on a regular basis helps to ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

Related Controls: AT-2, AT-3, CP-3, IR-2.

(3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [*Assignment: organization-defined procedures*].

Discussion: Corrective actions for systems contaminated due to information spillages may be time-consuming. Personnel may not have access to the contaminated systems while corrective actions are being taken, which may potentially affect their ability to conduct organizational business.

Related Controls: None.

(4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL

Employ the following controls for personnel exposed to information not within assigned access authorizations: [*Assignment: organization-defined controls*].

Discussion: Controls include ensuring that personnel who are exposed to spilled information are made aware of the laws, executive orders, directives, regulations, policies, standards,

and guidelines regarding the information and the restrictions imposed based on exposure to such information.

Related Controls: None.

References: None.

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

[Withdrawn: Moved to IR-4(11).]

3.9 MAINTENANCE

Quick link to Maintenance Summary Table

MA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] maintenance policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

MA-2 CONTROLLED MAINTENANCE

Control:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [*Assignment: organization-defined information*];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [*Assignment: organization-defined information*].

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

Control Enhancements:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2.]

(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [*Assignment: organization-defined automated mechanisms*]; and

(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Discussion: The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

Related Controls: MA-3.

References: [OMB A-130], [IR 8023].

MA-3 MAINTENANCE TOOLS

Control:

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [*Assignment: organization-defined frequency*].

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

Prevent the removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls: MP-6.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE

Restrict the use of maintenance tools to authorized personnel only.

Discussion: Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Related Controls: AC-3, AC-5, AC-6.

(5) MAINTENANCE TOOLS | EXECUTION WITH PRIVILEGE

Monitor the use of maintenance tools that execute with increased privilege.

Discussion: Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Related Controls: AC-3, AC-6.

(6) MAINTENANCE TOOLS | SOFTWARE UPDATES AND PATCHES

Inspect maintenance tools to ensure the latest software updates and patches are installed.

Discussion: Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Related Controls: AC-3, AC-6.

References: [SP 800-88].

MA-4 NONLOCAL MAINTENANCE

Control:

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

Discussion: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. [SP 800-63B] provides additional guidance on strong authentication and authenticators.

Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

Control Enhancements:

(1) NONLOCAL MAINTENANCE | LOGGING AND REVIEW

(a) Log [*Assignment: organization-defined audit events*] for nonlocal maintenance and diagnostic sessions; and

(b) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Discussion: Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

[Withdrawn: Incorporated into MA-1 and MA-4.]

(3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION

(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Discussion: Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls: MP-6, SI-3, SI-7.

(4) NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS

Protect nonlocal maintenance sessions by:

(a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and

(b) Separating the maintenance sessions from other network sessions with the system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths.

Discussion: Communications paths can be logically separated using encryption.

Related Controls: None.

(5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS

(a) Require the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and

(b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [*Assignment: organization-defined personnel or roles*].

Discussion: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Related Controls: None.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [*Assignment: organization-defined cryptographic mechanisms*].

Discussion: Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized

access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Related Controls: SC-8, SC-12, SC-13.

(7) NONLOCAL MAINTENANCE | DISCONNECT VERIFICATION

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

Discussion: Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

Related Controls: AC-12.

References: [FIPS 140-3], [FIPS 197], [FIPS 201-2], [SP 800-63-3], [SP 800-88].

MA-5 MAINTENANCE PERSONNEL

Control:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Control Enhancements:

(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

(a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all

volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develop and implement [*Assignment: organization-defined alternate controls*] in the event a system component cannot be sanitized, removed, or disconnected from the system.

Discussion: Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related Controls: MP-6, PL-2.

(2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. To mitigate the inherent risk of such exposure, organizations use maintenance personnel that are cleared (i.e., possess security clearances) to the classification level of the information stored on the system.

Related Controls: PS-3.

(3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. If access to classified information on organizational systems is restricted to U.S. citizens, the same restriction is applied to personnel performing maintenance on those systems.

Related Controls: PS-3.

(4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS

Ensure that:

(a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

Discussion: Personnel who conduct maintenance and diagnostic activities on organizational systems may be exposed to classified information. If non-U.S. citizens are permitted to perform maintenance and diagnostics activities on classified systems, then additional vetting is required to ensure agreements and restrictions are not being violated.

Related Controls: PS-3.

(5) MAINTENANCE PERSONNEL | NON-SYSTEM MAINTENANCE

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

Discussion: Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

Related Controls: None.

References: None.

MA-6 TIMELY MAINTENANCE

Control: Obtain maintenance support and/or spare parts for [*Assignment: organization-defined system components*] within [*Assignment: organization-defined time period*] of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Control Enhancements:

(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE

Perform preventive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Discussion: Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail. Methods of determining what preventive (or other) failure management policies to apply include original equipment manufacturer recommendations; statistical failure records; expert opinion; maintenance that has already been conducted on similar equipment; requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indications.

Related Controls: None.

(2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE

Perform predictive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Discussion: Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment's condition. The predictive maintenance approach employs principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thus minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability.

Related Controls: None.

(3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

Transfer predictive maintenance data to a maintenance management system using [*Assignment: organization-defined automated mechanisms*].

Discussion: A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Related Controls: None.

References: None.

MA-7 FIELD MAINTENANCE

Control: Restrict or prohibit field maintenance on [*Assignment: organization-defined systems or system components*] to [*Assignment: organization-defined trusted maintenance facilities*].

Discussion: Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site (i.e., operational environment). In certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigor or with the same quality control checks as depot maintenance. For critical systems designated as such by the organization, it may be necessary to restrict or prohibit field maintenance at the local site and require that such maintenance be conducted in trusted facilities with additional controls.

Related Controls: MA-2, MA-4, MA-5.

Control Enhancements: None.

References: None.

3.10 MEDIA PROTECTION

Quick link to Media Protection Summary Table

MP-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] media protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

MP-2 MEDIA ACCESS

Control: Restrict access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.

Control Enhancements:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Incorporated into MP-4(2).]

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28(1).]

References: [OMB A-130], [FIPS 199], [SP 800-111].

MP-3 MEDIA MARKING

Control:

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt [*Assignment: organization-defined types of system media*] from marking if the media remain within [*Assignment: organization-defined controlled areas*].

Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: AC-16, CP-9, MP-5, PE-22, SI-12.

Control Enhancements: None.

References: [EO 13556], [32 CFR 2002], [FIPS 199].

MP-4 MEDIA STORAGE

Control:

a. Physically control and securely store [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.

Control Enhancements:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28(1).]

(2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS

Restrict access to media storage areas and log access attempts and access granted using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include keypads, biometric readers, or card readers on the external entries to media storage areas.

Related Controls: AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.

References: [FIPS 199], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-111].

MP-5 MEDIA TRANSPORT

Control:

a. Protect and control [*Assignment: organization-defined types of system media*] during transport outside of controlled areas using [*Assignment: organization-defined controls*];

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic

mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

Control Enhancements:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS

[Withdrawn: Incorporated into MP-5.]

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES

[Withdrawn: Incorporated into MP-5.]

(3) MEDIA TRANSPORT | CUSTODIANS

Employ an identified custodian during transport of system media outside of controlled areas.

Discussion: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.

Related Controls: None.

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into SC-28(1).]

References: [FIPS 199], [SP 800-60-1], [SP 800-60-2].

MP-6 MEDIA SANITIZATION

Control:

a. Sanitize [*Assignment: organization-defined system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

Control Enhancements:

(1) MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY

Review, approve, track, document, and verify media sanitization and disposal actions.

Discussion: Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Related Controls: None.

(2) MEDIA SANITIZATION | EQUIPMENT TESTING

Test sanitization equipment and procedures [*Assignment: organization-defined frequency*] to ensure that the intended sanitization is being achieved.

Discussion: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

Related Controls: None.

(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

Discussion: Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Related Controls: None.

(4) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6.]

(5) MEDIA SANITIZATION | CLASSIFIED INFORMATION

[Withdrawn: Incorporated into MP-6.]

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION

[Withdrawn: Incorporated into MP-6.]

(7) MEDIA SANITIZATION | DUAL AUTHORIZATION

Enforce dual authorization for the sanitization of [*Assignment: organization-defined system media*].

Discussion: Organizations employ dual authorization to help ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls: AC-3, MP-2.

(8) MEDIA SANITIZATION | REMOTE PURGING OR WIPING OF INFORMATION

Provide the capability to purge or wipe information from [*Assignment: organization-defined systems or system components*] [*Selection: remotely; under the following conditions:* [*Assignment: organization-defined conditions*]].

Discussion: Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

Related Controls: None.

References: [32 CFR 2002], [OMB A-130], [NARA CUI], [FIPS 199], [SP 800-60-1], [SP 800-60-2], [SP 800-88], [SP 800-124], [IR 8023], [NSA MEDIA].

MP-7 MEDIA USE

Control:

a. [*Selection: Restrict; Prohibit*] the use of [*Assignment: organization-defined types of system media*] on [*Assignment: organization-defined systems or system components*] using [*Assignment: organization-defined controls*]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or

write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Control Enhancements:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

[Withdrawn: Incorporated into MP-7.]

(2) MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA

Prohibit the use of sanitization-resistant media in organizational systems.

Discussion: Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Related Controls: MP-6.

References: [FIPS 199], [SP 800-111].

MP-8 MEDIA DOWNGRADING

Control:

a. Establish [*Assignment: organization-defined system media downgrading process*] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;

b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

c. Identify [*Assignment: organization-defined system media requiring downgrading*]; and

d. Downgrade the identified system media using the established process.

Discussion: Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information.

Related Controls: None.

Control Enhancements:

(1) MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS

Document system media downgrading actions.

Discussion: Organizations can document the media downgrading process by providing information, such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

Related Controls: None.

(2) MEDIA DOWNGRADING | EQUIPMENT TESTING

Test downgrading equipment and procedures [*Assignment: organization-defined frequency*] to ensure that downgrading actions are being achieved.

Discussion: None.

Related Controls: None.

(3) MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION

Downgrade system media containing controlled unclassified information prior to public release.

Discussion: The downgrading of controlled unclassified information uses approved sanitization tools, techniques, and procedures.

Related Controls: None.

(4) MEDIA DOWNGRADING | CLASSIFIED INFORMATION

Downgrade system media containing classified information prior to release to individuals without required access authorizations.

Discussion: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Related Controls: None.

References: [32 CFR 2002], [NSA MEDIA].

3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

Quick link to Physical and Environmental Protection Summary Table

PE-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] physical and environmental protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

d. Remove individuals from the facility access list when access is no longer required.

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related Controls: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Control Enhancements:

(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE

Authorize physical access to the facility where the system resides based on position or role.

Discussion: Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Related Controls: AC-2, AC-3, AC-6.

(2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION

Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [*Assignment: organization-defined list of acceptable forms of identification*].

Discussion: Acceptable forms of identification include passports, REAL ID-compliant drivers' licenses, and Personal Identity Verification (PIV) cards. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

Related Controls: IA-2, IA-4, IA-5.

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

Restrict unescorted access to the facility where the system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;* [*Assignment: organization-defined physical access authorizations*]].

Discussion: Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Related Controls: PS-2, PS-6.

References: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

PE-3 PHYSICAL ACCESS CONTROL

Control:

a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems or devices*]; *guards*];

b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [*Assignment: organization-defined physical access controls*];

d. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Change combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

Control Enhancements:

(1) PHYSICAL ACCESS CONTROL | SYSTEM ACCESS

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the system*].

Discussion: Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls: None.

(2) PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS

Perform security checks [*Assignment: organization-defined frequency*] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

Discussion: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related Controls: AC-4, SC-7.

(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS

Employ guards to control [*Assignment: organization-defined physical access points*] to the facility where the system resides 24 hours per day, 7 days per week.

Discussion: Employing guards at selected physical access points to the facility provides a more rapid response capability for organizations. Guards also provide the opportunity for human surveillance in areas of the facility not covered by video surveillance.

Related Controls: CP-6, CP-7, PE-6.

(4) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS

Use lockable physical casings to protect [*Assignment: organization-defined system components*] from unauthorized physical access.

Discussion: The greatest risk from the use of portable devices—such as smart phones, tablets, and notebook computers—is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.

Related Controls: None.

(5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION

Employ [*Assignment: organization-defined anti-tamper technologies*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the system.

Discussion: Organizations can implement tamper detection and prevention at selected hardware components or implement tamper detection at some components and tamper prevention at other components. Detection and prevention activities can employ many types of anti-tamper technologies, including tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Related Controls: SA-16, SR-9, SR-11.

(6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING

[Withdrawn: Incorporated into CA-8.]

(7) PHYSICAL ACCESS CONTROL | PHYSICAL BARRIERS

Limit access using physical barriers.

Discussion: Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Related Controls: None.

(8) PHYSICAL ACCESS CONTROL | ACCESS CONTROL VESTIBULES

Employ access control vestibules at [*Assignment: organization-defined locations within the facility*].

Discussion: An access control vestibule is part of a physical access control system that typically provides a space between two sets of interlocking doors. Vestibules are designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as piggybacking or tailgating, results in unauthorized access to the facility. Interlocking door controllers can be used to limit the number of individuals who enter controlled access points and to provide containment areas while authorization for physical access is verified. Interlocking door controllers can be fully automated (i.e., controlling the opening and closing of the doors) or partially automated (i.e., using security guards to control the number of individuals entering the containment area).

Related Controls: None.

References: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-116].

PE-4 ACCESS CONTROL FOR TRANSMISSION

Control: Control physical access to [*Assignment: organization-defined system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security controls*].

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Control Enhancements: None.

References: None.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: Control physical access to output from [*Assignment: organization-defined output devices*] to prevent unauthorized individuals from obtaining the output.

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

[Withdrawn: Incorporated into PE-5.]

(2) ACCESS CONTROL FOR OUTPUT DEVICES | LINK TO INDIVIDUAL IDENTITY

Link individual identity to receipt of output from output devices.

Discussion: Methods for linking individual identity to the receipt of output from output devices include installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.

Related Controls: None.

(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES

[Withdrawn: Incorporated into PE-22.]

References: [IR 8023].

PE-6 MONITORING PHYSICAL ACCESS

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls: None.

(2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES

Recognize [*Assignment: organization-defined classes or types of intrusions*] and initiate [*Assignment: organization-defined response actions*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms. Physical access monitoring can be coordinated with intrusion detection

systems and system monitoring capabilities to provide integrated threat coverage for the organization.

Related Controls: SI-4.

(3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

(a) Employ video surveillance of [*Assignment: organization-defined operational areas*];

(b) Review video recordings [*Assignment: organization-defined frequency*]; and

(c) Retain video recordings for [*Assignment: organization-defined time period*].

Discussion: Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. There may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

Related Controls: None.

(4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS

Monitor physical access to the system in addition to the physical access monitoring of the facility at [*Assignment: organization-defined physical spaces containing one or more components of the system*].

Discussion: Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Related Controls: None.

References: None.

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3.]

PE-8 VISITOR ACCESS RECORDS

Control:

a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time period*];

b. Review visitor access records [*Assignment: organization-defined frequency*]; and

c. Report anomalies in visitor access records to [*Assignment: organization-defined personnel*].

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

Control Enhancements:

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW

Maintain and review visitor access records using [*Assignment: organization-defined automated mechanisms*].

Discussion: Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Related Controls: None.

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS

[Withdrawn: Incorporated into PE-2.]

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [*Assignment: organization-defined elements*].

Discussion: Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3, SA-8.

References: None.

PE-9 POWER EQUIPMENT AND CABLING

Control: Protect power equipment and power cabling for the system from damage and destruction.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

Control Enhancements:

(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING

Employ redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Discussion: Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Related Controls: None.

(2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS

Employ automatic voltage controls for [*Assignment: organization-defined critical system components*].

Discussion: Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Related Controls: None.

References: None.

PE-10 EMERGENCY SHUTOFF

Control:

a. Provide the capability of shutting off power to [*Assignment: organization-defined system or individual system components*] in emergency situations;

b. Place emergency shutoff switches or devices in [*Assignment: organization-defined location by system or system component*] to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls: PE-15.

Control Enhancements:

(1) EMERGENCY SHUTOFF | ACCIDENTAL AND UNAUTHORIZED ACTIVATION

[Withdrawn: Incorporated into PE-10.]

References: None.

PE-11 EMERGENCY POWER

Control: Provide an uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power*] in the event of a primary power source loss.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY POWER | ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY

Provide an alternate power supply for the system that is activated [*Selection: manually; automatically*] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related Controls: None.

(2) EMERGENCY POWER | ALTERNATE POWER SUPPLY — SELF-CONTAINED

Provide an alternate power supply for the system that is activated [*Selection: manually; automatically*] and that is:

(a) Self-contained;

(b) Not reliant on external power generation; and

(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.

Discussion: The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Related Controls: None.

References: None.

PE-12 EMERGENCY LIGHTING

Control: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related Controls: CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY LIGHTING | ESSENTIAL MISSION AND BUSINESS FUNCTIONS

Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

Discussion: Organizations define their essential missions and functions.

Related Controls: None.

References: None.

PE-13 FIRE PROTECTION

Control: Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

Employ fire detection systems that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of

information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(2) FIRE PROTECTION | SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

(a) Employ fire suppression systems that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*]; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Discussion: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

[Withdrawn: Incorporated into PE-13(2).]

(4) FIRE PROTECTION | INSPECTIONS

Ensure that the facility undergoes [*Assignment: organization-defined frequency*] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [*Assignment: organization-defined time period*].

Discussion: Authorized and qualified personnel within the jurisdiction of the organization include state, county, and city fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Related Controls: None.

References: None.

PE-14 ENVIRONMENTAL CONTROLS

Control:

a. Maintain [*Selection (one or more): temperature; humidity; pressure; radiation;* [*Assignment: organization-defined environmental control*]] levels within the facility where the system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitor environmental control levels [*Assignment: organization-defined frequency*].

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls: AT-3, CP-2.

Control Enhancements:

(1) ENVIRONMENTAL CONTROLS | AUTOMATIC CONTROLS

Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [*Assignment: organization-defined automatic environmental controls*].

Discussion: The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Related Controls: None.

(2) ENVIRONMENTAL CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [*Assignment: organization-defined personnel or roles*].

Discussion: The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Related Controls: None.

References: None.

PE-15 WATER DAMAGE PROTECTION

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

Detect the presence of water near the system and alert [*Assignment: organization-defined personnel or roles*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include notification systems, water detection sensors, and alarms.

Related Controls: None.

References: None.

PE-16 DELIVERY AND REMOVAL

Control:

a. Authorize and control [*Assignment: organization-defined types of system components*] entering and exiting the facility; and

b. Maintain records of the system components.

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

Control Enhancements: None.

References: None.

PE-17 ALTERNATE WORK SITE

Control:

a. Determine and document the [*Assignment: organization-defined alternate work sites*] allowed for use by employees;

b. Employ the following controls at alternate work sites: [*Assignment: organization-defined controls*];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

Control Enhancements: None.

References: [SP 800-46].

PE-18 LOCATION OF SYSTEM COMPONENTS

Control: Position system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls: CP-2, PE-5, PE-19, PE-20, RA-3.

(1) LOCATION OF SYSTEM COMPONENTS | FACILITY SITE

[Withdrawn: Moved to PE-23.]

References: None.

PE-19 INFORMATION LEAKAGE

Control: Protect the system from information leakage due to electromagnetic signals emanations.

Discussion: Information leakage is the intentional or unintentional release of data or information to an untrusted environment from electromagnetic signals emanations. The security categories

or classifications of systems (with respect to confidentiality), organizational security policies, and risk tolerance guide the selection of controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Related Controls: AC-18, PE-18, PE-20.

Control Enhancements:

(1) INFORMATION LEAKAGE | NATIONAL EMISSIONS POLICIES AND PROCEDURES

Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.

Discussion: Emissions Security (EMSEC) policies include the former TEMPEST policies.

Related Controls: None.

References: [FIPS 199].

PE-20 ASSET MONITORING AND TRACKING

Control: Employ [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*].

Discussion: Asset location technologies can help ensure that critical assets—including vehicles, equipment, and system components—remain in authorized locations. Organizations consult with the Office of the General Counsel and senior agency official for privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.

Related Controls: CM-8, PE-16, PM-8.

Control Enhancements: None.

References: None.

PE-21 ELECTROMAGNETIC PULSE PROTECTION

Control: Employ [*Assignment: organization-defined protective measures*] against electromagnetic pulse damage for [*Assignment: organization-defined systems and system components*].

Discussion: An electromagnetic pulse (EMP) is a short burst of electromagnetic energy that is spread over a range of frequencies. Such energy bursts may be natural or man-made. EMP interference may be disruptive or damaging to electronic equipment. Protective measures used to mitigate EMP risk include shielding, surge suppressors, ferro-resonant transformers, and earth grounding. EMP protection may be especially significant for systems and applications that are part of the U.S. critical infrastructure.

Related Controls: PE-18, PE-19.

Control Enhancements: None.

References: None.

PE-22 COMPONENT MARKING

Control: Mark [*Assignment: organization-defined system hardware components*] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

Discussion: Hardware components that may require marking include input and output devices. Input devices include desktop and notebook computers, keyboards, tablets, and smart phones. Output devices include printers, monitors/video displays, facsimile machines, scanners, copiers, and audio devices. Permissions controlling output to the output devices are addressed in AC-3 or AC-4. Components are marked to indicate the impact level or classification level of the system to which the devices are connected, or the impact level or classification level of the information permitted to be output. Security marking refers to the use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Security marking is generally not required for hardware components that process, store, or transmit information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components that process, store, or transmit public information in order to indicate that such information is publicly releasable. Marking of system hardware components reflects applicable laws, executive orders, directives, policies, regulations, and standards.

Related Controls: AC-3, AC-4, AC-16, MP-3.

Control Enhancements: None.

References: [IR 8023].

PE-23 FACILITY LOCATION

Control:

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

Related Controls: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

References: None.

3.12 PLANNING

Quick link to Planning Summary Table

PL-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-18], [SP 800-30], [SP 800-39], [SP 800-100].

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

Control:

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [*Assignment: organization-defined individuals or groups*]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [*Assignment: organization-defined personnel or roles*];

c. Review the plans [*Assignment: organization-defined frequency*];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Discussion: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section 2.1 describes the different types of requirements that are

relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related Controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.

Control Enhancements:

(1) SYSTEM SECURITY AND PRIVACY PLANS | CONCEPT OF OPERATIONS

[Withdrawn: Incorporated into PL-7.]

(2) SYSTEM SECURITY AND PRIVACY PLANS | FUNCTIONAL ARCHITECTURE

[Withdrawn: Incorporated into PL-8.]

(3) SYSTEM SECURITY AND PRIVACY PLANS | PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

[Withdrawn: Incorporated into PL-2.]

References: [OMB A-130], [SP 800-18], [SP 800-37], [SP 800-160-1], [SP 800-160-2].

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2.]

PL-4 RULES OF BEHAVIOR

Control:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior [*Assignment: organization-defined frequency*]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [*Selection (one or more):* [*Assignment: organization-defined frequency*]; *when the rules are revised or updated*].

Discussion: Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Related Controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Discussion: Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls: AC-22, AU-13.

References: [OMB A-130], [SP 800-18].

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into RA-8.]

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2.]

PL-7 CONCEPT OF OPERATIONS

Control:

a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and

b. Review and update the CONOPS [*Assignment: organization-defined frequency*].

Discussion: The CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents. The CONOPS is a living document that requires updating throughout the system development life cycle. For example, during system design reviews, the concept of operations is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development life cycle documents, and systems engineering documents.

Related Controls: PL-2, SA-2, SI-12.

Control Enhancements: None.

References: [OMB A-130].

PL-8 SECURITY AND PRIVACY ARCHITECTURES

Control:

a. Develop security and privacy architectures for the system that:

   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

   3. Describe how the architectures are integrated into and support the enterprise architecture; and

   4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [*Assignment: organization-defined frequency*] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Discussion: The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-7, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can

also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

[SP 800-160-1] provides guidance on the use of security architectures as part of the system development life cycle process. [OMB M-19-03] requires the use of the systems security engineering concepts described in [SP 800-160-1] for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

Control Enhancements:

(1) SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH

Design the security and privacy architectures for the system using a defense-in-depth approach that:

(a) Allocates [*Assignment: organization-defined controls*] to [*Assignment: organization-defined locations and architectural layers*]; and

(b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

Discussion: Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and

cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC-3).

Related Controls: SC-2, SC-3, SC-29, SC-36.

(2) SECURITY AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY

Require that [*Assignment: organization-defined controls*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

Discussion: Information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By deploying different products at different locations, there is an increased likelihood that at least one of the products will detect the malicious code. With respect to privacy, vendors may offer products that track personally identifiable information in systems. Products may use different tracking methods. Using multiple products may result in more assurance that personally identifiable information is inventoried.

Related Controls: SC-29, SR-3.

References: [OMB A-130], [SP 800-160-1], [SP 800-160-2].

PL-9 CENTRAL MANAGEMENT

Control: Centrally manage [*Assignment: organization-defined controls and related processes*].

Discussion: Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Related Controls: PL-8, PM-9.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37].

PL-10 BASELINE SELECTION

Control: Select a control baseline for the system.

Discussion: Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in [SP 800-53B]. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in [SP 800-53B] are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. [CNSSI 1253] provides guidance on control baselines for national security systems.

Related Controls: PL-2, PL-11, RA-2, RA-3, SA-8.

Control Enhancements: None.

References: [FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253].

PL-11 BASELINE TAILORING

Control: Tailor the selected control baseline by applying specified tailoring actions.

Discussion: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA], [PRIVACT], and [OMB A-130]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8.

Control Enhancements: None.

References: [FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253].

3.13 PROGRAM MANAGEMENT

PROGRAM MANAGEMENT CONTROLS

[FISMA], [PRIVACT], and [OMB A-130] require federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal information systems and to protect individual privacy. The program management (PM) controls described in this section are implemented at the organization level and not directed at individual information systems. The PM controls have been designed to facilitate organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards. The controls are independent of [FIPS 200] impact levels and, therefore, are not associated with the control baselines described in [SP 800-53B].

Organizations document program management controls in the information security and privacy program plans. The organization-wide information security program plan (see PM-1) and privacy program plan (see PM-18) supplement system security and privacy plans (see PL-2) developed for organizational information systems. Together, the system security and privacy plans for the individual information systems and the information security and privacy program plans cover the totality of security and privacy controls employed by the organization.

Quick link to Program Management Summary Table

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control:

a. Develop and disseminate an organization-wide information security program plan that:

   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

   3. Reflects the coordination among organizational entities responsible for information security; and

   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Review and update the organization-wide information security program plan [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

c. Protect the information security program plan from unauthorized disclosure and modification.

Discussion: An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program

and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-2, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level, and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Control Enhancements: None.

References: [FISMA], [OMB A-130], [SP 800-37], [SP 800-39].

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

Control: Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Discussion: The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

Related Controls: None.

Control Enhancements: None.

References: [OMB M-17-25], [SP 800-37], [SP 800-39], [SP 800-181].

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

Control:

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

Discussion: Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

Related Controls: PM-4, SA-2.

Control Enhancements: None.

References: [OMB A-130].

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

   1. Are developed and maintained;

   2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

   3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-5.

Related Controls: CA-5, CA-7, PM-3, RA-7, SI-12.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [SP 800-37].

PM-5 SYSTEM INVENTORY

Control: Develop and update [*Assignment: organization-defined frequency*] an inventory of organizational systems.

Discussion: [OMB A-130] provides guidance on developing systems inventories and associated reporting requirements. System inventory refers to an organization-wide inventory of systems, not system components as described in CM-8.

Related Controls: None.

Control Enhancements:

(1) SYSTEM INVENTORY | INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Establish, maintain, and update [*Assignment: organization-defined frequency*] an inventory of all systems, applications, and projects that process personally identifiable information.

Discussion: An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

Related Controls: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

References: [OMB A-130], [IR 8062].

PM-6 MEASURES OF PERFORMANCE

Control: Develop, monitor, and report on the results of information security and privacy measures of performance.

Discussion: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

Related Controls: CA-7, PM-9.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-55], [SP 800-137].

PM-7 ENTERPRISE ARCHITECTURE

Control: Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Discussion: The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and the organization's security and privacy architectures consistent with the organizational risk management strategy. For PM-7, security and privacy architectures are developed at a system-of-systems level, representing all organizational

systems. For PL-8, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework [SP 800-37] and supporting security standards and guidelines.

Related Controls: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Control Enhancements:

(1) ENTERPRISE ARCHITECTURE | OFFLOADING

Offload [*Assignment: organization-defined non-essential functions or services*] to other systems, system components, or an external provider.

Discussion: Not every function or service that a system provides is essential to organizational mission or business functions. Printing or copying is an example of a non-essential but supporting service for an organization. Whenever feasible, such supportive but non-essential functions or services are not co-located with the functions or services that support essential mission or business functions. Maintaining such functions on the same system or system component increases the attack surface of the organization's mission-essential functions or services. Moving supportive but non-essential functions to a non-critical system, system component, or external provider can also increase efficiency by putting those functions or services under the control of individuals or providers who are subject matter experts in the functions or services.

Related Controls: SA-8.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-160-1], [SP 800-160-2].

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Control Enhancements: None.

References: [EO 13636], [OMB A-130], [HSPD 7], [DHS NIPP].

PM-9 RISK MANAGEMENT STRATEGY

Control:

a. Develops a comprehensive strategy to manage:

   1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and

   2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Discussion: An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

Related Controls: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Control Enhancements: None.

References: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-161], [IR 8023].

PM-10 AUTHORIZATION PROCESS

Control:

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

Discussion: Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Related Controls: CA-6, CA-7, PL-2.

Control Enhancements: None.

References: [SP 800-37], [SP 800-39], [SP 800-181].

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

Control:

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes [*Assignment: organization-defined frequency*].

Discussion: Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Related Controls: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Control Enhancements: None.

References: [OMB A-130], [FIPS 199],[SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1].

PM-12 INSIDER THREAT PROGRAM

Control: Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Discussion: Organizations that handle classified information are required, under Executive Order 13587 [EO 13587] and the National Insider Threat Policy [ODNI NITP], to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of controlled unclassified and other information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from offices in the department or agency for insider threat analysis, and conduct self-assessments of department or agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The

participation of a legal team, including consultation with the senior agency official for privacy, ensures that monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.

Control Enhancements: None.

References: [EO 13587], [NITP12], [ODNI NITP].

PM-13 SECURITY AND PRIVACY WORKFORCE

Control: Establish a security and privacy workforce development and improvement program.

Discussion: Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Related Controls: AT-2, AT-3.

Control Enhancements: None.

References: [OMB A-130], [SP 800-181].

PM-14 TESTING, TRAINING, AND MONITORING

Control:

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

   1. Are developed and maintained; and

   2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related Controls: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137].

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

Control: Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

Discussion: Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: SA-11, SI-5.

Control Enhancements: None.

References: [OMB A-130].

PM-16 THREAT AWARENESS PROGRAM

Control: Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Discussion: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information, including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

Related Controls: IR-4, PM-12.

Control Enhancements:

(1) THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Discussion: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-

established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Related Controls: None.

References: None.

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

Control:

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and

b. Review and update the policy and procedures [*Assignment: organization-defined frequency*].

Discussion: Controlled unclassified information is defined by the National Archives and Records Administration along with the safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002] and, specifically for systems external to the federal organization, 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes.

Related Controls: CA-6, PM-10.

Control Enhancements: None.

References: [32 CFR 2002], [SP 800-171], [SP 800-172], [NARA CUI].

PM-18 PRIVACY PROGRAM PLAN

Control:

a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:

   1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

   2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

   3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;

   4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;

   5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and

   6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

b. Update the plan [*Assignment: organization-defined frequency*] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

Discussion: A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management, common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization.

Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

Related Controls: PM-8, PM-9, PM-19.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130].

PM-19 PRIVACY PROGRAM LEADERSHIP ROLE

Control: Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Discussion: The privacy officer is an organizational official. For federal agencies—as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines—this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has roles on the data management board (see PM-23) and the data integrity board (see PM-24).

Related Controls: PM-18, PM-20, PM-23, PM-24, PM-27.

Control Enhancements: None.

References: [OMB A-130].

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control: Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

Discussion: For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, [PRIVACT] exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

Related Controls: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

Control Enhancements:

(1) DISSEMINATION OF PRIVACY PROGRAM INFORMATION | PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

(a) Are written in plain language and organized in a way that is easy to understand and navigate;

(b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

(c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Discussion: Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: None.

References: [PRIVACT], [OMB A-130], [OMB M-17-06].

PM-21 ACCOUNTING OF DISCLOSURES

Control:

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

1. Date, nature, and purpose of each disclosure; and

2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Discussion: The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the [PRIVACT]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

Related Controls: AC-3, AU-2, PT-2.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130].

PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT

Control: Develop and document organization-wide policies and procedures for:

a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;

b. Correcting or deleting inaccurate or outdated personally identifiable information;

c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

Discussion: Personally identifiable information quality management includes steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. Organizations consider creating policies and procedures for the removal of such information.

The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information. Processes for correcting or deleting data are clearly defined and publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means

to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.

Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

Related Controls: PM-23, SI-18.

Control Enhancements: None.

References: [OMB A-130], [OMB M-19-15], [SP 800-188].

PM-23 DATA GOVERNANCE BODY

Control: Establish a Data Governance Body consisting of [*Assignment: organization-defined roles*] with [*Assignment: organization-defined responsibilities*].

Discussion: A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personally identifiable information across the information life cycle as well as reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the [EVIDACT] and policies set forth under [OMB M-19-23].

Related Controls: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.

Control Enhancements: None.

References: [EVIDACT], [OMB A-130], [OMB M-19-23], [SP 800-188].

PM-24 DATA INTEGRITY BOARD

Control: Establish a Data Integrity Board to:

a. Review proposals to conduct or participate in a matching program; and

b. Conduct an annual review of all matching programs in which the agency has participated.

Discussion: A Data Integrity Board is the board of senior officials designated by the head of a federal agency and is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records from two or more automated [PRIVACT] systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior agency official for privacy.

Related Controls: AC-4, PM-19, PM-23, PT-2, PT-8.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [OMB A-108].

PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Control:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures [*Assignment: organization-defined frequency*].

Discussion: The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Related Controls: PM-23, PT-3, SA-3, SA-8, SI-12.

Control Enhancements: None.

References: [OMB A-130].

PM-26 COMPLAINT MANAGEMENT

Control: Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [*Assignment: organization-defined time period*];

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [*Assignment: organization-defined time period*]; and

e. Response to complaints, concerns, or questions from individuals within [*Assignment: organization-defined time period*].

Discussion: Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

Related Controls: IR-7, IR-9, PM-22, SI-18.

Control Enhancements: None.

References: [OMB A-130].

PM-27 PRIVACY REPORTING

Control:

a. Develop [*Assignment: organization-defined privacy reports*] and disseminate to:

   1. [*Assignment: organization-defined oversight bodies*] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

   2. [*Assignment: organization-defined officials*] and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports [*Assignment: organization-defined frequency*].

Discussion: Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Related Controls: IR-9, PM-19.

Control Enhancements: None.

References: [FISMA], [OMB A-130], [OMB A-108].

PM-28 RISK FRAMING

Control:

a. Identify and document:

   1. Assumptions affecting risk assessments, risk responses, and risk monitoring;

   2. Constraints affecting risk assessments, risk responses, and risk monitoring;

   3. Priorities and trade-offs considered by the organization for managing risk; and

   4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to [*Assignment: organization-defined personnel*]; and

c. Review and update risk framing considerations [*Assignment: organization-defined frequency*].

Discussion: Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information

owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Related Controls: CA-7, PM-9, RA-3, RA-7.

Control Enhancements: None.

References: [OMB A-130], [SP 800-39].

PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

Control:

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

Discussion: The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Related Controls: PM-2, PM-19.

Control Enhancements: None.

References: [SP 800-37], [SP 800-181].

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Control:

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management strategy consistently across the organization; and

c. Review and update the supply chain risk management strategy on [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Discussion: An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-2) is implemented at the system level.

Related Controls: CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT STRATEGY | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Discussion: The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-6) and supply chain risk assessment processes (see RA-3(1)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-3, SR-6.

References: [PRIVACT], [FASC18], [EO 13873], [41 CFR 201], [OMB A-130], [OMB M-17-06] [CNSSD 505], [ISO 27036], [ISO 20243], [SP 800-161], [IR 8272].

PM-31 CONTINUOUS MONITORING STRATEGY

Control: Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: [*Assignment: organization-defined metrics*];

b. Establishing [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessment of control effectiveness;

c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Discussion: Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6,

PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

References: [SP 800-37], [SP 800-39], [SP 800-137], [SP 800-137A].

PM-32 PURPOSING

Control: Analyze [*Assignment: organization-defined systems or systems components*] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Discussion: Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Related Controls: CA-7, PL-2, RA-3, RA-9.

Control Enhancements: None.

References: [SP 800-160-1], [SP 800-160-2].

3.14 PERSONNEL SECURITY

Quick link to Personnel Security Summary Table

PS-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] personnel security policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

PS-2 POSITION RISK DESIGNATION

Control:

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [*Assignment: organization-defined frequency*].

Discussion: Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Control Enhancements: None.

References: [5 CFR 731], [SP 800-181].

PS-3 PERSONNEL SCREENING

Control:

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening*].

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Control Enhancements:

(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION

Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Discussion: Classified information is the most sensitive information that the Federal Government processes, stores, or transmits. It is imperative that individuals have the requisite security clearances and system access authorizations prior to gaining access to such

information. Access authorizations are enforced by system access controls (see AC-3) and flow controls (see AC-4).

Related Controls: AC-3, AC-4.

(2) PERSONNEL SCREENING | FORMAL INDOCTRINATION

Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

Discussion: Types of classified information that require formal indoctrination include Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartmented Information (SCI).

Related Controls: AC-3, AC-4.

(3) PERSONNEL SCREENING | INFORMATION REQUIRING SPECIAL PROTECTIVE MEASURES

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Discussion: Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.

Related Controls: None.

(4) PERSONNEL SCREENING | CITIZENSHIP REQUIREMENTS

Verify that individuals accessing a system processing, storing, or transmitting [*Assignment: organization-defined information types*] meet [*Assignment: organization-defined citizenship requirements*].

Discussion: None.

Related Controls: None.

References: [EO 13526], [EO 13587], [FIPS 199], [FIPS 201-2], [SP 800-60-1], [SP 800-60-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

PS-4 PERSONNEL TERMINATION

Control: Upon termination of individual employment:

a. Disable system access within [*Assignment: organization-defined time period*];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

Discussion: System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including

in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Control Enhancements:

(1) PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS

(a) Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

(b) Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Discussion: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: None.

(2) PERSONNEL TERMINATION | AUTOMATED ACTIONS

Use [*Assignment: organization-defined automated mechanisms*] to [*Selection (one or more): notify* [*Assignment: organization-defined personnel or roles*] *of individual termination actions*; *disable access to system resources*].

Discussion: In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.

Related Controls: None.

References: None.

PS-5 PERSONNEL TRANSFER

Control:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within

organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Control Enhancements: None.

References: None.

PS-6 ACCESS AGREEMENTS

Control:

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [*Assignment: organization-defined frequency*]; and

c. Verify that individuals requiring access to organizational information and systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Discussion: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

Control Enhancements:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Incorporated into PS-3.]

(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

Verify that access to classified information requiring special protection is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria; and

(c) Have read, understood, and signed a nondisclosure agreement.

Discussion: Classified information that requires special protection includes collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: None.

(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS

(a) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

(b) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Discussion: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: PS-4.

References: None.

PS-7 EXTERNAL PERSONNEL SECURITY

Control:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [*Assignment: organization-defined time period*]; and

e. Monitor provider compliance with personnel security requirements.

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Control Enhancements: None.

References: [SP 800-35], [SP 800-63-3].

PS-8 PERSONNEL SANCTIONS

Control:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion: Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls: All XX-1 Controls, PL-4, PM-12, PS-6, PT-1.

Control Enhancements: None.

References: None.

PS-9 POSITION DESCRIPTIONS

Control: Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Related Controls: None.

Control Enhancements: None.

References: [SP 800-181].

3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

Quick link to Personally Identifiable Information Processing and Transparency table

PT-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] personally identifiable information processing and transparency policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings, breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: None.

Control Enhancements: None.

References: [OMB A-130].

PT-2 AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION

Control:

a. Determine and document the [*Assignment: organization-defined authority*] that permits the [*Assignment: organization-defined processing*] of personally identifiable information; and

b. Restrict the [*Assignment: organization-defined processing*] of personally identifiable information to only that which is authorized.

Discussion: The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, [PRIVACT] statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.

Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

Related Controls: AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

Control Enhancements:

(1) AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | DATA TAGGING

Attach data tags containing [*Assignment: organization-defined authorized processing*] to [*Assignment: organization-defined elements of personally identifiable information*].

Discussion: Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of

personally identifiable information throughout the system. Data tags may also support the use of automated tools.

Related Controls: AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | AUTOMATION

Manage enforcement of the authorized processing of personally identifiable information using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms augment verification that only authorized processing is occurring.

Related Controls: CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

References: [PRIVACT], [OMB A-130], [IR 8112].

PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES

Control:

a. Identify and document the [*Assignment: organization-defined purpose(s)*] for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the [*Assignment: organization-defined processing*] of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement [*Assignment: organization-defined mechanisms*] to ensure that any changes are made in accordance with [*Assignment: organization-defined requirements*].

Discussion: Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization's privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, [PRIVACT] statements, computer matching notices, and other applicable Federal Register notices.

Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

Related Controls: AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18.

Control Enhancements:

(1) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | DATA TAGGING

Attach data tags containing the following purposes to [*Assignment: organization-defined elements of personally identifiable information*]: [*Assignment: organization-defined processing purposes*].

Discussion: Data tags support the tracking of processing purposes by conveying the purposes along with the relevant elements of personally identifiable information throughout the system. By conveying the processing purposes in a data tag along with the personally identifiable information as the information transits a system, a system owner or operator can identify whether a change in processing would be compatible with the identified and documented purposes. Data tags may also support the use of automated tools.

Related Controls: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION

Track processing purposes of personally identifiable information using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms augment tracking of the processing purposes.

Related Controls: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

References: [PRIVACT], [OMB A-130], [IR 8112].

PT-4 CONSENT

Control: Implement [*Assignment: organization-defined tools or mechanisms*] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

Discussion: Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.

Related Controls: AC-16, PT-2, PT-5.

Control Enhancements:

(1) CONSENT | TAILORED CONSENT

Provide [*Assignment: organization-defined mechanisms*] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.

Discussion: While some processing may be necessary for the basic functionality of the product or service, other processing may not. In these circumstances, organizations allow individuals to select how specific personally identifiable information elements may be processed. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviors, such as abandonment of the product or service.

Related Controls: PT-2.

(2) CONSENT | JUST-IN-TIME CONSENT

Present [*Assignment: organization-defined consent mechanisms*] to individuals at [*Assignment: organization-defined frequency*] and in conjunction with [*Assignment: organization-defined personally identifiable information processing*].

Discussion: Just-in-time consent enables individuals to participate in how their personally identifiable information is being processed at the time or in conjunction with specific types of data processing when such participation may be most useful to the individual. Individual assumptions about how personally identifiable information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or the type of processing creates significant privacy risk. Organizations use discretion to determine when to use just-in-time consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.

Related Controls: PT-2.

(3) CONSENT | REVOCATION

Implement [*Assignment: organization-defined tools or mechanisms*] for individuals to revoke consent to the processing of their personally identifiable information.

Discussion: Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations consider usability factors in enabling easy-to-use revocation capabilities.

Related Controls: PT-2.

References: [PRIVACT], [OMB A-130], [SP 800-63-3].

PT-5 PRIVACY NOTICE

Control: Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at [*Assignment: organization-defined frequency*];

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes [*Assignment: organization-defined information*].

Discussion: Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide

privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

Related Controls: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.

Control Enhancements:

(1) PRIVACY NOTICE | JUST-IN-TIME NOTICE

Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [*Assignment: organization-defined frequency*].

Discussion: Just-in-time notices inform individuals of how organizations process their personally identifiable information at a time when such notices may be most useful to the individuals. Individual assumptions about how personally identifiable information will be processed might not be accurate or reliable if time has passed since the organization last presented notice or the circumstances under which the individual was last provided notice have changed. A just-in-time notice can explain data actions that organizations have identified as potentially giving rise to greater privacy risk for individuals. Organizations can use a just-in-time notice to update or remind individuals about specific data actions as they occur or highlight specific changes that occurred since last presenting notice. A just-in-time notice can be used in conjunction with just-in-time consent to explain what will occur if consent is declined. Organizations use discretion to determine when to use a just-in-time notice and may use supporting information on user demographics, focus groups, or surveys to learn about users' privacy interests and concerns.

Related Controls: PM-21.

(2) PRIVACY NOTICE | PRIVACY ACT STATEMENTS

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Discussion: If a federal agency asks individuals to supply information that will become part of a system of records, the agency is required to provide a [PRIVACT] statement on the form used to collect the information or on a separate form that can be retained by the individual. The agency provides a [PRIVACT] statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.

[PRIVACT] statements provide formal notice to individuals of the authority that authorizes the solicitation of the information; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant system of records notice. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding the notice provisions of the [PRIVACT].

Related Controls: PT-6.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [OMB A-108].

PT-6 SYSTEM OF RECORDS NOTICE

Control: For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;

b. Publish system of records notices in the Federal Register; and

c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

Discussion: The [PRIVACT] requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a [PRIVACT] system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in [OMB A-108].

Related Controls: AC-3, PM-20, PT-2, PT-3, PT-5.

Control Enhancements:

(1) SYSTEM OF RECORDS NOTICE | ROUTINE USES

Review all routine uses published in the system of records notice at [*Assignment: organization-defined frequency*] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

Discussion: A [PRIVACT] routine use is a particular kind of disclosure of a record outside of the federal agency maintaining the system of records. A routine use is an exception to the [PRIVACT] prohibition on the disclosure of a record in a system of records without the prior written consent of the individual to whom the record pertains. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The [PRIVACT] requires agencies to describe each routine use of the records maintained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses by explicitly publishing them in the relevant system of records notice.

Related Controls: None.

(2) SYSTEM OF RECORDS NOTICE | EXEMPTION RULES

Review all Privacy Act exemptions claimed for the system of records at [*Assignment: organization-defined frequency*] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

Discussion: The [PRIVACT] includes two sets of provisions that allow federal agencies to claim exemptions from certain requirements in the statute. In certain circumstances, these provisions allow agencies to promulgate regulations to exempt a system of records from select provisions of the [PRIVACT]. At a minimum, organizations' [PRIVACT] exemption

regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the [PRIVACT] from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.

Related Controls: None.

References: [PRIVACT], [OMB A-108].

PT-7 SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION

Control: Apply [*Assignment: organization-defined processing conditions*] for specific categories of personally identifiable information.

Discussion: Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

Related Controls: IR-9, PT-2, PT-3, RA-3.

Control Enhancements:

(1) SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | SOCIAL SECURITY NUMBERS

When a system processes Social Security numbers:

(a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

(b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Discussion: Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.

Related Controls: IA-4.

(2) SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | FIRST AMENDMENT INFORMATION

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Discussion: The [PRIVACT] limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding these requirements.

Related Controls: None.

References: [PRIVACT], [OMB A-130], [OMB A-108], [NARA CUI].

PT-8 COMPUTER MATCHING REQUIREMENTS

Control: When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;

c. Publish a matching notice in the Federal Register;

d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Discussion: The [PRIVACT] establishes requirements for federal and non-federal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated [PRIVACT] systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to federal benefit programs or federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any.

Related Controls: PM-24.

Control Enhancements: None.

References: [PRIVACT], [CMPPA], [OMB A-130], [OMB A-108].

3.16 RISK ASSESSMENT

Quick link to Risk Assessment Summary Table

RA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] risk assessment policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

RA-2 SECURITY CATEGORIZATION

Control:

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. [CNSSI 1253] provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with [USA PATRIOT] and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

Control Enhancements:

(1) SECURITY CATEGORIZATION | IMPACT-LEVEL PRIORITIZATION

Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

Discussion: Organizations apply the "high-water mark" concept to each system categorized in accordance with [FIPS 199], resulting in systems designated as low impact, moderate impact, or high impact. Organizations that desire additional granularity in the system impact designations for risk-based decision-making, can further partition the systems into sub-categories of the initial system categorization. For example, an impact-level prioritization on a moderate-impact system can produce three new sub-categories: low-moderate systems, moderate-moderate systems, and high-moderate systems. Impact-level prioritization and the resulting sub-categories of the system give organizations an opportunity to focus their investments related to security control selection and the tailoring of control baselines in responding to identified risks. Impact-level prioritization can also be used to determine those systems that may be of heightened interest or value to adversaries or represent a critical loss to the federal enterprise, sometimes described as high value assets. For such high value assets, organizations may be more focused on complexity, aggregation, and information exchanges. Systems with high value assets can be prioritized by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems.

Alternatively, organizations can apply the guidance in [CNSSI 1253] for security objective-related categorization.

Related Controls: None.

References: [FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253], [NARA CUI].

RA-3 RISK ASSESSMENT

Control:

a. Conduct a risk assessment, including:

   1. Identifying threats to and vulnerabilities in the system;

   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [*Selection: security and privacy plans; risk assessment report;* [*Assignment: organization-defined document*]];

d. Review risk assessment results [*Assignment: organization-defined frequency*];

e. Disseminate risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

f. Update the risk assessment [*Assignment: organization-defined frequency*] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Discussion: Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related Controls: CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.

Control Enhancements:

(1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT

(a) Assess supply chain risks associated with [*Assignment: organization-defined systems, system components, and system services*]; and

(b) Update the supply chain risk assessment [*Assignment: organization-defined frequency*], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Discussion: Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-2, RA-9, PM-17, PM-30, SR-2.

(2) RISK ASSESSMENT | USE OF ALL-SOURCE INTELLIGENCE

Use all-source intelligence to assist in the analysis of risk.

Discussion: Organizations employ all-source intelligence to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of information derived from all available sources, including publicly available or open-source information, measurement and signature intelligence, human intelligence, signals intelligence, and imagery intelligence. All-source intelligence is used to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. The risk analysis may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.

Related Controls: None.

(3) RISK ASSESSMENT | DYNAMIC THREAT AWARENESS

Determine the current cyber threat environment on an ongoing basis using [*Assignment: organization-defined means*].

Discussion: The threat awareness information that is gathered feeds into the organization's information security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations may change the privilege or authentication thresholds required to perform certain operations.

Related Controls: AT-2.

(4) RISK ASSESSMENT | PREDICTIVE CYBER ANALYTICS

Employ the following advanced automation and analytics capabilities to predict and identify risks to [*Assignment: organization-defined systems or system components*]: [*Assignment: organization-defined advanced automation and analytics capabilities*].

Discussion: A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and analytics capabilities are typically supported by artificial intelligence concepts, including machine learning. Examples include Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine assisted decision tools. Note, however, that sophisticated adversaries may be able

to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

Related Controls: None.

References: [OMB A-130], [SP 800-30], [SP 800-39], [SP 800-161], [IR 8023], [IR 8062], [IR 8272].

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3.]

RA-5 VULNERABILITY MONITORING AND SCANNING

Control:

a. Monitor and scan for vulnerabilities in the system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability

monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as "bug bounties") to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

Control Enhancements:

(1) VULNERABILITY MONITORING AND SCANNING | UPDATE TOOL CAPABILITY

[Withdrawn: Incorporated into RA-5.]

(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED

Update the system vulnerabilities to be scanned [*Selection (one or more):* [*Assignment: organization-defined frequency*]*; prior to a new scan; when new vulnerabilities are identified and reported*].

Discussion: Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls: SI-5.

(3) VULNERABILITY MONITORING AND SCANNING | BREADTH AND DEPTH OF COVERAGE

Define the breadth and depth of vulnerability scanning coverage.

Discussion: The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element).

Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. [SP 800-53A] provides additional information on the breadth and depth of coverage.

Related Controls: None.

(4) VULNERABILITY MONITORING AND SCANNING | DISCOVERABLE INFORMATION

Determine information about the system that is discoverable and take [*Assignment: organization-defined corrective actions*].

Discussion: Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

Related Controls: AU-13, SC-26.

(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS

Implement privileged access authorization to [*Assignment: organization-defined system components*] for [*Assignment: organization-defined vulnerability scanning activities*].

Discussion: In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls: None.

(6) VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES

Compare the results of multiple vulnerability scans using [*Assignment: organization-defined automated mechanisms*].

Discussion: Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.

Related Controls: None.

(7) VULNERABILITY MONITORING AND SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS

[Withdrawn: Incorporated into CM-8.]

(8) VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS

Review historic audit logs to determine if a vulnerability identified in a [*Assignment: organization-defined system*] has been previously exploited within an [*Assignment: organization-defined time period*].

Discussion: Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the trade craft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

Related Controls: AU-6, AU-11.

(9) VULNERABILITY MONITORING AND SCANNING | PENETRATION TESTING AND ANALYSES

[Withdrawn: Incorporated into CA-8.]

(10) VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

Discussion: An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation.

Related Controls: None.

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion: The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Related Controls: None.

References: [ISO 29147], [SP 800-40], [SP 800-53A], [SP 800-70], [SP 800-115], [SP 800-126], [IR 7788], [IR 8011-4], [IR 8023].

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Control: Employ a technical surveillance countermeasures survey at [*Assignment: organization-defined locations*] [*Selection (one or more):* [*Assignment: organization-defined frequency*]; when the following events or indicators occur: [*Assignment: organization-defined events or indicators*]].

Discussion: A technical surveillance countermeasures survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could be used in the conduct of a technical penetration of the surveyed facility. Technical surveillance countermeasures surveys also provide evaluations of the technical security posture of organizations and facilities and include visual, electronic, and physical examinations of surveyed facilities, internally and externally. The surveys also provide useful input for risk assessments and information regarding organizational exposure to potential adversaries.

Related Controls: None.

Control Enhancements: None.

References: None.

RA-7 RISK RESPONSE

Control: Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Discussion: Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Related Controls: CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.

Control Enhancements: None.

References: [FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-160-1].

RA-8 PRIVACY IMPACT ASSESSMENTS

Control: Conduct privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and

b. Initiating a new collection of personally identifiable information that:

   1. Will be processed using information technology; and

   2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Discussion: A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analysis and a formal document that details the process and the outcome of the analysis.

Organizations conduct and develop a privacy impact assessment with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization's activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization's senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel. Moreover, a privacy impact assessment is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization's practices, or other factors alter the privacy risks associated with the use of such information technology.

To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes that may have different names,

including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization's practices with respect to privacy. Although conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable laws. For federal agencies, privacy impact assessments may be required by [EGOV]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Related Controls: CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.

Control Enhancements: None.

References: [EGOV], [OMB A-130], [OMB M-03-22].

RA-9 CRITICALITY ANALYSIS

Control: Identify critical system components and functions by performing a criticality analysis for [*Assignment: organization-defined systems, system components, or system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Discussion: Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls: CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.

Control Enhancements: None.

References: [IR 8179].

RA-10 THREAT HUNTING

Control:

a. Establish and maintain a cyber threat hunting capability to:

   1. Search for indicators of compromise in organizational systems; and

   2. Detect, track, and disrupt threats that evade existing controls; and

b. Employ the threat hunting capability [*Assignment: organization-defined frequency*].

Discussion: Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

Related Controls: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Control Enhancements: None.

References: [SP 800-30].

3.17 SYSTEM AND SERVICES ACQUISITION

Quick link to System and Services Acquisition Summary Table

SA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] system and services acquisition policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SA-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [SP 800-160-1].

SA-2 ALLOCATION OF RESOURCES

Control:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Discussion: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls: PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37], [SP 800-160-1].

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Control:

a. Acquire, develop, and manage the system using [*Assignment: organization-defined system development life cycle*] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Discussion: A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition

and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.

Control Enhancements:

(1) SYSTEM DEVELOPMENT LIFE CYCLE | MANAGE PREPRODUCTION ENVIRONMENT

Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

Discussion: The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense are examples of managing the preproduction environment for defense contractors. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

Related Controls: CM-2, CM-4, RA-3, RA-9, SA-4.

(2) SYSTEM DEVELOPMENT LIFE CYCLE | USE OF LIVE OR OPERATIONAL DATA

(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

(b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

Discussion: Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to organizations. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data. Organizations can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.

Related Controls: PM-25, RA-3.

(3) SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH

Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

Discussion: Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development life cycle.

Related Controls: MA-6.

References: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-160-1], [SP 800-171], [SP 800-172].

SA-4 ACQUISITION PROCESS

Control: Include the following requirements, descriptions, and criteria, explicitly or by reference, using [*Selection (one or more): standardized contract language;* [*Assignment: organization-defined contract language*]] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Discussion: Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160-1] describes the process of requirements engineering as part of the system development life cycle.

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 for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, 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 controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related Controls: None.

(2) ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;* [*Assignment: organization-defined design and implementation information*]] at [*Assignment: organization-defined level of detail*].

Discussion: Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related Controls: None.

(3) ACQUISITION PROCESS | DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES

Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:

(a) **[*Assignment: organization-defined systems engineering methods*];**

(b) **[*Assignment: organization-defined* [*Selection (one or more): systems security; privacy*] *engineering methods*]; and**

(c) **[*Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes*].**

Discussion: Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Transparency in the methods and techniques that developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes provides an increased level of assurance in the trustworthiness of the system, system component, or system service being acquired.

Related Controls: None.

(4) ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS

[Withdrawn: Incorporated into CM-8(9).]

(5) ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS

Require the developer of the system, system component, or system service to:

(a) Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Discussion: Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Related Controls: None.

(6) ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS

(a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

(b) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

Discussion: Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. See [NSA CSFC].

Related Controls: SC-8, SC-12, SC-13.

(7) ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES

(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and

(b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.

Discussion: See [NIAP CCEVS] for additional information on NIAP. See [NIST CMVP] for additional information on FIPS-validated cryptographic modules.

Related Controls: IA-7, SC-12, SC-13.

(8) ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

Discussion: The objective of continuous monitoring plans is to determine if the planned, required, and deployed controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into continuous monitoring programs implemented by organizations. Continuous monitoring plans can include the types of control assessment and monitoring

activities planned, frequency of control monitoring, and actions to be taken when controls fail or become ineffective.

Related Controls: CA-7.

(9) ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls: CM-7, SA-9.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Discussion: Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Related Controls: IA-2, IA-8, PM-9.

(11) ACQUISITION PROCESS | SYSTEM OF RECORDS

Include [*Assignment: organization-defined Privacy Act requirements*] in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.

Discussion: When, by contract, an organization provides for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirements of the [PRIVACT] to be applied to the system of records.

Related Controls: PT-6.

(12) ACQUISITION PROCESS | DATA OWNERSHIP

(a) Include organizational data ownership requirements in the acquisition contract; and

(b) Require all data to be removed from the contractor's system and returned to the organization within [*Assignment: organization-defined time frame*].

Discussion: Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a time frame defined by the contract.

Related Controls: None.

References: [PRIVACT], [OMB A-130], [ISO 15408-1], [ISO 15408-2], [ISO 15408-3], [ISO 29148], [FIPS 140-3], [FIPS 201-2], [SP 800-35], [SP 800-37], [SP 800-70], [SP 800-73-4], [SP 800-137], [SP 800-160-1], [SP 800-161], [IR 7539], [IR 7622], [IR 7676], [IR 7870], [IR 8062], [NIAP CCEVS], [NSA CSFC].

SA-5 SYSTEM DOCUMENTATION

Control:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security and privacy functions and mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

   1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

   3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [*Assignment: organization-defined actions*] in response; and

d. Distribute documentation to [*Assignment: organization-defined personnel or roles*].

Discussion: System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

Control Enhancements:

(1) SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

[Withdrawn: Incorporated into SA-4(1).]

(2) SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES

[Withdrawn: Incorporated into SA-4(2).]

(3) SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN

[Withdrawn: Incorporated into SA-4(2).]

(4) SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN

[Withdrawn: Incorporated into SA-4(2).]

(5) SYSTEM DOCUMENTATION | SOURCE CODE

[Withdrawn: Incorporated into SA-4(2).]

References: [SP 800-160-1].

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7.]

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7.]

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Control: Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [*Assignment: organization-defined systems security and privacy engineering principles*].

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

Related Controls: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5.

Control Enhancements:

(1) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CLEAR ABSTRACTIONS

Implement the security design principle of clear abstractions.

Discussion: The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces—

combined with a precise definition of their functional behavior—promotes ease of analysis, inspection, and testing as well as the correct and secure use of the system. The clarity of an abstraction is subjective. Examples that reflect the application of this principle include avoidance of redundant, unused interfaces; information hiding; and avoidance of semantic overloading of interfaces or their parameters. Information hiding (i.e., representation-independent programming), is a design discipline used to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

Related Controls: None.

(2) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST COMMON MECHANISM

Implement the security design principle of least common mechanism in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized [POPEK74]. Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource. Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security [SALTZER75]. Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing the system state among different programs. A single program that corrupts a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels [LAMPSON73].

Related Controls: None.

(3) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MODULARITY AND LAYERING

Implement the security design principles of modularity and layering in [*Assignment: organization-defined systems or system components*].

Discussion: The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle. Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy. Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.

Related Controls: SC-2, SC-3.

(4) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PARTIALLY ORDERED DEPENDENCIES

Implement the security design principle of partially ordered dependencies in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally

related modules or components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers. While providing functionality to higher layers, some layers can be self-contained and not dependent on lower layers. While a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed. Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.

Related Controls: None.

(5) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | EFFICIENTLY MEDIATED ACCESS

Implement the security design principle of efficiently mediated access in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system. Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, by using hardware mechanisms, efficiently mediated access can be achieved. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.

Related Controls: AC-25.

(6) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SHARING

Implement the security design principle of minimized sharing in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation. In order to protect user-domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid performance and covert storage and timing channel problems. Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be reentrant or virtualized to preserve separation. Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.

Related Controls: SC-31.

(7) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REDUCED COMPLEXITY

Implement the security design principle of reduced complexity in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more analyzable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be

successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain; that is, simpler systems contain fewer vulnerabilities. An benefit of reduced complexity is that it is easier to understand whether the intended security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and the existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex. Transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6) may require implementing the older and newer technologies simultaneously during the transition period. This may result in a temporary increase in system complexity during the transition.

Related Controls: None.

(8) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE EVOLVABILITY

Implement the security design principle of secure evolvability in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system's structure, interfaces, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or upgraded system capability; maintenance and sustainment activities; and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage. A system may be secure in some new contexts, but there is no guarantee that its emergent behavior will always be secure. It is easier to build trustworthiness into a system from the outset, and it follows that the sustainment of system trustworthiness requires planning for change as opposed to adapting in an ad hoc or non-methodical manner. The benefits of this principle include reduced vendor life cycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.

Related Controls: CM-3.

(9) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMPONENTS

Implement the security design principle of trusted components in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of trusted components states that a component is trustworthy to at least a level commensurate with the security dependencies it supports (i.e., how much it is trusted to perform its security functions by other components). This principle enables the composition of components such that trustworthiness is not inadvertently diminished and the trust is not consequently misplaced. Ultimately, this principle demands some metric by which the trust in a component and the trustworthiness of a component can be measured on the same abstract scale. The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships.

The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption. However, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth layering within the component or a replication of components. Defense-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

Related Controls: None.

(10) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL TRUST

Implement the security design principle of hierarchical trust in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or an assurance case (assurance argument) when composing a secure system from heterogeneously trustworthy components. To analyze a system composed of heterogeneously trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If a more trustworthy component located in a lower layer of the system were to depend on a less trustworthy component in a higher layer, this would, in effect, put the components in the same "less trustworthy" equivalence class per the principle of trusted components. Trust relationships, or chains of trust, can have various manifestations. For example, the root certificate of a certificate hierarchy is the most trusted node in the hierarchy, whereas the leaves in the hierarchy may be the least trustworthy nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware base), which is located at the lowest layer of the system, is the most trustworthy component. The principle of hierarchical trust, however, does not prohibit the use of overly trustworthy components. There may be cases in a system of low trustworthiness where it is reasonable to employ a highly trustworthy component rather than one that is less trustworthy (e.g., due to availability or other cost-benefit driver). For such a case, any dependency of the highly trustworthy component upon a less trustworthy component does not degrade the trustworthiness of the resulting low-trust system.

Related Controls: None.

(11) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | INVERSE MODIFICATION THRESHOLD

Implement the security design principle of inverse modification threshold in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of inverse modification threshold builds on the principle of trusted components and the principle of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component also increases to the same degree. Protection from unauthorized modification can come in the form of the component's own self-protection and innate trustworthiness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).

Related Controls: None.

(12) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL PROTECTION

Implement the security design principle of hierarchical protection in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel. The trustworthiness of users is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in "system high" environments where users are highly trustworthy and where other protections are put in place to bound and protect the "system high" execution environment.

Related Controls: None.

(13) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SECURITY ELEMENTS

Implement the security design principle of minimized security elements in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of minimized security elements states that the system does not have extraneous trusted components. The principle of minimized security elements has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally costlier to construct and implement, owing to the increased rigor of development processes. Trusted components require greater security analysis to qualify their trustworthiness. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. The analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to ascertain than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.

Related Controls: None.

(14) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST PRIVILEGE

Implement the security design principle of least privilege in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has need to view the audit data that has been collected but no need to perform operations on that data.

In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are

directly operated on by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality and that the access modes for the elements (e.g., read, write) are minimal.

Related Controls: AC-6, CM-7.

(15) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PREDICATE PERMISSION

Implement the security design principle of predicate permission in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed. [SALTZER75] originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects. The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires two different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.

Related Controls: AC-5.

(16) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-RELIANT TRUSTWORTHINESS

Implement the security design principle of self-reliant trustworthiness in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection. The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.

Related Controls: None.

(17) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DISTRIBUTED COMPOSITION

Implement the security design principle of secure distributed composition in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a stand-alone to a distributed system or a system-of-systems can have unexpected or emergent results. Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a

system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.

Related Controls: None.

(18) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMMUNICATIONS CHANNELS

Implement the security design principle of trusted communications channels in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the communication channel (to protect against interception and modification and to further increase the assurance of proper end-to-end communication).

Related Controls: SC-8, SC-12, SC-13.

(19) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CONTINUOUS PROTECTION

Implement the security design principle of continuous protection in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurances that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown). Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to protect itself from tampering; and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing) and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternative operational modes).

Continuous protection also applies to systems designed to operate in varying configurations, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational need that drives the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state). Insufficient traceability and verification may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of life cycle protection needs as stakeholder security requirements.

Related Controls: AC-25.

(20) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE METADATA MANAGEMENT

Implement the security design principle of secure metadata management in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure metadata management states that metadata are "first class" objects with respect to security policy when the policy requires either complete protection of information or that the security subsystem be self-protecting. The principle of secure metadata management is driven by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies on for correct execution. Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it comprises information) to users and programs that process the data. In contrast, metadata is information about data, such as a file name or the date when the file was created. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the classification level or impact level of a file name), including self-referential metadata.

The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labeled or indirectly attributed with sensitivity levels. The corollary of labeled metadata for MLS systems states that objects containing metadata are labeled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.

Related Controls: None.

(21) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-ANALYSIS

Implement the security design principle of self-analysis in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of trustworthiness invested in the system. At the system level, self-analysis can be achieved through hierarchical assessments of trustworthiness established in a bottom-up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher-level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established. At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity. Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Related Controls: CA-7.

(22) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCOUNTABILITY AND TRACEABILITY

Implement the security design principle of accountability and traceability in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. The principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem). To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that are carried out. The accountability policy also requires that audit trail itself be protected from unauthorized access and modification. The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serves is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy and the actions of individuals associated with the violation of the security policy.

Related Controls: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

(23) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DEFAULTS

Implement the security design principle of secure defaults in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that follow a "deny unless explicitly authorized" strategy. The initial configuration aspect of this principle requires that any "as shipped" configuration of a system, subsystem, or system component does not aid in the violation of the security policy and can prevent the system from operating in the default configuration for those cases where the security policy itself requires configuration by the operational user.

Restrictive defaults mean that the system will operate "as-shipped" with adequate self-protection and be able to prevent security breaches before the intended security policy and system configuration is established. In cases where the protection provided by the "as-shipped" product is inadequate, stakeholders assess the risk of using it prior to establishing a secure initial state. Adherence to the principle of secure defaults guarantees that a system is established in a secure state upon successfully completing initialization. In situations where the system fails to complete initialization, either it will perform a requested operation using secure defaults or it will not perform the operation. Refer to the principles of continuous protection and secure failure and recovery that parallel this principle to provide the ability to detect and recover from failure.

The security engineering approach to this principle states that security mechanisms deny requests unless the request is found to be well-formed and consistent with the security policy. The insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.

Related Controls: CM-2, CM-6, SA-4.

(24) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE FAILURE AND RECOVERY

Implement the security design principle of secure failure and recovery in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated.

Failure is a condition in which the behavior of a component deviates from its specified or expected behavior for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration.

Another technique that can be used to recover from failures is to perform a rollback to a secure state (which may be the initial state) and then either shutdown or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access. For example, a nominally "atomic" operation interrupted before completion does not violate security policy and is designed to handle interruption events by employing higher-level atomicity and rollback mechanisms (e.g., transactions). If a service is being used, its atomicity properties are well-documented and characterized so that the component availing itself of that service can detect and handle interruption events appropriately. For example, a system is designed to gracefully respond to disconnection and support resynchronization and data consistency after disconnection.

Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defense in depth, can allow the system to continue in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services. By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance. Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviors. Increased complexity generally reduces trustworthiness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.

Related Controls: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.

(25) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ECONOMIC SECURITY

Implement the security design principle of economic security in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence as well as the necessary analyses to assess and draw trustworthiness and risk conclusions from the evidence.

Related Controls: RA-3.

(26) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PERFORMANCE SECURITY

Implement the security design principle of performance security in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat.

The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Related Controls: SC-12, SC-13, SI-2, SI-7.

(27) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HUMAN FACTORED SECURITY

Implement the security design principle of human factored security in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to

understand the impact of their choices. Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.

Related Controls: None.

(28) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCEPTABLE SECURITY

Implement the security design principle of acceptable security in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users' expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.

Related Controls: None.

(29) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REPEATABLE AND DOCUMENTED PROCEDURES

Implement the security design principle of repeatable and documented procedures in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use. In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and documented procedures can be introduced at various stages within the system development life cycle and contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.

Related Controls: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

(30) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PROCEDURAL RIGOR

Implement the security design principle of procedural rigor in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of unspecified functionality is prevented.

Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand

the system as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification.

Finally, modifications to an existing system component are easier when there are detailed specifications that describe its current design instead of studying source code or schematics to try to understand how it works. Procedural rigor helps ensure that security functional and assurance requirements have been satisfied, and it contributes to a better-informed basis for the determination of trustworthiness and risk posture. Procedural rigor is commensurate with the degree of assurance desired for the system. If the required trustworthiness of the system is low, a high level of procedural rigor may add unnecessary cost, whereas when high trustworthiness is critical, the cost of high procedural rigor is merited.

Related Controls: None.

(31) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE SYSTEM MODIFICATION

Implement the security design principle of secure system modification in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any system changes. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is needed prior to its implementation and deployment. This principle parallels the principle of secure evolvability.

Related Controls: CM-3, CM-4.

(32) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SUFFICIENT DOCUMENTATION

Implement the security design principle of sufficient documentation in [*Assignment: organization-defined systems or system components*].

Discussion: The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to rather than detract from system security. Despite attempts to comply with principles such as human factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always intuitively obvious. Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection. Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.

Related Controls: AT-2, AT-3, SA-5.

(33) SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZATION

Implement the privacy principle of minimization using [*Assignment: organization-defined processes*].

Discussion: The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

Related Controls: PE-8, PM-25, SC-42, SI-12.

References: [PRIVACT], [OMB A-130], [FIPS 199], [FIPS 200], [SP 800-37], [SP 800-53A], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [IR 8062].

SA-9 EXTERNAL SYSTEM SERVICES

Control:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [*Assignment: organization-defined controls*];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [*Assignment: organization-defined processes, methods, and techniques*].

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

Control Enhancements:

(1) EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS

(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

Discussion: Information security services include the operation of security devices, such as firewalls or key management services as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

Related Controls: CA-6, RA-3, RA-8.

(2) EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [*Assignment: organization-defined external system services*].

Discussion: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls: CM-6, CM-7.

(3) EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [*Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships*].

Discussion: Trust relationships between organizations and external service providers reflect the degree of confidence that the risk from using external services is at an acceptable level. Trust relationships can help organizations gain increased levels of confidence that service providers are providing adequate protection for the services rendered and can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the potentially large number of entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control that organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements.

Related Controls: SR-2.

(4) EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

Take the following actions to verify that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests: [*Assignment: organization-defined actions*].

Discussion: As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations. Actions that organizations take to address such concerns include requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, such as providers with which organizations have had successful trust relationships; and conducting routine, periodic, unscheduled visits to service provider facilities.

Related Controls: None.

(5) EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION

Restrict the location of [*Selection (one or more): information processing; information or data; system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Discussion: The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria that organizations use. For example, organizations may desire that data or information storage