Draft NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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

INFORMATION SECURITY

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

Draft NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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

July 2020

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 800-53B
Natl. Inst. Stand. Technol. Spec. Publ. 800-53B, **85 pages** (July 2020)

CODEN: NSPUE2

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

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.

Public comment period: July 31, 2020 through September 11, 2020

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 security and privacy control baselines for the Federal Government. There are three security control baselines for low-impact, moderate-impact, and high-impact information systems as well as a privacy baseline that is applied to systems irrespective of impact level. In addition to the control baselines, this publication provides tailoring guidance and a set of working assumptions that help guide and inform the control selection process for organizations. Finally, this publication provides guidance on the development of overlays to facilitate control baseline customization for specific communities of interest, technologies, and environments of operation.

Keywords

Assurance; impact level; privacy control; privacy control baseline; security control; security control baseline; tailoring; control selection; control overlays.

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

John W. Wilmer
Deputy CIO for Cybersecurity and DoD SISO

Kevin Dulany
Director, Cybersecurity Policy and Partnerships

Office of the Director of National Intelligence

La'nala Jones
Acting Chief Information Officer

Vacant
Deputy Chief Information Officer

Ben Phelps
Acting Director, Cybersecurity Division and 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*	McKay Tolboe *DoD*	Dorian Pappas *Intelligence Community*	Kelley Dempsey *NIST*
Ehijele Olumese *The MITRE Corporation*	Lydia Humphries *Booz Allen Hamilton*	Daniel Faigin *Aerospace Corporation*	Naomi Lefkovitz *NIST*
Esten Porter *The MITRE Corporation*	Julie Snyder *The MITRE Corporation*	Christina Sames *The MITRE Corporation*	Christian Enloe *NIST*
David Black *The MITRE Corporation*	Rich Graubart *The MITRE Corporation*	Peter Duspiva *Intelligence Community*	Kaitlin Boeckl *NIST*
Eduardo Takamura *NIST*	Ned Goren *NIST*	Andrew Regenscheid *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 the professional staff from the NIST Computer Security Division and the Applied Cybersecurity Division and the input from representatives from the Federal CIO Council and Interagency Working Group for their contributions in helping to improve the technical content of the publication. Finally, the authors gratefully acknowledge the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose insightful and constructive comments improved the quality, thoroughness, and usefulness of this publication.

Notes to Reviewers

NIST Special Publication (SP) 800-53B has been developed to provide security and privacy control baselines for the Federal Government. These control baselines had previously been published in NIST SP 800-53 [SP 800-53]. The control baselines were moved to a separate publication so that SP 800-53 could serve as a consolidated catalog of security and privacy controls regardless of how those controls were used by different communities of interest. NIST SP 800-37, Revision 2 [SP 800-37] (i.e., *Risk Management Framework*), provides two distinct approaches for control selection. The first approach uses the control baselines and tailoring process described in this publication. The second approach uses a systems development life cycle requirements engineering process to generate security and privacy requirements, which in turn guide and inform the selection of controls to satisfy the requirements. This organization-defined control selection approach also supports the use of other security, privacy, and risk frameworks (e.g., the Cybersecurity Framework, Privacy Framework). Thus, different user communities can use the same consolidated catalog of security and privacy controls to meet their specific security and privacy needs within the context of whatever control selection process or framework the organization desires to use.

The security and privacy control baselines have been updated with the controls described in SP 800-53, Revision 5. The content of the control baselines reflects the results of a comprehensive interagency review conducted during the summer of 2017. The control baselines also reflect the continuing input and analyses of threat data and empirical cyber-attack data collected since the last update to [SP 800-53].

In addition to your feedback on the three security control baselines, NIST is also seeking your comments on the privacy control baseline and the privacy control baseline selection criteria. SInce the selection of the privacy control baseline is based on a mapping of the controls and control enhancements in [SP 800-53] to the privacy program responsibilities under OMB Circular A-130 [OMB A-130], suggested changes to the privacy control baseline must be supported by a reference to [OMB A-130]. Alternatively, you may provide a description and rationale for new or modified privacy control baseline selection criteria.

Your feedback on this draft publication is important to us. We appreciate each contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape the final publication to ensure that it meets the needs and expectations of our customers.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sec-cert@nist.gov.

172

COMPLIANCE AND DUE DILIGENCE

Compliance requires that organizations exercise *due diligence* regarding information security and privacy risk management. Security and privacy due diligence requires organizations to establish a comprehensive risk management program, that, in part, uses the flexibility 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 system to operate, and continuously monitor the system. Risk management frameworks and processes are essential in developing, implementing, and maintaining the protection measures that are 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 missions and business functions, U.S. critical infrastructure, and continuity of government.

173

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 in establishing a Risk Management Framework for information security and privacy for the Federal Government. This common foundation provides the Federal Government and its contractors 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 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.

174

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.

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 entitled, *Task Force on Cyber Deterrence* [DSB 2017], the Defense Science Board provides a sobering assessment of the current vulnerabilities in the U.S. critical infrastructure and the information systems that support the 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 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.

NIST SP 800-53B responds to the call by the Defense Science Board by providing a proactive and systemic approach to developing and making available to federal agencies and private sector organizations a comprehensive set of security and privacy control baselines for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud-based systems, mobile devices, and industrial and process control systems. The control baselines provide a starting point for organizations in the security and privacy control selection process. Using the tailoring guidance and assumptions provided, organizations can customize their security and privacy control baselines to ensure that they have the capability to protect their critical and essential operations and assets. The ultimate objective is to make the 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.

Errata

This table contains changes that have been incorporated into Special Publication 800-53B. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	REVISION	PAGE

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY AND PRIVACY CONTROL BASELINES

Security controls are the safeguards or countermeasures selected and implemented within an information system[1] or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk. Privacy controls are the administrative, technical, and physical safeguards employed within a system or an organization to ensure compliance with applicable privacy requirements and to manage privacy risks.[2] Security and privacy controls are selected and implemented to satisfy the security and privacy requirements levied on an information system and/or organization. The 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 effective implementation of controls are important tasks that have significant implications for the operations and assets of organizations as well as the welfare of individuals and the Nation.

NIST Special Publication (SP) 800-37 [SP 800-37] defines two approaches for the selection of security and privacy controls: a *baseline* control selection approach and an *organization-generated* control selection approach. The baseline control selection approach uses control baselines, which are predefined sets of controls specifically assembled to meet the protection needs of a group, organization, or community of interest. The control baselines serve as a starting point for the protection of individuals' privacy, information, and information systems. The organization-generated control selection approach is not addressed in this publication.

1.1 PURPOSE AND APPLICABILITY

This publication establishes security and privacy control baselines for federal information systems[3] and organizations and provides tailoring guidance for those baselines. The use of the security control baselines is mandatory, in accordance with OMB Circular A-130 [OMB A-130] and the provisions of the Federal Information Security Modernization Act[4] [FISMA], which requires the implementation of a set of minimum controls to protect federal information and information systems. Whereas use of the privacy control baseline is not mandated by law or [OMB A-130], SP 800-53B, along with other supporting NIST publications, is designed to help

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

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

[3] 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.

[4] 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. CNSS Policy No. 22 [CNSSP 22] and CNSS Instruction No. 1253 [CNSSI 1253] provide guidance for *national security systems*. DoD Instruction 8510.01 [DODI 8510.01] provides guidance for the Department of Defense.

organizations identify the security and privacy controls needed to manage risk and satisfy the security and privacy requirements in FISMA, the Privacy Act of 1974 [PRIVACT], selected OMB policies (e.g., [OMB A-130]), and designated Federal Information Processing Standards (FIPS), among others.[5] The publication accomplishes this objective by providing security and privacy control baselines as a starting point to meet the protection needs of organizations. The controls can be implemented within any organization or information system that processes, stores, or transmits information. The controls in the baselines are tailored following the process described in Section 2.4 to further facilitate the management of security and privacy risk specific to the organization. The tailoring process can be guided and informed by many factors, including organizational mission and business needs, stakeholder protection needs, and assessments of risk. The combination of control baseline selection and control tailoring processes can help organizations satisfy their stated security and privacy requirements.

SECURITY AND PRIVACY CONTROL BASELINES

Security and privacy control baselines are predefined sets of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest. The control baselines serve as a starting point for the protection of individuals' privacy, information, and information systems and can be tailored (i.e., customized)—appropriately taking into account organizational missions and business functions, specific and credible threat information, the environment in which the organization operates, and individuals' privacy interests.

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, system security or privacy officers

[5] While the control baselines established in this publication are designed 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 baselines, as appropriate.

- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts
- Commercial entities, including industry partners, who produce component products and systems and develop security and privacy technologies

1.3 ORGANIZATIONAL RESPONSIBILITIES

Organizations have the responsibility to choose a control selection approach in accordance with [SP 800-37].[6] If the baseline control selection approach is chosen, organizations select a security control baseline and privacy control baseline as described in Chapter Three. Once the control baseline is selected, organizations apply the tailoring guidance provided in Chapter Two to help ensure the resulting controls are necessary and sufficient to manage security risk[7] and privacy risk.[8]

1.4 RELATIONSHIP TO OTHER PUBLICATIONS

This publication establishes security and privacy control baselines derived from the controls in NIST SP 800-53 [SP 800-53]. The control baselines in this publication are in accordance with requirements for federal information and information systems included in [OMB A-130],[9] Federal Information Processing Standard 199 [FIPS 199], and Federal Information Processing Standard 200 [FIPS 200]. [SP 800-37] provides guidance on control selection approaches.

1.5 REVISIONS AND EXTENSIONS

The security and privacy controls specified in the baselines represent the state-of-the-practice protection measures for individuals, information systems, and organizations. The controls comprising the baselines are periodically reviewed and revised 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, attacks, and information processing methods; and the availability of new technologies. Thus, the security and privacy controls specified in the baselines 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 changes to the baseline undergo a rigorous and transparent public review process to obtain public and private sector feedback and to build a consensus for baseline changes. The public review process provides a stable, flexible, and technically sound set of security and privacy control baselines.

[6] In the *baseline* control selection approach and *organization-generated* control selection approach, organizations develop a well-defined set of security and privacy requirements using a life cycle-based systems engineering process as described in the Risk Management Framework (RMF) *Prepare—System Level* step, Task P-15, *Requirements Definition*. This process generates a set of requirements that can be used to guide and inform the selection of controls to satisfy the requirements.

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

[8] [IR 8062] introduces privacy risk assessment concepts.

[9] [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.

1.6 PUBLICATION ORGANIZATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with control baselines, selecting the appropriate baseline, baseline assumptions, tailoring baselines, overlays, and capabilities.
- **Chapter Three** provides a set of tables organized by control family that contain the controls that comprise the low-impact, moderate-impact, and high-impact security control baselines as well as the privacy control baseline.
- A list of informative References[10] is provided after Chapter Three.
- Supporting appendices include:
  - **Appendix A:** Glossary;
  - **Appendix B:** Acronyms; and
  - **Appendix C**: Overlay Guidance.

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

CHAPTER TWO

THE FUNDAMENTALS

CONTROL BASELINES, TAILORING, OVERLAYS, AND CAPABILITIES

This chapter presents the fundamental concepts associated with security and privacy control baselines, including the purpose of control baselines, how control baselines are selected, assumptions associated with control baselines, how the tailoring process is used to customize controls and baselines, the purpose of overlays and how overlays are used to address the security and privacy needs of communities of interest, and how the concept of capabilities can facilitate the grouping of mutually reinforcing controls.

2.1 CONTROL BASELINES

A significant challenge for organizations is selecting a set of security and privacy controls which, if correctly implemented and determined to be effective, adequately responds to mission and business risk while complying with security and privacy requirements defined by applicable laws, Executive Orders, regulations, policies, and directives. There is no single set of controls that addresses all security and privacy concerns in every situation. However, choosing the most appropriate controls for a specific situation or system to adequately respond to risk requires a fundamental understanding of the organization's missions and business priorities, the mission and business functions that the systems will support, and the environments where the systems will operate. It also requires close collaboration with key organizational stakeholders. With that understanding, organizations can demonstrate how to effectively and cost-effectively assure the confidentiality, integrity, and availability of organizational information and systems as well as the privacy of individuals in the context of supporting the organization's mission and business functions.

The concept of a control *baseline* is introduced to assist organizations in selecting a set of controls for their systems that is commensurate with security and privacy risk. A control baseline is a collection of controls from [SP 800-53] assembled to address the protection needs of a group, organization, or community of interest.[11] The control baseline provides a generalized set of controls that represents an initial starting point for the subsequent tailoring activities that can be applied to the baseline to produce a targeted or customized security and privacy solution for the entity that it is intended to serve. The selection of controls for control baselines is based on a variety of factors, including sector-specific requirements, threat information, organizational assumptions and constraints, mission or business requirements, types of systems, operating environments, specific technologies, individuals' privacy interests, laws, Executive Orders, regulations, policies, directives, standards, or industry best practices. The control baselines are tailored or customized by each organization, sector, or individual company based on specific operating conditions and other factors. Tailoring activities are described in greater detail in Section 2.4.

[11] The U.S. Government, in accordance with the requirements set forth in [FISMA], [OMB A-130], and Federal Information Processing Standards, has established federally mandated security control baselines. The control baselines for non-national security systems are listed in [Chapter Three].

2.2 SELECTING CONTROL BASELINES

Information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) in order to provide confidentiality, integrity, and availability. Privacy programs are responsible for ensuring compliance with applicable privacy requirements and for managing the risks to individuals associated with the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as "processing") of personally identifiable information (PII).[12] When a system processes PII, the information security and privacy programs have a shared responsibility to manage the impacts to individuals that arise from security risks and collaborate to determine the security catageorization and the selection and tailoring of controls from the security control baselines.

Security Control Baselines

In preparation for selecting and tailoring the appropriate security control baselines for organizational systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. The process of determining information criticality and sensitivity is known as *security categorization* and is described in [FIPS 199].[13] The results of security categorization help guide and inform the selection of security control baselines to protect systems and information. The control baselines selected for systems are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, or the Nation if there is a loss of confidentiality, integrity, or availability. [FIPS 199] requires organizations to categorize systems as low-impact, moderate-impact, or high-impact for the stated security objectives of confidentiality, integrity, and availability.[14]

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular system, the high water mark concept (introduced in [FIPS 199]) is used in [FIPS 200] to determine the impact level of the system. The impact level of the system, in turn, is used for the express purpose of selecting the applicable security control baseline from one of the three baselines identified in Chapter Three.[15] Thus, a *low-impact* system is defined as a system in which all three of the security objectives are low. A *moderate-impact* system is a system in which at least one of the security objectives is moderate and no security objective is high. Finally, a *high-impact* system is a system in which at least one security objective is high.

[12] Privacy programs may also choose to consider the risks to individuals that may arise from their interactions with information systems where the processing of PII 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.

[13] [CNSSI 1253] provides security categorization guidance for national security systems.

[14] NIST SP 800-60 (Volumes 1 and 2) [SP 800-60-1] [SP 800-60-2] provides guidance for the assignment of security categories to information systems. [SP 800-37] provides guidance for the specific tasks of the Risk Management Framework (RMF) Categorize step.

[15] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, security controls are not categorized by security objective. Rather, the security controls are grouped into baselines to provide a general protection capability for classes of information systems based on impact level.

Once the impact level of the system is determined, organizations select the appropriate security control baseline.[16] The selection of the security control baseline is based on the [FIPS 200] impact level of the information system as determined by the security categorization process described above. The organization selects one of three security control baselines from Chapter Three corresponding to the low-impact, moderate-impact, or high-impact categorization of the system. Note that not all controls or control enhancements are assigned to control baselines as indicated in the tables in Chapter Three. The controls and control enhancements that are assigned to baselines are indicated by an "**x"** in the low, moderate, or high columns in Tables 3-1 through 3-20. The use of the term control *baseline* is intentional. The controls and control enhancements in the baselines are a starting point from which controls/enhancements may be removed, added, or specialized based on the tailoring guidance in Section 2.4.[17]

Privacy Control Baseline

In addition to the three security control baselines, Chapter Three provides a privacy control baseline for federal agencies to address privacy requirements and manage privacy risks that arise from the *processing* of PII. The controls are selected from the set of controls and control enhancements in [SP 800-53].[18] The controls and control enhancements that are assigned to the privacy baseline are indicated by an "**x**". Whereas the selection of security controls for the security control baselines is based on an assessment of impact and the corresponding security categorization, as described above, the selection of privacy controls works differently. The selection of the privacy control baseline is based on a mapping of the controls and control enhancements in [SP 800-53] to the privacy program responsibilities under [OMB A-130]. This approach provides a starting point from which controls or control enhancements may be removed, added, or specialized based on the tailoring guidance in Section 2.4.[19] Organizations assess the applicable legal and policy requirements, and conduct privacy risk assessments, to guide the selection and implementation of these controls or enhancements in order to meet requirements and manage privacy risks.

A mapping between the privacy requirements in [OMB A-130] and the relevant controls from the control catalog in [SP 800-53] is provided on the NIST web site.[20] This mapping supports the implementation of the privacy requirements by federal agencies and nonfederal organizations that are required to meet such requirements based on federal contracts or other agreements. However, federal agencies should not assume that the implementation of the controls means

[16] The general control baseline selection process may be augmented or further detailed by additional sector-specific guidance as described in Appendix C, *Overlays*.

[17] Specialization refers to the modification of controls or control enhancements (including organization-defined parameters), or supplemental guidance to allow an organization to further refine the control baseline to address specific requirements, technologies, missions or business functions, or environments of operation. To address the need for specialized sets of controls for communities of interest, systems, and organizations, the *overlay* concept is introduced. For more information on overlays, see Appendix C.

[18] Privacy control enhancements in Tables 3-1 through 3-20 in Chapter Three cannot be selected and implemented without the selection and implementation of the associated base control. Such actions may require collaboration with security programs in cases where the security program has responsibility for the base control. Organizations ensure that the responsibility for the selection and implementation of controls is clearly defined between the information security and privacy programs.

[19] See footnote 17.

[20] See [NIST CSRC].

that they have met all of their obligations under [OMB A-130]. Agencies may need to take additional, separate steps to fully comply with OMB privacy requirements.

2.3 CONTROL BASELINE ASSUMPTIONS

The control baselines in Chapter Three address the protection needs of a diverse set of constituencies, including individual users and organizations. Thus, certain working *assumptions* generally underlie the control baselines in Chapter Three. These assumptions, made when determining the baselines in Chapter Three, consider the environments in which organizational information systems operate, including legislative, regulatory, or policy obligations; the nature of organizational operations; the specific functionality employed within the systems; the types of threats confronting organizations, missions/business processes, and systems; individuals' privacy interests; and the types of information processed, stored, or transmitted by systems. Articulating the underlying assumptions is a key element in the *Risk Framing* step of the risk management process described in NIST SP 800-39 [SP 800-39] and reinforced in the *Prepare* step in [SP 800-37]. Specific assumptions that underlie the control baselines in Chapter Three include:

- Organizational systems are located in physical facilities.
- Information in organizational systems is relatively persistent.[21]
- Organizational systems are multi-user (either serially or concurrently) in operation.
- Some information in organizational systems is not shareable with other users who have authorized access to the same systems.
- Organizational systems exist in networked environments, and are general purpose in nature.
- Organizations have the necessary structure, resources, and infrastructure to implement the controls.[22]

If any of the above assumptions are not valid, then some of the security controls allocated to the control baselines in Chapter Three may not be applicable—a situation that can be addressed by applying the tailoring guidance in Section 2.4 and the results of organization- and system-level risk assessments. Additional assumptions that are **not** addressed in the baselines include:

- Insider threats exist within organizations.
- Classified information is processed, stored, or transmitted by organizational systems.[23]
- Advanced persistent threats (APTs) exist within organizations.
- Information requires specialized protection based on legislation, directives, regulations, or policies.
- Organizational systems communicate with other systems across different security domains.

[21] Persistent data/information refers to data/information with utility for a relatively long duration (e.g., days, weeks).

[22] In general, federal departments and agencies satisfy this assumption. However, the assumption can become an issue for nonfederal entities, such as municipalities, first responders, and small businesses. Such entities may not be large enough or sufficiently resourced to have elements dedicated to providing the range of security or privacy capabilities that are assumed by the baselines. Organizations consider such factors in their risk-based decisions.

[23] See NIST SP 800-59 [SP 800-59] and CNSS Instruction 1253 [CNSSI 1253].

If any of these assumptions apply, then additional controls from [SP 800-53] are likely needed to ensure adequate protection—a situation that can also be effectively addressed by applying the tailoring guidance in Section 2.4 (specifically, security control supplementation) and the results of organization- and system-level assessments of risk.

2.4 TAILORING CONTROL BASELINES

After selecting an appropriate control baseline, organizations initiate a tailoring process to align the controls more closely with the specific security and privacy requirements identified by the organization.[24] The tailoring process is part of an organization-wide risk management process that includes framing, assessing, responding to, and monitoring information security and privacy risks. Tailoring decisions are not carried out in a vacuum. While tailoring decisions are focused on security and privacy considerations, the decisions are typically aligned with other risk-related issues that organizations must routinely address. Risk-related issues such as cost, schedule, and performance are considered in the determination of which controls to employ in organizational systems and environments of operation.[25] The tailoring process can include but is not limited to the following activities:[26]

- Identifying and designating common controls
- Applying scoping considerations
- Selecting compensating controls
- Assigning values to organization-defined control parameters via explicit assignment and selection statements
- Supplementing baselines with additional controls and control enhancements
- Providing specification information for control implementation

Organizations use risk management guidance to facilitate risk-based decision making regarding the applicability of the controls in the baselines. Ultimately, organizations employ the tailoring process to achieve cost-effective solutions that support organizational missions and business needs and provide security and privacy protections commensurate with risk.[27] Organizations have the flexibility to tailor at the organization level for systems in support of a line of business or mission/business process, at the individual system level, or by using a combination of the two. However, organizations do not arbitrarily remove security and privacy controls from baselines. Tailoring decisions are expected to be defensible based on mission and business needs, a sound rationale, and explicit risk-based determinations.[28]

[24] Some organizations may select security and privacy controls from [SP 800-53] without the use of control baselines. For example, organizations may choose their controls as part of a life cycle-based systems engineering process during the development of systems, system components, or system services.

[25] It is inappropriate to tailor out security or privacy controls that pertain to specific federal legislative, regulatory, or policy requirements.

[26] See Section 2.2, Privacy Control Baseline, for additional guidance on tailoring privacy controls.

[27] See [SP 800-37], Task P-4.

[28] Tailoring decisions can be based on the timing and applicability of selected controls under certain conditions. That is, security and privacy controls may not apply in every situation, or the parameter values for assignment statements may change under certain circumstances. Federal agencies conduct baseline tailoring activities in accordance with OMB policy. In certain situations, OMB may prohibit agencies from tailoring specific security or privacy controls.

Tailoring decisions, including the risk-based justification for the decisions, are documented in the system security and privacy plans for organizational systems.[29] Every control from the selected control baseline is accounted for by the organization. If certain controls are tailored out, the rationale is recorded in the system security and privacy plans and subsequently approved by the responsible officials within the organization as part of the approval process for the plans. Documenting risk management decisions during the baseline tailoring process is imperative for organizational officials to have the necessary information to make credible, risk-based decisions regarding security and privacy and to do so in a manner that fully supports transparency, traceability, and accountability.

Identifying and Designating Common Controls

Common controls are controls that may be inherited by one or more organizational systems. If a system inherits a common control provided by another entity (internal or external), there is no need to implement the control within that system. Organizational decisions on which controls are designated as common controls may affect the responsibilities of individual system owners with regard to the implementation of the controls in a baseline.[30] Common control providers ensure that current implementation information and assessment results are available to facilitate decision making by system owners and authorizing officials. System owners and authorizing officials determine if the common controls available for inheritance actually provide protection commensurate with risk for inheriting systems.[31]

Common control designation and control implementation can affect organizations' resource expenditures. That is, in general, the greater the number of common controls implemented, the greater the potential cost savings since the protective measures are amortized over many systems. Additionally, deployment of controls as common controls often provides a more standardized, stable, scalable, and secure implementation across the organization as opposed to the same control implemented separately on multiple individual systems.

Applying Scoping Considerations

Scoping considerations, when applied in conjunction with risk management guidance, provide organizations with a more granular foundation with which to make risk-based decisions.[32] The application of these scoping considerations can eliminate unnecessary controls from the initial control baselines and ensure that organizations select *only* those controls that are needed to provide a level of protection that is commensurate with risk. Organizations may apply the scoping considerations described below as needed to assist with making risk-based decisions regarding control selection and specification.

[29] [SP 800-18] provides guidance on developing system security plans. Guidance on developing privacy plans is forthcoming.

[30] See the *Organizational Prepare* Step, Task P-5, *Common Control Identification*, in [SP 800-37] for more information about organizational decisions on designating common controls.

[31] Organizations may also leverage the use of hybrid controls. Hybrid controls are controls that are partially implemented by one or more common control providers and partially implemented by the information system.

[32] The scoping considerations listed in this section are exemplary and *not* intended to limit organizations in rendering risk-based decisions based on other organization-defined considerations with appropriate justification or rationale.

- *Control Implementation, Applicability, and Placement Considerations*

The growing complexity of systems requires careful analysis in the implementation of security and privacy controls. Controls in the initial baselines may not be applicable to every component in the system. Controls are applicable only to system components that provide or support the security or privacy functions or capabilities addressed by the controls.[33] Organizations make explicit risk-based decisions about where to apply or allocate specific controls in organizational systems to achieve the needed security or privacy function or capability and to satisfy security and privacy requirements.

- *Operational and Environmental Considerations*

Certain controls in the control baselines assume the existence of operational or environmental factors. Where operational or environmental factors are absent or significantly diverge from the baseline assumptions described in Section 2.3, it is justifiable to tailor the baseline. Some of the more common operational and environmental factors include but are not limited to mobile devices and operations; single-user systems and operations; data connectivity and bandwidth; non-networked (i.e., air-gapped) systems; systems that have very limited or sporadic bandwidth such as tactical systems that support warfighter or law enforcement missions; cyber-physical systems, sensors, and Internet of Things (IoT) devices; limited functionality systems, such as facsimile machines, printers, scanners, and digital cameras; systems processing, storing, or transmitting non-persistent information or systems that employ virtualization techniques to establish non-persistent instantiations of operating systems and applications; and systems that require public access.

- *Technology Considerations*

Controls that refer to specific technologies—such as wireless, cryptography, or public key infrastructure—are applicable only if those technologies are implemented or are required for use within organizational systems. Controls that can be effectively supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. If automated mechanisms are not available, cost-effective, or technically feasible, compensating controls, implemented through nonautomated mechanisms or procedures, can be implemented to satisfy specified controls or control enhancements.

- *Mission and Business Considerations*

Certain controls may not be appropriate if implementing those controls has the potential to degrade, debilitate, or interfere with organizational missions or business functions, including endangering or harming individuals. However, decisions on the appropriateness of control implemention always consider legislative, regulatory, and/or policy requirements.

- *Legal and Policy Considerations*

Although controls that are used to meet legislative, regulatory, or policy requirements are not to be tailored out of control baselines, some legislative, regulatory, or policy requirements may only apply in specified circumstances. It is justifiable to tailor the baseline when these circumstances are not applicable to an organization or certain systems.

[33] For example, auditing controls are typically applied to components of a system that provide auditing capabilities and are not necessarily applied to every user-level component within the organization.

- *Security Objective Considerations*

Controls that support only one or two of the security objectives (i.e., confidentiality, integrity, or availability) may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) only if the downgrading action: reflects the [FIPS 199] security category for the supported security objectives before considering the [FIPS 200] impact level (i.e., high water mark); is supported by an organizational assessment of risk; and does not adversely affect the level of protection for the security-relevant information within the system. For example, if a system is categorized as moderate-impact using the high water mark concept because confidentiality and/or integrity are moderate but availability is low, there are several controls that only support the availability security objective and that could potentially be downgraded to the low baseline controls. In this scenario, it may be appropriate to refrain from implementing CP-2(1) because the control enhancement only supports availability and is selected in the moderate baseline but not in the low baseline. The following security controls and control enhancements are candidates for downgrading for each of the security categories:

- *Confidentiality:* AC-21, MA-3(3), MP-3, MP-4, MP-5, MP-6(1), MP-6(2), PE-4, PE-5, SC-4
- *Integrity:* CM-5, CM-5(1), CM-5(3), SI-7, SI-7(1), SI-7(5), SI-10
- *Availability:* CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-7(6), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-8(5), CP-9(2), CP-9(3), CP-9(5), CP-9(6), CP-10(2), CP-10(4), CP-11, MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-15(1)

Selecting Compensating Controls

Compensating controls are used by organizations in lieu of specific controls in control baselines. The use of compensating controls is appropriate when controls are tailored out of the control baseline by necessity, but the protection provided by the controls is still needed to reduce risk to an acceptable level. Compensating controls are often chosen when implementing a baseline control is technically infeasible, not cost effective, or the control implementation negatively affects organizational missions or business functions.[34] For technology-based scoping considerations, compensating controls are often temporary and used only until the system is updated. Compensating controls are intended to provide equivalent or comparable protection[35] for systems, organizations, and individuals.[36] Compensating controls are selected after applying the scoping considerations in the tailoring process. To use compensating controls, organizations:

- Select compensating controls from the control catalog in [SP 800-53].
- Provide a rationale for how compensating controls satisfy security or privacy requirements and why the baseline controls could not be implemented.

[34] For example, additional physical security controls may be implemented in lieu of a device lock in certain real-time mission or business applications. In a small organization, more frequent auditing, targeted role-based training, or stronger personnel screening may be implemented in lieu of separation of duties. Well-defined procedures, targeted role-based training, and more frequent auditing may be implemented in lieu of automated mechanisms.

[35] Compensating controls are not used to avoid the need to comply with requirements. Rather, the use of such controls provides alternative and suitable security and privacy protections to facilitate risk management.

[36] More than one compensating control may be required to provide the equivalent protection for a control that has been tailored out from a control baseline.

- Adopt suitable compensating controls from other sources if appropriate compensating controls are not available in [SP 800-53].[37]
- Assess and accept the security and privacy risks associated with implementing compensating controls.

Assigning Control Parameter Values

Controls and control enhancements containing embedded parameters (i.e., *assignment* and *selection* statements) give organizations the flexibility to specify values for certain portions of controls and control enhancements to support specific organizational requirements. After the application of scoping considerations and the selection of compensating controls, organizations review the controls and control enhancements for assignment or selection statements and determine the appropriate organization-defined values for the identified parameters. The parameter values may be driven by mission or business requirements or the values may be prescribed by laws, Executive Orders, directives, regulations, policies, standards, guidelines, or industry best practices. Figure 1 illustrates the concept of organization-defined parameters.

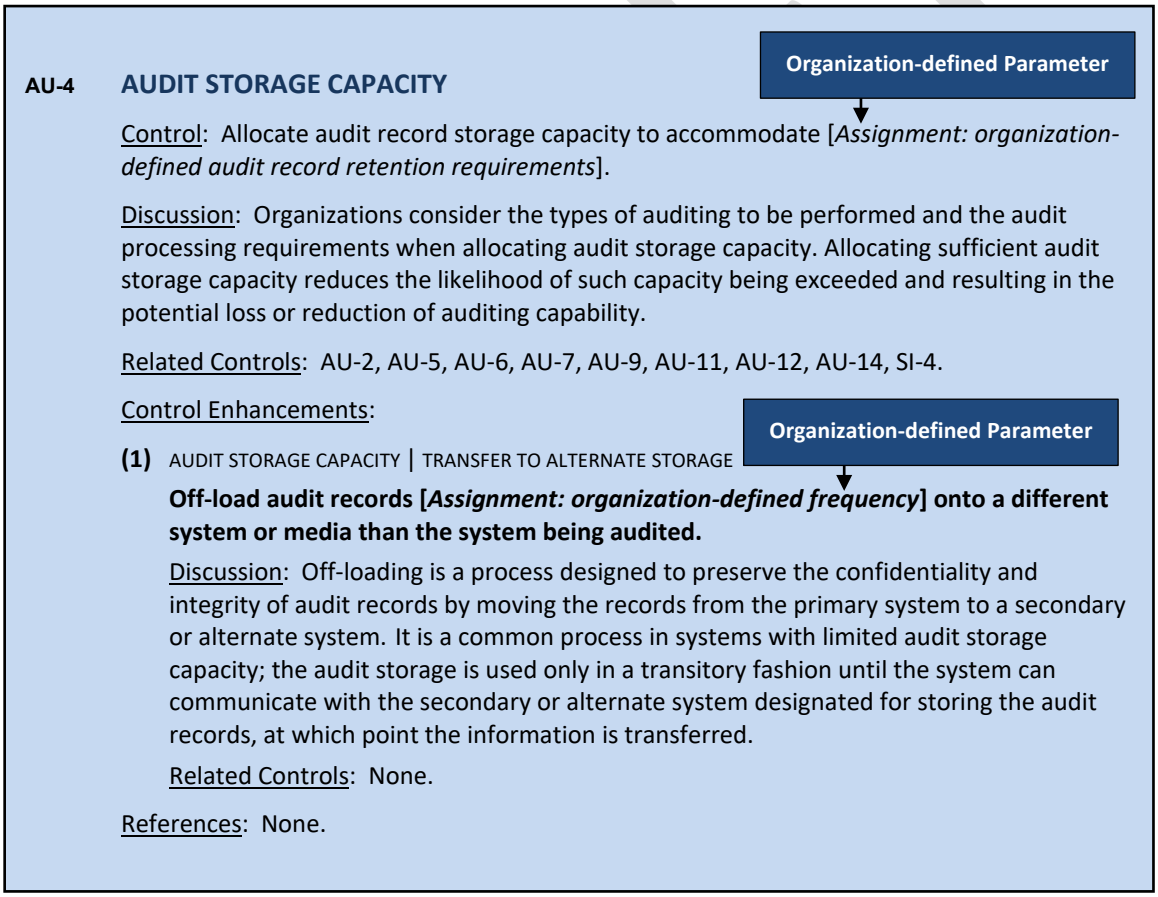

FIGURE 1: ORGANIZATION-DEFINED CONTROL PARAMETERS

[37] Organizations make every attempt to select compensating controls from the consolidated control catalog in [SP 800-53]. Organization-defined compensating controls are employed *only* when organizations determine that the control catalog does not contain suitable compensating controls.

Once organizations specify the parameter values for the controls and control enhancements, the specified assignment and selection values become a permanent part of the control and control enhancement. As such, they are documented in security and privacy program plans or system security and privacy plans, as appropriate. Organizations can specify the parameter values before selecting compensating controls since the parameter specification completes the control definitions and may affect the need for compensating controls. There can be significant benefits to collaborating on the development of parameter values for controls. For organizations that work together on a frequent basis or regularly conduct exchanges of information, it may be useful to develop a mutually agreeable set of control parameter values.

Supplementing Control Baselines

In certain situations, additional controls or control enhancements beyond the controls and enhancements contained in the control baselines in Chapter Three may be required to address specific threats to organizations, mission/business processes, and systems; to address privacy-related issues for individuals; and to satisfy the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Organizational assessments of risk provide essential information for determining the necessity and sufficiency of the controls and control enhancements in the control baselines. Organizations are encouraged to make maximum use of the control catalog in [SP 800-53] to supplement control baselines with additional controls or control enhancements.

Providing Additional Specification Information for Control Implementation

Since controls and control enhancements are statements of security or privacy functions or capabilities that are conveyed at higher levels of abstraction, the controls may lack sufficient information for implementation. Therefore, additional details may be necessary to fully define the intent of a given control for implementation purposes and to ensure that the security and privacy requirements related to that control are satisfied. For example, additional information may be provided as part of the process of moving from control to specification requirements, and may involve *refinement* of implementation details, *refinement* of scope, or *iteration* to apply the same control differently to different scopes. The need to provide additional control specification information occurs routinely when controls are employed in a system engineering process as part of requirements engineering. Organizations ensure that if existing control information is not sufficient to define the intended implementation details for the control, such information is provided to system owners and common control providers. Organizations have the flexibility to determine whether additional control specification information is included as part of the control statement or in a separate control addendum section. When providing additional detail, organizations are cautioned not to change the intent of the base control or modify the original language in the control. The additional implementation information is documented in the system security and privacy plans.

2.5 CAPABILITIES

Organizations consider defining a set of capabilities a precursor to the control selection process. The concept of *capability* recognizes that satisfying security or privacy requirements seldom derives from a single control but rather from a set of mutually reinforcing controls. For example, organizations may wish to define a capability for secure remote authentication. This capability can be achieved by the selection and implementation of a set of controls from [SP

800-53] (e.g., IA-2 [1], IA-2 [2], IA-2 [8], IA-2 [9], and SC-8 [1]). Moreover, capabilities can address a variety of areas that can include technical means, physical means, procedural means, or any combination thereof. Thus, in addition to the above capability for secure remote access, organizations may also need security capabilities that address physical means, such as tamper detection on a cryptographic module or anomaly detection/analysis on an orbiting spacecraft.

As the number of controls in [SP 800-53] grows in response to an increasingly sophisticated threat space, it is important for organizations to have the ability to describe key capabilities needed to protect organizational missions and business functions, and to subsequently select controls that—if properly designed, developed, and implemented—produce such capabilities. This simplifies how the protection problem is viewed conceptually. In essence, using the construct of a capability provides a shorthand method of grouping controls that are employed for a common purpose or to achieve a common objective. This is an important consideration, for example, when assessing controls for effectiveness.[38]

Traditionally, assessments have been conducted on a control-by-control basis, producing results that are characterized as pass (i.e., control satisfied) or fail (i.e., control not satisfied). However, the failure of a single control or in some cases, multiple controls, may not affect the overall capability needed by an organization. Moreover, employing the broader construct of a capability allows an organization to assess the severity of the vulnerabilities discovered in its information systems and determine if the failure of a particular control or the decision not to deploy a certain control affects the overall capability needed for mission/business protection. It also facilitates conducting *root cause* analyses to determine if the failure of one control can be traced to the failure of other controls based on the established control relationships. Ultimately, authorization decisions (i.e., risk acceptance decisions) are made based on the degree to which the desired capabilities have been effectively achieved and are meeting the security and privacy requirements defined by an organization. These risk-based decisions are directly related to the organizational risk tolerance that is defined as part of an organization's risk management strategy.

[38] NIST Interagency Report 8011, Vol. 1 [IR 8011 v1], describes the grouping of controls by purpose that facilitates automated control assessments.

CHAPTER THREE

THE CONTROL BASELINES

SECURITY AND PRIVACY CONTROL BASELINES

Tables 3-1 through 3-20 provide a listing the controls and control enhancements assigned to the control families in [SP 800-53] and the respective control allocations to the privacy control baseline and the low-impact, moderate-impact, and high-impact security control baselines. Section 2.2 (Privacy Control Baseline) provides additional information on the privacy control selection criteria.

SECURITY AND PRIVACY CONTROL BASELINE RELATIONSHIPS

- Controls and control enhancements that are assigned to security control baselines are used to manage risks arising from the loss of confidentiality, integrity, and availability. Since Senior Agency Officials for Privacy (SAOPs) have the responsibility for managing privacy risk in accordance with [OMB A-130], and since privacy risks arise from both the processing of PII and the loss of confidentiality, integrity, and availability of PII, it is important that organizations consider how privacy and security programs collaborate in activities related to these controls such as categorization, tailoring, implementation, and assessment.
- Controls and control enhancements that are assigned only to the privacy control baseline and not to the security control baselines are important for managing privacy program responsibilities under [OMB A-130 but do not generally support the management of risks that arise from the loss of confidentiality, integrity, and availability.
- Controls and control enhancements that are assigned to both the privacy and security control baselines are used to manage privacy program responsibilities under [OMB A-130] and risks that arise from the loss of confidentiality, integrity, and availability (including PII).
- Some controls and control enhancements are not assigned to any control baseline. Through tailoring, organizations make their own determinations as to whether the controls and control enhancements are needed to meet applicable requirements or are useful for managing risks that arise from the loss of confidentiality, integrity, and availability or the processing of PII.

3.1 ACCESS CONTROL FAMILY

Table 3-1 provides a summary of the controls and control enhancements assigned to the Access Control Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	**Policy and Procedures**	x	x	x	x
AC-2	**Account Management**		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE	W: Incorporated into AC-2k.			
AC-2(11)	USAGE CONDITIONS				x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK USERS			x	x
AC-2(14)	PROHIBIT SPECIFIC ACCOUNT TYPES				
AC-3	**Access Enforcement**		x	x	x
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTION	W: Incorporated into AC-6.			
AC-3(2)	DUAL AUTHORIZATION				
AC-3(3)	MANDATORY ACCESS CONTROL				
AC-3(4)	DISCRETIONARY ACCESS CONTROL				
AC-3(5)	SECURITY-RELEVANT INFORMATION				
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	W: Incorporated into MP-4, SC-28.			
AC-3(7)	ROLE-BASED ACCESS CONTROL				
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS				
AC-3(9)	CONTROLLED RELEASE				
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS				
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES				
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS				
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL				
AC-3(14)	INDIVIDUAL ACCESS	x			
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL				
AC-4	**Information Flow Enforcement**			x	x
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES				
AC-4(2)	PROCESSING DOMAINS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL				
AC-4(4)	FLOW CONTROL OF ENCRYPTED INFORMATION				x
AC-4(5)	EMBEDDED DATA TYPES				
AC-4(6)	METADATA				
AC-4(7)	ONE-WAY FLOW MECHANISMS				
AC-4(8)	SECURITY AND PRIVACY POLICY FILTERS				
AC-4(9)	HUMAN REVIEWS				
AC-4(10)	ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS				
AC-4(11)	CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS				
AC-4(12)	DATA TYPE IDENTIFIERS				
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS				
AC-4(14)	SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS				
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION				
AC-4(16)	INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS	W: Incorporated into AC-4.			
AC-4(17)	DOMAIN AUTHENTICATION				
AC-4(18)	SECURITY ATTRIBUTE BINDING	W: Incorporated into AC-16.			
AC-4(19)	VALIDATION OF METADATA				
AC-4(20)	APPROVED SOLUTIONS				
AC-4(21)	PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS				
AC-4(22)	ACCESS ONLY				
AC-4(23)	MODIFY NON-RELEASABLE INFORMATION				
AC-4(24)	INTERNAL NORMALIZED FORMAT				
AC-4(25)	DATA SANITIZATION				
AC-4(26)	AUDIT FILTERING ACTIONS				
AC-4(27)	REDUNDANT/INDEPENDENT FILTERING MECHANISMS				
AC-4(28)	LINEAR FILTER PIPELINES				
AC-4(29)	FILTER ORCHESTRATION ENGINES				
AC-4(30)	FILTER MECHANISMS USING MULTIPLE PROCESSES				
AC-4(31)	FAILED CONTENT TRANSFER PREVENTION				
AC-4(32)	PROCESS REQUIREMENTS FOR INFORMATION TRANSFER				
AC-5	**Separation of Duties**			x	x
AC-6	**Least Privilege**			x	x
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS			x	x
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS			x	x
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS				x
AC-6(4)	SEPARATE PROCESSING DOMAINS				
AC-6(5)	PRIVILEGED ACCOUNTS			x	x
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS				
AC-6(7)	REVIEW OF USER PRIVILEGES		x	x	x
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION				
AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS		x	x	x
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-7	**Unsuccessful Logon Attempts**		x	x	x
AC-7(1)	AUTOMATIC ACCOUNT LOCK	W: Incorporated into AC-7.			
AC-7(2)	PURGE OR WIPE MOBILE DEVICE				
AC-7(3)	BIOMETRIC ATTEMPT LIMITING				
AC-7(4)	USE OF ALTERNATE FACTOR				
AC-8	**System Use Notification**		x	x	x
AC-9	**Previous Logon Notification**				
AC-9(1)	UNSUCCESSFUL LOGONS				
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS				
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES				
AC-9(4)	ADDITIONAL LOGON INFORMATION				
AC-10	**Concurrent Session Control**				x
AC-11	**Device Lock**			x	x
AC-11(1)	PATTERN-HIDING DISPLAYS			x	x
AC-12	**Session Termination**			x	x
AC-12(1)	USER-INITIATED LOGOUTS				
AC-12(2)	TERMINATION MESSAGE				
AC-12(3)	TIMEOUT WARNING MESSAGE				
AC-13	Supervision and Review-Access Control	W: Incorporated into AC-2, AU-6.			
AC-14	**Permitted Actions without Identification or Authentication**		x	x	x
AC-14(1)	NECESSARY USES	W: Incorporated into AC-14.			
AC-15	Automated Marking	W: Incorporated into MP-3.			
AC-16	**Security and Privacy Attributes**				
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION				
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS				
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM				
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS				
AC-16(5)	ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES				
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION				
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION				
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES				
AC-16(9)	ATTRIBUTE REASSIGNMENT – REGRADING MECHANISMS				
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS				
AC-17	**Remote Access**		x	x	x
AC-17(1)	MONITORING AND CONTROL			x	x
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION			x	x
AC-17(3)	MANAGED ACCESS CONTROL POINTS			x	x
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS			x	x
AC-17(5)	MONITORING FOR UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-17(6)	PROTECTION OF MECHANISM INFORMATION				
AC-17(7)	ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	W: Incorporated into AC-3(10).			
AC-17(8)	DISABLE NONSECURE NETWORK PROTOCOLS	W: Incorporated into CM-7.			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-17(9)	DISCONNECT OR DISABLE ACCESS				
AC-17(10)	AUTHENTICATE REMOTE COMMANDS				
AC-18	**Wireless Access**		x	x	x
AC-18(1)	AUTHENTICATION AND ENCRYPTION			x	x
AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-18(3)	DISABLE WIRELESS NETWORKING			x	x
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS				x
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS				x
AC-19	**Access Control for Mobile Devices**		x	x	x
AC-19(1)	USE OF WRITABLE AND PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(2)	USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(3)	USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER	W: Incorporated into MP-7.			
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION				
AC-19(5)	FULL DEVICE AND CONTAINER-BASED ENCRYPTION			x	x
AC-20	**Use of External Systems**		x	x	x
AC-20(1)	LIMITS ON AUTHORIZED USE			x	x
AC-20(2)	PORTABLE STORAGE DEVICES — RESTRICTED USE			x	x
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE				
AC-20(4)	NETWORK-ACCESSIBLE STORAGE DEVICES				
AC-20(5)	PORTABLE STORAGE DEVICES — PROHIBITED USE				
AC-20(6)	NON-ORGANIZATIONALLY OWNED SYSTEMS — PROHIBITED USE				
AC-21	**Information Sharing**			x	x
AC-21(1)	AUTOMATED DECISION SUPPORT				
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL				
AC-22	**Publicly Accessible Content**		x	x	x
AC-23	**Data Mining Protection**				
AC-24	**Access Control Decisions**				
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION				
AC-24(2)	NO USER OR PROCESS IDENTITY				
AC-25	**Reference Monitor**				

761

3.2 AWARENESS AND TRAINING FAMILY

Table 3-2 provides a summary of the controls and control enhancements assigned to the Awareness and Training Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	x	x	x	x
AT-2	**Awareness Training**	x	x	x	x
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	BREACH	x			
AT-2(6)	ADVANCED PERSISTENT THREAT				
AT-2(7)	CYBER THREAT ENVIRONMENT				
AT-2(8)	TRAINING FEEDBACK				
AT-3	**Role-Based Training**	x	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	ACCESSING PERSONALLY IDENTIFIABLE INFORMATION	x			
AT-4	**Training Records**	x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	W: Incorporated into PM-15.			

3.3 AUDIT AND ACCOUNTABILITY FAMILY

Table 3-3 provides a summary of the controls and control enhancements assigned to the Audit and Accountability Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-3: AUDIT AND ACCOUNTABILITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AU-1	**Policy and Procedures**	x	x	x	x
AU-2	**Event Logging**	x	x	x	x
AU-2(1)	COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES	W: Incorporated into AU-12.			
AU-2(2)	SELECTION OF AUDIT EVENTS BY COMPONENT	W: Incorporated into AU-12.			
AU-2(3)	REVIEWS AND UPDATES	W: Incorporated into AU-2.			
AU-2(4)	PRIVILEGED FUNCTIONS	W: Incorporated into AC-6(9).			
AU-3	**Content of Audit Records**		x	x	x
AU-3(1)	ADDITIONAL AUDIT INFORMATION			x	x
AU-3(2)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT				x
AU-3(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS				
AU-4	**Audit Log Storage Capacity**		x	x	x
AU-4(1)	TRANSFER TO ALTERNATE STORAGE				
AU-5	**Response to Audit Logging Process Failures**		x	x	x
AU-5(1)	STORAGE CAPACITY WARNING				x
AU-5(2)	REAL-TIME ALERTS				x
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS				
AU-5(4)	SHUTDOWN ON FAILURE				
AU-5(5)	ALTERNATE AUDIT LOGGING CAPABILITY				
AU-6	**Audit Record Review, Analysis, and Reporting**		x	x	x
AU-6(1)	AUTOMATED PROCESS INTEGRATION			x	x
AU-6(2)	AUTOMATED SECURITY ALERTS	W: Incorporated into SI-4.			
AU-6(3)	CORRELATE AUDIT RECORD REPOSITORIES			x	x
AU-6(4)	CENTRAL REVIEW AND ANALYSIS				
AU-6(5)	INTEGRATED ANALYSIS OF AUDIT RECORDS				x
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING				x
AU-6(7)	PERMITTED ACTIONS				
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS				
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES				
AU-6(10)	AUDIT LEVEL ADJUSTMENT	W: Incorporated into AU-6.			
AU-7	**Audit Record Reduction and Report Generation**			x	x
AU-7(1)	AUTOMATIC PROCESSING			x	x
AU-7(2)	AUTOMATIC SORT AND SEARCH	W: Incorporated into AU-7(1).			
AU-8	**Time Stamps**		x	x	x
AU-8(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE			x	x
AU-8(2)	SECONDARY AUTHORITATIVE TIME SOURCE				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AU-9	**Protection of Audit Information**		x	x	x
AU-9(1)	HARDWARE WRITE-ONCE MEDIA				
AU-9(2)	STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS				x
AU-9(3)	CRYPTOGRAPHIC PROTECTION				x
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS			x	x
AU-9(5)	DUAL AUTHORIZATION				
AU-9(6)	READ-ONLY ACCESS				
AU-9(7)	STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM				
AU-10	**Non-repudiation**				x
AU-10(1)	ASSOCIATION OF IDENTITIES				
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY				
AU-10(3)	CHAIN OF CUSTODY				
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY				
AU-10(5)	DIGITAL SIGNATURES	W: Incorporated into SI-7.			
AU-11	**Audit Record Retention**	x	x	x	x
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY				
AU-12	**Audit Record Generation**		x	x	x
AU-12(1)	SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL				x
AU-12(2)	STANDARDIZED FORMATS				
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS				x
AU-12(4)	QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION				
AU-13	**Monitoring for Information Disclosure**				
AU-13(1)	USE OF AUTOMATED TOOLS				
AU-13(2)	REVIEW OF MONITORED SITES				
AU-13(3)	UNAUTHORIZED REPLICATION OF INFORMATION				
AU-14	**Session Audit**				
AU-14(1)	SYSTEM START-UP				
AU-14(2)	CAPTURE AND RECORD CONTENT	W: Incorporated into AU-14.			
AU-14(3)	REMOTE VIEWING AND LISTENING				
AU-15	**Alternate Audit Logging Capability**	W: Incorporated into AU-5(5).			
AU-16	**Cross-Organizational Auditing Logging**				
AU-16(1)	IDENTITY PRESERVATION				
AU-16(2)	SHARING OF AUDIT INFORMATION				
AU-16(3)	DISASSOCIABILITY				

773

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

Table 3-4 provides a summary of the controls and control enhancements assigned to the Assessment, Authorization, and Monitoring Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-4: ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CA-1	**Policies and Procedures**	x	x	x	x
CA-2	**Control Assessments**	x	x	x	x
CA-2(1)	INDEPENDENT ASSESSORS			x	x
CA-2(2)	SPECIALIZED ASSESSMENTS				x
CA-2(3)	EXTERNAL ORGANIZATIONS				
CA-3	**Information Exchange**		x	x	x
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(25).			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(26).			
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(27).			
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS	W: Moved to SC-7(28).			
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	W: Incorporated into SC-7(5).			
CA-3(6)	TRANSFER AUTHORIZATIONS				x
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES				
CA-4	**Security Certification**	W: Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**	x	x	x	x
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				
CA-6	**Authorization**	x	x	x	x
CA-6(1)	JOINT AUTHORIZATION — INTRA - ORGANIZATION				
CA-6(2)	JOINT AUTHORIZATION — INTER - ORGANIZATIONS				
CA-7	**Continuous Monitoring**	x	x	x	x
CA-7(1)	INDEPENDENT ASSESSMENT			x	x
CA-7(2)	TYPES OF ASSESSMENTS	W: Incorporated into CA-2.			
CA-7(3)	TREND ANALYSES				
CA-7(4)	RISK MONITORING	x	x	x	x
CA-7(5)	CONSISTENCY ANALYSIS				
CA-8	**Penetration Testing**				x
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM				x
CA-8(2)	RED TEAM EXERCISES				
CA-8(3)	FACILITY PENETRATION TESTING				
CA-9	**Internal System Connections**		x	x	x
CA-9(1)	COMPLIANCE CHECKS				

781 3.5 CONFIGURATION MANAGEMENT FAMILY

782 Table 3-5 provides a summary of the controls and control enhancements assigned to the
783 Configuration Management Family. The controls are allocated to the low-impact, moderate-
784 impact, and high-impact security control baselines and the privacy control baseline, as
785 appropriate.

786 **TABLE 3-5: CONFIGURATION MANAGEMENT FAMILY**

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CM-1	**Policy and Procedures**	x	x	x	x
CM-2	**Baseline Configuration**		x	x	x
CM-2(1)	REVIEWS AND UPDATES	W: Incorporated into CM-2.			
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY			x	x
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS			x	x
CM-2(4)	UNAUTHORIZED SOFTWARE	W: Incorporated into CM-7.			
CM-2(5)	AUTHORIZED SOFTWARE	W: Incorporated into CM-7.			
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS				
CM-2(7)	CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS			x	x
CM-3	**Configuration Change Control**			x	x
CM-3(1)	AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES				x
CM-3(2)	TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES			x	x
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION				
CM-3(4)	SECURITY AND PRIVACY REPRESENTATIVES			x	x
CM-3(5)	AUTOMATED SECURITY RESPONSE				
CM-3(6)	CRYPTOGRAPHY MANAGEMENT				x
CM-3(7)	REVIEW SYSTEM CHANGES				
CM-3(8)	PREVENT OR RESTRICT CONFIGURATION CHANGES				
CM-4	**Impact Analyses**	x	x	x	x
CM-4(1)	SEPARATE TEST ENVIRONMENTS				x
CM-4(2)	VERIFICATION OF CONTROLS			x	x
CM-5	**Access Restrictions for Change**		x	x	x
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS				x
CM-5(2)	REVIEW SYSTEM CHANGES	W: Incorporated into CM-3(7).			
CM-5(3)	SIGNED COMPONENTS				x
CM-5(4)	DUAL AUTHORIZATION				
CM-5(5)	PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION				
CM-5(6)	LIMIT LIBRARY PRIVILEGES				
CM-5(7)	AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS	W: Incorporated into SI-7.			
CM-6	**Configuration Settings**		x	x	x
CM-6(1)	AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION				x
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES				x
CM-6(3)	UNAUTHORIZED CHANGE DETECTION	W: Incorporated into SI-7.			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6(4)	CONFORMANCE DEMONSTRATION	W: Incorporated into CM-4.			
CM-7	**Least Functionality**		x	x	x
CM-7(1)	PERIODIC REVIEW			x	x
CM-7(2)	PREVENT PROGRAM EXECUTION			x	x
CM-7(3)	REGISTRATION COMPLIANCE				
CM-7(4)	UNAUTHORIZED SOFTWARE — BLACKLISTING				
CM-7(5)	AUTHORIZED SOFTWARE — WHITELISTING			x	x
CM-7(6)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES				
CM-7(7)	CODE EXECUTION IN PROTECTED ENVIRONMENTS				
CM-7(8)	BINARY OR MACHINE EXECUTABLE CODE				
CM-8	**System Component Inventory**		x	x	x
CM-8(1)	UPDATES DURING INSTALLATION AND REMOVAL			x	x
CM-8(2)	AUTOMATED MAINTENANCE				x
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION			x	x
CM-8(4)	ACCOUNTABILITY INFORMATION				x
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS				
CM-8(6)	ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS				
CM-8(7)	CENTRALIZED REPOSITORY				
CM-8(8)	AUTOMATED LOCATION TRACKING				
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS				
CM-9	**Configuration Management Plan**			x	x
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY				
CM-10	**Software Usage Restrictions**		x	x	x
CM-10(1)	OPEN SOURCE SOFTWARE				
CM-11	**User-Installed Software**		x	x	x
CM-11(1)	ALERTS FOR UNAUTHORIZED INSTALLATIONS	W: Incorporated into CM-8(3).			
CM-11(2)	SOFTWARE INSTALLATION WITH PRIVILEGED STATUS				
CM-12	**Information Location**			x	x
CM-12(1)	AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION			x	x
CM-13	**Data Action Mapping**				

787

3.6 CONTINGENCY PLANNING FAMILY

Table 3-6 provides a summary of the controls and control enhancements assigned to the Contingency Planning Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-6: CONTINGENCY PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-1	**Policy and Procedures**		x	x	x
CP-2	**Contingency Plan**		x	x	x
CP-2(1)	COORDINATE WITH RELATED PLANS			x	x
CP-2(2)	CAPACITY PLANNING				x
CP-2(3)	RESUME MISSIONS AND BUSINESS FUNCTIONS			x	x
CP-2(4)	RESUME ALL MISSIONS AND BUSINESS FUNCTIONS	W: Incorporated into CP-2(3).			
CP-2(5)	CONTINUE MISSIONS AND BUSINESS FUNCTIONS				x
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES				
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS				
CP-2(8)	IDENTIFY CRITICAL ASSETS			x	x
CP-3	**Contingency Training**		x	x	x
CP-3(1)	SIMULATED EVENTS				x
CP-3(2)	MECHANISMS USED IN TRAINING ENVIRONMENTS				
CP-4	**Contingency Plan Testing**		x	x	x
CP-4(1)	COORDINATE WITH RELATED PLANS			x	x
CP-4(2)	ALTERNATE PROCESSING SITE				x
CP-4(3)	AUTOMATED TESTING				
CP-4(4)	FULL RECOVERY AND RECONSTITUTION				
CP-5	Contingency Plan Update	W: Incorporated into CP-2.			
CP-6	**Alternate Storage Site**			x	x
CP-6(1)	SEPARATION FROM PRIMARY SITE			x	x
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES				x
CP-6(3)	ACCESSIBILITY			x	x
CP-7	**Alternate Processing Site**			x	x
CP-7(1)	SEPARATION FROM PRIMARY SITE			x	x
CP-7(2)	ACCESSIBILITY			x	x
CP-7(3)	PRIORITY OF SERVICE			x	x
CP-7(4)	PREPARATION FOR USE				x
CP-7(5)	EQUIVALENT INFORMATION SECURITY SAFEGUARDS	W: Incorporated into CP-7.			
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE				
CP-8	**Telecommunications Services**			x	x
CP-8(1)	PRIORITY OF SERVICE PROVISIONS			x	x
CP-8(2)	SINGLE POINTS OF FAILURE			x	x
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS				x
CP-8(4)	PROVIDER CONTINGENCY PLAN				x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING				
CP-9	**System Backup**		x	x	x
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY			x	x
CP-9(2)	TEST RESTORATION USING SAMPLING				x
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION				x
CP-9(4)	PROTECTION FROM UNAUTHORIZED MODIFICATION	W: Incorporated into CP-9.			
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE				x
CP-9(6)	REDUNDANT SECONDARY SYSTEM				
CP-9(7)	DUAL AUTHORIZATION				
CP-9(8)	CRYPTOGRAPHIC PROTECTION			x	x
CP-10	**System Recovery and Reconstitution**		x	x	x
CP-10(1)	CONTINGENCY PLAN TESTING	W: Incorporated into CP-4.			
CP-10(2)	TRANSACTION RECOVERY			x	x
CP-10(3)	COMPENSATING SECURITY CONTROLS	W: Incorporated into PL-11.			
CP-10(4)	RESTORE WITHIN TIME PERIOD				x
CP-10(5)	FAILOVER CAPABILITY	W: Incorporated into SI-13.			
CP-10(6)	COMPONENT PROTECTION				
CP-11	**Alternate Communications Protocols**				
CP-12	**Safe Mode**				
CP-13	**Alternative Security Mechanisms**				
CP-14	**Self-Challenge**				

793

3.7 IDENTIFICATION AND AUTHENTICATION FAMILY

Table 3-7 provides a summary of the controls and control enhancements assigned to the Identification and Authentication Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-1	**Policy and Procedures**		x	x	x
IA-2	**Identification and Authentication (Organizational Users)**		x	x	x
IA-2(1)	MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x
IA-2(2)	MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE				
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	W: Incorporated into IA-2(8).			
IA-2(10)	SINGLE SIGN-ON				
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W: Incorporated into IA-2(1)(2).			
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION				
IA-3	**Device Identification and Authentication**			x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION				
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W: Incorporated into IA-3(1).			
IA-3(3)	DYNAMIC ADDRESS ALLOCATION				
IA-3(4)	DEVICE ATTESTATION				
IA-4	**Identifier Management**		x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS				
IA-4(2)	SUPERVISOR AUTHORIZATION	W: Incorporated into IA-12(1).			
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	W: Incorporated into IA-12(2).			
IA-4(4)	IDENTIFY USER STATUS			x	x
IA-4(5)	DYNAMIC MANAGEMENT				
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT				
IA-4(7)	IN-PERSON REGISTRATION	W: Incorporated into IA-12(4).			
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS				
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION				
IA-5	**Authenticator Management**		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION			x	x
IA-5(3)	IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION	W: Incorporated into IA-12(4).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-5(4)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	W: Incorporated into IA-5(1).			
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY				
IA-5(6)	PROTECTION OF AUTHENTICATORS			x	x
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS				
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS				
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT				
IA-5(10)	DYNAMIC CREDENTIAL BINDING				
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION	W: Incorporated into IA-2(1)(2).			
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE				
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS				
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES				
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES				
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE				
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS				
IA-5(18)	PASSWORD MANAGERS				
IA-6	**Authenticator Feedback**		x	x	x
IA-7	**Cryptographic Module Authentication**		x	x	x
IA-8	**Identification and Authentication (Non-Organizational Users)**		x	x	x
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES		x	x	x
IA-8(2)	ACCEPTANCE OF EXTERNAL CREDENTIALS		x	x	x
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS	W: Incorporated into IA-8(2).			
IA-8(4)	USE OF NIST-ISSUED PROFILES		x	x	x
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS				
IA-8(6)	DISASSOCIABILITY				
IA-9	**Service Identification and Authentication**				
IA-9(1)	INFORMATION EXCHANGE	W: Complete withdrawal.			
IA-9(2)	TRANSMISSION OF DECISIONS	W: Incorporated into IA-9.			
IA-10	**Adaptive Authentication**				
IA-11	**Re-authentication**		x	x	x
IA-12	**Identity Proofing**			x	x
IA-12(1)	SUPERVISOR AUTHORIZATION				
IA-12(2)	IDENTITY EVIDENCE			x	x
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION			x	x
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION				x
IA-12(5)	ADDRESS CONFIRMATION			x	x
IA-12(6)	ACCEPT EXTERNALLY-PROOFED IDENTITIES				

800

3.8 INCIDENT RESPONSE FAMILY

Table 3-8 provides a summary of the controls and control enhancements assigned to the Incident Response Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-8: INCIDENT RESPONSE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IR-1	**Policy and Procedures**	x	x	x	x
IR-2	**Incident Response Training**		x	x	x
IR-2(1)	SIMULATED EVENTS				x
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS				x
IR-3	**Incident Response Testing**	x		x	x
IR-3(1)	AUTOMATED TESTING				
IR-3(2)	COORDINATION WITH RELATED PLANS			x	x
IR-3(3)	CONTINUOUS IMPROVEMENT				
IR-4	**Incident Handling**	x	x	x	x
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES			x	x
IR-4(2)	DYNAMIC RECONFIGURATION				
IR-4(3)	CONTINUITY OF OPERATIONS				
IR-4(4)	INFORMATION CORRELATION				x
IR-4(5)	AUTOMATIC DISABLING OF SYSTEM				
IR-4(6)	INSIDER THREATS — SPECIFIC CAPABILITIES				
IR-4(7)	INSIDER THREATS — INTRA-ORGANIZATION COORDINATION				
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS				
IR-4(9)	DYNAMIC RESPONSE CAPABILITY				
IR-4(10)	SUPPLY CHAIN COORDINATION				
IR-4(11)	INTEGRATED INCIDENT RESPONSE TEAM				
IR-4(12)	MALICIOUS CODE AND FORENSIC ANALYSIS				
IR-4(13)	BEHAVIOR ANALYSIS				
IR-4(14)	SECURITY OPERATIONS CENTER				
IR-4(15)	PUBLIC RELATIONS AND REPUTATION REPAIR				
IR-5	**Incident Monitoring**		x	x	x
IR-5(1)	AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS				x
IR-6	**Incident Reporting**	x	x	x	x
IR-6(1)	AUTOMATED REPORTING			x	x
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS				
IR-6(3)	SUPPLY CHAIN COORDINATION			x	x
IR-7	**Incident Response Assistance**	x	x	x	x
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT			x	x
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS				
IR-8	**Incident Response Plan**	x	x	x	x
IR-8(1)	PRIVACY BREACHES	x			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IR-9	**Information Spillage Response**				
IR-9(1)	RESPONSIBLE PERSONNEL	W: Incorporated in IR-9.			
IR-9(2)	TRAINING				
IR-9(3)	POST-SPILL OPERATIONS				
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL				
IR-10	**Incident Analysis**				x

806

3.9 MAINTENANCE FAMILY

Table 3-9 provides a summary of the controls and control enhancements assigned to the Maintenance Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-9: MAINTENANCE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MA-1	**Policy and Procedures**		x	x	x
MA-2	**Controlled Maintenance**		x	x	x
MA-2(1)	RECORD CONTENT	W: Incorporated into MA-2.			
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES				x
MA-3	**Maintenance Tools**			x	x
MA-3(1)	INSPECT TOOLS			x	x
MA-3(2)	INSPECT MEDIA			x	x
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL			x	x
MA-3(4)	RESTRICTED TOOL USE				
MA-3(5)	EXECUTION WITH PRIVILEGE				
MA-3(6)	SOFTWARE UPDATES AND PATCHES				
MA-4	**Nonlocal Maintenance**		x	x	x
MA-4(1)	LOGGING AND REVIEW				
MA-4(2)	DOCUMENT NONLOCAL MAINTENANCE	W: Incorporated into MA-1, MA-4.			
MA-4(3)	COMPARABLE SECURITY AND SANITIZATION				x
MA-4(4)	AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS				
MA-4(5)	APPROVALS AND NOTIFICATIONS				
MA-4(6)	CRYPTOGRAPHIC PROTECTION				
MA-4(7)	DISCONNECT VERIFICATION				
MA-5	**Maintenance Personnel**		x	x	x
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS				x
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS				
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS				
MA-5(4)	FOREIGN NATIONALS				
MA-5(5)	NON-SYSTEM MAINTENANCE				
MA-6	**Timely Maintenance**			x	x
MA-6(1)	PREVENTIVE MAINTENANCE				
MA-6(2)	PREDICTIVE MAINTENANCE				
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE				
MA-7	**Field Maintenance**				

3.10 MEDIA PROTECTION FAMILY

Table 3-10 provides a summary of the controls and control enhancements assigned to the Media Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-10: MEDIA PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MP-1	**Policy and Procedures**	x	x	x	x
MP-2	**Media Access**		x	x	x
MP-2(1)	AUTOMATED RESTRICTED ACCESS	W: Incorporated into MP-4(2).			
MP-2(2)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-3	**Media Marking**			x	x
MP-4	**Media Storage**			x	x
MP-4(1)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-4(2)	AUTOMATED RESTRICTED ACCESS				
MP-5	**Media Transport**			x	x
MP-5(1)	PROTECTION OUTSIDE OF CONTROLLED AREAS	W: Incorporated into MP-5.			
MP-5(2)	DOCUMENTATION OF ACTIVITIES	W: Incorporated into MP-5.			
MP-5(3)	CUSTODIANS				
MP-5(4)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-6	**Media Sanitization**	x	x	x	x
MP-6(1)	REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY				x
MP-6(2)	EQUIPMENT TESTING				x
MP-6(3)	NONDESTRUCTIVE TECHNIQUES				x
MP-6(4)	CONTROLLED UNCLASSIFIED INFORMATION	W: Incorporated into MP-6.			
MP-6(5)	CLASSIFIED INFORMATION	W: Incorporated into MP-6.			
MP-6(6)	MEDIA DESTRUCTION	W: Incorporated into MP-6.			
MP-6(7)	DUAL AUTHORIZATION				
MP-6(8)	REMOTE PURGING OR WIPING OF INFORMATION				
MP-7	**Media Use**		x	x	x
MP-7(1)	PROHIBIT USE WITHOUT OWNER	W: Incorporated into MP-7.			
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA				
MP-8	**Media Downgrading**				
MP-8(1)	DOCUMENTATION OF PROCESS				
MP-8(2)	EQUIPMENT TESTING				
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION				
MP-8(4)	CLASSIFIED INFORMATION				

3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

Table 3-11 provides a summary of the controls and control enhancements assigned to the Physical and Environmental Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-11: PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-1	**Policy and Procedures**		x	x	X
PE-2	**Physical Access Authorizations**		x	x	x
PE-2(1)	ACCESS BY POSITION AND ROLE				
PE-2(2)	TWO FORMS OF IDENTIFICATION				
PE-2(3)	RESTRICT UNESCORTED ACCESS				
PE-3	**Physical Access Control**		x	x	x
PE-3(1)	SYSTEM ACCESS				x
PE-3(2)	FACILITY AND SYSTEMS				
PE-3(3)	CONTINUOUS GUARDS				
PE-3(4)	LOCKABLE CASINGS				
PE-3(5)	TAMPER PROTECTION				
PE-3(6)	FACILITY PENETRATION TESTING	W: Incorporated into CA-8.			
PE-3(7)	PHYSICAL BARRIERS				
PE-3(8)	ACCESS CONTROL VESTIBULES				
PE-4	**Access Control for Transmission**			x	x
PE-5	**Access Control for Output Devices**			x	x
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS	W: Incorporated into PE-5.			
PE-5(2)	LINK TO INDIVIDUAL IDENTITY				
PE-5(3)	MARKING OUTPUT DEVICES				
PE-6	**Monitoring Physical Access**		x	x	x
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT			x	x
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES				
PE-6(3)	VIDEO SURVEILLANCE				
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				x
PE-7	**Visitor Control**	W: Incorporated into PE-2, PE-3.			
PE-8	**Visitor Access Records**		x	x	x
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW				x
PE-8(2)	PHYSICAL ACCESS RECORDS	W: Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**			x	x
PE-9(1)	REDUNDANT CABLING				
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS				
PE-10	**Emergency Shutoff**			x	x
PE-10(1)	ACCIDENTAL AND UNAUTHORIZED ACTIVATION	W: Incorporated into PE-10.			
PE-11	**Emergency Power**			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-11(1)	ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY				x
PE-11(2)	ALTERNATE POWER SUPPLY — SELF-CONTAINED				
PE-12	**Emergency Lighting**		x	x	x
PE-12(1)	ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS				
PE-13	**Fire Protection**		x	x	x
PE-13(1)	DETECTION SYSTEMS – AUTOMATIC ACTIVATION AND NOTIFICATION			x	x
PE-13(2)	SUPPRESSION SYSTEMS – AUTOMATIC ACTIVATION AND NOTIFICATION				x
PE-13(3)	AUTOMATIC FIRE SUPPRESSION	W: Incorporated into PE-13(2).			
PE-13(4)	INSPECTIONS				
PE-14	**Environmental Controls**		x	x	x
PE-14(1)	AUTOMATIC CONTROLS				
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS				
PE-15	**Water Damage Protection**		x	x	x
PE-15(1)	AUTOMATION SUPPORT				x
PE-16	**Delivery and Removal**		x	x	x
PE-17	**Alternate Work Site**			x	x
PE-18	**Location of System Components**				x
PE-18(1)	FACILITY SITE	W: Moved to PE-23.			
PE-19	**Information Leakage**				
PE-19(1)	NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES				
PE-20	**Asset Monitoring and Tracking**				
PE-21	**Electromagnetic Pulse Protection**				
PE-22	**Component Marking**				
PE-23	**Facility Location**				

825

3.12 PLANNING FAMILY

Table 3-12 provides a summary of the controls and control enhancements assigned to the Planning Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-12: PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	**System Security Plan Update**	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	**Privacy Impact Assessment**	W: Incorporated into RA-8.			
PL-6	**Security-Related Activity Planning**	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE-IN-DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

3.13 PROGRAM MANAGEMENT FAMILY

Table 3-13 provides a summary of the controls and control enhancements assigned to the Program Management Family. These controls are implemented at the organization level and are not directed at individual information systems. The Program Management controls are designed to facilitate compliance with applicable federal laws, Executive Orders, directives, regulations, policies, and standards.

TABLE 3-13: PROGRAM MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PM-1	**Information Security Program Plan**		x	x	x
PM-2	**Information Security Program Leadership Role**		x	x	x
PM-3	**Information Security and Privacy Resources**	x	x	x	x
PM-4	**Plan of Action and Milestones Process**	x	x	x	x
PM-5	**System Inventory**		x	x	x
PM-5(1)	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	x	x	x	x
PM-6	**Measures of Performance**	x	x	x	x
PM-7	**Enterprise Architecture**	x	x	x	x
PM-7(1)	OFFLOADING		x	x	x
PM-8	**Critical Infrastructure Plan**	x	x	x	x
PM-9	**Risk Management Strategy**	x	x	x	x
PM-10	**Authorization Process**	x	x	x	x
PM-11	**Mission and Business Process Definition**	x	x	x	x
PM-12	**Insider Threat Program**		x	x	x
PM-13	**Security and Privacy Workforce**	x	x	x	x
PM-14	**Testing, Training, and Monitoring**	x	x	x	x
PM-15	**Security and Privacy Groups and Associations**		x	x	x
PM-16	**Threat Awareness Program**		x	x	x
PM-16(1)	AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE		x	x	x
PM-17	**Protecting Controlled Unclassified Information on External Systems**		x	x	x
PM-18	**Privacy Program Plan**	x	x	x	x
PM-19	**Privacy Program Leadership Role**	x	x	x	x
PM-20	**Dissemination of Privacy Program Information**	x	x	x	x
PM-21	**Accounting of Disclosures**	x	x	x	x
PM-22	**Personally Identifiable Information Quality Management**	x	x	x	x
PM-23	**Data Governance Body**		x	x	x
PM-24	**Data Integrity Board**	x	x	x	x
PM-25	**Minimization of PII Used in Testing, Training, and Research**	x	x	x	x
PM-26	**Complaint Management**	x	x	x	x
PM-27	**Privacy Reporting**	x	x	x	x
PM-28	**Risk Framing**		x	x	x
PM-29	**Risk Management Program Leadership Roles**		x	x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PM-30	**Supply Chain Risk Management Strategy**		x	x	x
PM-31	**Continuous Monitoring Strategy**	x	x	x	x
PM-32	**Purposing**		x	x	x
PM-33	**Privacy Policies on Websites, Applications, and Digital Services**	x			

839

3.14 PERSONNEL SECURITY FAMILY

Table 3-14 provides a summary of the controls and control enhancements assigned to the Personnel Security Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-14: PERSONNEL SECURITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PS-1	**Policy and Procedures**		x	x	x
PS-2	**Position Risk Designation**		x	x	x
PS-3	**Personnel Screening**		x	x	x
PS-3(1)	CLASSIFIED INFORMATION				
PS-3(2)	FORMAL INDOCTRINATION				
PS-3(3)	INFORMATION WITH SPECIAL PROTECTION MEASURES				
PS-3(4)	CITIZENSHIP REQUIREMENTS				
PS-4	**Personnel Termination**		x	x	x
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS				
PS-4(2)	AUTOMATED NOTIFICATION				x
PS-5	**Personnel Transfer**		x	x	x
PS-6	**Access Agreements**		x	x	x
PS-6(1)	INFORMATION REQUIRING SPECIAL PROTECTION	W: Incorporated into PS-3.			
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION				
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS				
PS-7	**External Personnel Security**		x	x	x
PS-8	**Personnel Sanctions**		x	x	x

3.15 PII PROCESSING AND TRANSPARENCY FAMILY

Table 3-15 provides a summary of the controls and control enhancements assigned to the Personally Identifiable Information Processing and Transparency Family. The controls are allocated to the privacy control baseline in accordance with the selection criteria defined in Section 2.2.

TABLE 3-15: PROCESSING PERMISSIONS FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PT-1	**Policy and Procedures**	x	Privacy controls are not allocated to the security control baselines. Privacy baseline controls are selected based on the selection criteria defined in Section 2.2.		
PT-2	**Authority to Process Personally Identifiable Information**	x			
PT-2(1)	DATA TAGGING				
PT-2(2)	AUTOMATION				
PT-3	**Personally Identifiable Information Processing Purposes**	x			
PT-3(1)	DATA TAGGING				
PT-3(2)	AUTOMATION				
PT-4	**Minimization**	x			
PT-5	**Consent**	x			
PT-5(1)	TAILORED CONSENT				
PT-5(2)	JUST-IN-TIME CONSENT				
PT-6	**Privacy Notice**	x			
PT-6(1)	JUST-IN-TIME NOTICE				
PT-6(2)	PRIVACY ACT STATEMENTS	x			
PT-7	**System of Records Notice**	x			
PT-7(1)	ROUTINE USES	x			
PT-7(2)	EXEMPTION RULES	x			
PT-8	**Specific Categories of Personally Identifiable Information**	x			
PT-8(1)	SOCIAL SECURITY NUMBERS	x			
PT-8(2)	FIRST AMENDMENT INFORMATION	x			
PT-9	**Computer Matching Requirements**	x			

3.16 RISK ASSESSMENT FAMILY

Table 3-16 provides a summary of the controls and control enhancements assigned to the Risk Assessment Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-1	**Policy and Procedures**	x	x	x	x
RA-2	**Security Categorization**		x	x	x
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	**Risk Assessment**	x	x	x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		x	x	x
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	Risk Assessment Update	W: Incorporated into RA-3.			
RA-5	**Vulnerability Monitoring and Scanning**		x	x	x
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE SYSTEM VULNERABILITIES		x	x	x
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				x
RA-5(5)	PRIVILEGED ACCESS			x	x
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM				
RA-6	**Technical Surveillance Countermeasures Survey**				
RA-7	**Risk Response**	x	x	x	x
RA-8	**Privacy Impact Assessments**	x			
RA-9	**Criticality Analysis**			x	x
RA-10	**Threat Hunting**				

3.17 SYSTEM AND SERVICES ACQUISITION FAMILY

Table 3-17 provides a summary of the controls and control enhancements assigned to the System and Services Acquisition Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-17: SYSTEM AND SERVICES ACQUISITION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-1	**Policy and Procedures**	x	x	x	x
SA-2	**Allocation of Resources**		x	x	x
SA-3	**System Development Life Cycle**		x	x	x
SA-3(1)	MANAGE PREPRODUCTION ENVIRONMENT				
SA-3(2)	USE OF LIVE OR OPERATIONAL DATA				
SA-3(3)	TECHNOLOGY REFRESH				
SA-4	**Acquisition Process**	x	x	x	x
SA-4(1)	FUNCTIONAL PROPERTIES OF CONTROLS			x	x
SA-4(2)	DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS			x	x
SA-4(3)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES				
SA-4(4)	ASSIGNMENT OF COMPONENTS TO SYSTEMS	W: Incorporated into CM-8(9).			
SA-4(5)	SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS				x
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS				
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES				
SA-4(8)	CONTINUOUS MONITORING PLAN FOR CONTROLS				
SA-4(9)	FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE			x	x
SA-4(10)	USE OF APPROVED PIV PRODUCTS		x	x	x
SA-4(11)	SYSTEM OF RECORDS				
SA-4(12)	DATA OWNERSHIP				
SA-5	**System Documentation**		x	x	x
SA-5(1)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	W: Incorporated into SA-4(1).			
SA-5(2)	SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES	W: Incorporated into SA-4(2).			
SA-5(3)	HIGH-LEVEL DESIGN	W: Incorporated into SA-4(2).			
SA-5(4)	LOW-LEVEL DESIGN	W: Incorporated into SA-4(2).			
SA-5(5)	SOURCE CODE	W: Incorporated into SA-4(2).			
SA-6	**Software Usage Restrictions**	W: Incorporated into CM-10 and SI-7.			
SA-7	**User-Installed Software**	W: Incorporated into CM-11 and SI-7.			
SA-8	**Security and Privacy Engineering Principles**		x	x	x
SA-8(1)	CLEAR ABSTRACTIONS				
SA-8(2)	LEAST COMMON MECHANISM				
SA-8(3)	MODULARITY AND LAYERING				
SA-8(4)	PARTIALLY ORDERED DEPENDENCIES				
SA-8(5)	EFFICIENTLY MEDIATED ACCESS				
SA-8(6)	MINIMIZED SHARING				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-8(7)	REDUCED COMPLEXITY				
SA-8(8)	SECURE EVOLVABILITY				
SA-8(9)	TRUSTED COMPONENTS				
SA-8(10)	HIERARCHICAL TRUST				
SA-8(11)	INVERSE MODIFICATION THRESHOLD				
SA-8(12)	HIERARCHICAL PROTECTION				
SA-8(13)	MINIMIZED SECURITY ELEMENTS				
SA-8(14)	LEAST PRIVILEGE				
SA-8(15)	PREDICATE PERMISSION				
SA-8(16)	SELF-RELIANT TRUSTWORTHINESS				
SA-8(17)	SECURE DISTRIBUTED COMPOSITION				
SA-8(18)	TRUSTED COMMUNICATIONS CHANNELS				
SA-8(19)	CONTINUOUS PROTECTION				
SA-8(20)	SECURE METADATA MANAGEMENT				
SA-8(21)	SELF-ANALYSIS				
SA-8(22)	ACCOUNTABILITY AND TRACEABILITY				
SA-8(23)	SECURE DEFAULTS				
SA-8(24)	SECURE FAILURE AND RECOVERY				
SA-8(25)	ECONOMIC SECURITY				
SA-8(26)	PERFORMANCE SECURITY				
SA-8(27)	HUMAN FACTORED SECURITY				
SA-8(28)	ACCEPTABLE SECURITY				
SA-8(29)	REPEATABLE AND DOCUMENTED PROCEDURES				
SA-8(30)	PROCEDURAL RIGOR				
SA-8(31)	SECURE SYSTEM MODIFICATION				
SA-8(32)	SUFFICIENT DOCUMENTATION				
SA-9	**External System Services**	x	x	x	x
SA-9(1)	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS				
SA-9(2)	IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES			x	x
SA-9(3)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS				
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS				
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION				
SA-9(6)	ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS				
SA-9(7)	ORGANIZATION-CONTROLLED INTEGRITY CHECKING				
SA-9(8)	PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION				
SA-10	**Developer Configuration Management**			x	x
SA-10(1)	SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION				
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT				
SA-10(3)	HARDWARE INTEGRITY VERIFICATION				
SA-10(4)	TRUSTED GENERATION				
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL				
SA-10(6)	TRUSTED DISTRIBUTION				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-11	**Developer Testing and Evaluation**	x		x	x
SA-11(1)	STATIC CODE ANALYSIS				
SA-11(2)	THREAT MODELING AND VULNERABILITY ANALYSES				
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE				
SA-11(4)	MANUAL CODE REVIEWS				
SA-11(5)	PENETRATION TESTING				
SA-11(6)	ATTACK SURFACE REVIEWS				
SA-11(7)	VERIFY SCOPE OF TESTING AND EVALUATION				
SA-11(8)	DYNAMIC CODE ANALYSIS				
SA-11(9)	INTERACTIVE APPLICATION SECURITY TESTING				
SA-12	**Supply Chain Protection**	W: Moved to SR Family.			
SA-12(1)	ACQUISITION STRATEGIES, TOOLS, AND METHODS	W: Moved to SR-5.			
SA-12(2)	SUPPLIER REVIEWS	W: Moved to SR-6.			
SA-12(3)	TRUSTED SHIPPING AND WAREHOUSING	W: Incorporated into SR-3.			
SA-12(4)	DIVERSITY OF SUPPLIERS	W: Moved to SR-3(1).			
SA-12(5)	LIMITATION OF HARM	W: Moved to SR-3(2).			
SA-12(6)	MINIMIZING PROCUREMENT TIME	W: Incorporated into SR-5(1).			
SA-12(7)	ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	W: Moved to SR-5(2).			
SA-12(8)	USE OF ALL-SOURCE INTELLIGENCE	W: Incorporated into RA-3(2).			
SA-12(9)	OPERATIONS SECURITY	W: Moved to SR-7.			
SA-12(10)	VALIDATE AS GENUINE AND NOT ALTERED	W: Moved to SR-4(3).			
SA-12(11)	PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	W: Moved to SR-6(1).			
SA-12(12)	INTER-ORGANIZATIONAL AGREEMENTS	W: Moved to SR-8.			
SA-12(13)	CRITICAL INFORMATION SYSTEM COMPONENTS	W: Incorporated into MA-6 and RA-9.			
SA-12(14)	IDENTITY AND TRACEABILITY	W: Moved to SR-4(1)(2).			
SA-12(15)	PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	W: Incorporated into SR-3.			
SA-13	**Trustworthiness**	W: Incorporated into SA-8.			
SA-14	**Criticality Analysis**	W: Incorporated into RA-9.			
SA-14(1)	CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING	W: Incorporated into SA-20.			
SA-15	**Development Process, Standards, and Tools**			x	x
SA-15(1)	QUALITY METRICS				
SA-15(2)	SECURITY TRACKING TOOLS				
SA-15(3)	CRITICALITY ANALYSIS			x	x
SA-15(4)	THREAT MODELING AND VULNERABILITY ANALYSIS	W: Incorporated into SA-11(2).			
SA-15(5)	ATTACK SURFACE REDUCTION				
SA-15(6)	CONTINUOUS IMPROVEMENT				
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS				
SA-15(8)	REUSE OF THREAT AND VULNERABILITY INFORMATION				
SA-15(9)	USE OF LIVE DATA	W: Incorporated into SA-3(2).			
SA-15(10)	INCIDENT RESPONSE PLAN				
SA-15(11)	ARCHIVE SYSTEM OR COMPONENT				
SA-15(12)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-16	**Developer-Provided Training**				x
SA-17	**Developer Security Architecture and Design**				x
SA-17(1)	FORMAL POLICY MODEL				
SA-17(2)	SECURITY-RELEVANT COMPONENTS				
SA-17(3)	FORMAL CORRESPONDENCE				
SA-17(4)	INFORMAL CORRESPONDENCE				
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN				
SA-17(6)	STRUCTURE FOR TESTING				
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE				
SA-17(8)	ORCHESTRATION				
SA-17(9)	DESIGN DIVERSITY				
SA-18	**Tamper Resistance and Detection**	W: Moved to SR-9.			
SA-18(1)	MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE	W: Moved to SR-9(1).			
SA-18(2)	INSPECTION OF SYSTEMS OR COMPONENTS	W: Moved to SR-9(2).			
SA-19	**Component Authenticity**	W: Moved to SR-10.			
SA-19(1)	ANTI-COUNTERFEIT TRAINING	W: Moved to SR-10(1).			
SA-19(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR	W: Moved to SR-10(2).			
SA-19(3)	COMPONENT DISPOSAL	W: Moved to SR-10(3).			
SA-19(4)	ANTI-COUNTERFEIT SCANNING	W: Moved to SR-10(4).			
SA-20	**Customized Development of Critical Components**				
SA-21	**Developer Screening**				x
SA-21(1)	VALIDATION OF SCREENING	W: Incorporated into SA-21.			
SA-22	**Unsupported System Components**		x	x	x
SA-22(1)	ALTERNATIVE SOURCES FOR CONTINUED SUPPORT	W: Incorporated into SA-22.			
SA-23	**Specialization**				

865

3.18 SYSTEM AND COMMUNICATIONS PROTECTION FAMILY

Table 3-18 provides a summary of the controls and control enhancements assigned to the System and Communications Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-18: SYSTEM AND COMMUNICATIONS PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-1	**Policy and Procedures**		x	x	x
SC-2	**Separation of System and User Functionality**			x	x
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS				
SC-2(2)	DISASSOCIABILITY				
SC-3	**Security Function Isolation**				x
SC-3(1)	HARDWARE SEPARATION				
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS				
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY				
SC-3(4)	MODULE COUPLING AND COHESIVENESS				
SC-3(5)	LAYERED STRUCTURES				
SC-4	**Information in Shared System Resources**			x	x
SC-4(1)	SECURITY LEVELS	W: Incorporated into SC-4.			
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING				
SC-5	**Denial of Service Protection**		x	x	x
SC-5(1)	RESTRICT ABILITY TO ATTACK OTHER SYSTEMS				
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY				
SC-5(3)	DETECTION AND MONITORING				
SC-6	**Resource Availability**				
SC-7	**Boundary Protection**		x	x	x
SC-7(1)	PHYSICALLY SEPARATED SUBNETWORKS	W: Incorporated into SC-7.			
SC-7(2)	PUBLIC ACCESS	W: Incorporated into SC-7.			
SC-7(3)	ACCESS POINTS			x	x
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES			x	x
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION			x	x
SC-7(6)	RESPONSE TO RECOGNIZED FAILURES	W: Incorporated into SC-7(18).			
SC-7(7)	PREVENT SPLIT TUNNELING FOR REMOTE DEVICES			x	x
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS			x	x
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC				
SC-7(10)	PREVENT EXFILTRATION				
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC				
SC-7(12)	HOST-BASED PROTECTION				
SC-7(13)	ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS				
SC-7(14)	PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS				
SC-7(15)	NETWORKED PRIVILEGED ACCESSES				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-7(16)	PREVENT DISCOVERY OF COMPONENTS AND DEVICES				
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS				
SC-7(18)	FAIL SECURE				x
SC-7(19)	BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS				
SC-7(20)	DYNAMIC ISOLATION AND SEGREGATION				
SC-7(21)	ISOLATION OF SYSTEM COMPONENTS				x
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS				
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE				
SC-7(24)	PERSONALLY IDENTIFIABLE INFORMATION				
SC-7(25)	UNCLASSIFIED NATIONAL SECURITY CONNECTIONS				
SC-7(26)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS				
SC-7(27)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS				
SC-7(28)	CONNECTIONS TO PUBLIC NETWORKS				
SC-7(29)	SEPARATE SUBNETS TO ISOLATE FUNCTIONS				
SC-8	**Transmission Confidentiality and Integrity**			x	x
SC-8(1)	CRYPTOGRAPHIC PROTECTION			x	x
SC-8(2)	PRE- AND POST-TRANSMISSION HANDLING				
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS				
SC-8(4)	CONCEAL OR RANDOMIZE COMMUNICATIONS				
SC-8(5)	PROTECTED DISTRIBUTION SYSTEM				
SC-9	Transmission Confidentiality	W: Incorporated into SC-8.			
SC-10	**Network Disconnect**			x	x
SC-11	**Trusted Path**				
SC-11(1)	IRREFUTABLE COMMUNICATIONS PATH				
SC-12	**Cryptographic Key Establishment and Management**		x	x	x
SC-12(1)	AVAILABILITY				x
SC-12(2)	SYMMETRIC KEYS				
SC-12(3)	ASYMMETRIC KEYS				
SC-12(4)	PKI CERTIFICATES	W: Incorporated into SC-12.			
SC-12(5)	PKI CERTIFICATES / HARDWARE TOKENS	W: Incorporated into SC-12.			
SC-12(6)	PHYSICAL CONTROL OF KEYS				
SC-13	**Cryptographic Protection**		x	x	x
SC-13(1)	FIPS-VALIDATED CRYPTOGRAPHY	W: Incorporated into SC-13.			
SC-13(2)	NSA-APPROVED CRYPTOGRAPHY	W: Incorporated into SC-13.			
SC-13(3)	INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS	W: Incorporated into SC-13.			
SC-13(4)	DIGITAL SIGNATURES	W: Incorporated into SC-13.			
SC-14	Public Access Protections	W: Incorporated into AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.			
SC-15	**Collaborative Computing Devices and Applications**		x	x	x
SC-15(1)	PHYSICAL OR LOGICAL DISCONNECT				
SC-15(2)	BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	W: Incorporated into SC-7.			
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS				
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-16	**Transmission of Security and Privacy Attributes**				
SC-16(1)	INTEGRITY VERIFICATION				
SC-16(2)	ANTI-SPOOFING MECHANISMS				
SC-17	**Public Key Infrastructure Certificates**			x	x
SC-18	**Mobile Code**			x	x
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS				
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE				
SC-18(3)	PREVENT DOWNLOADING AND EXECUTION				
SC-18(4)	PREVENT AUTOMATIC EXECUTION				
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS				
SC-19	**Voice over Internet Protocol**	W: Technology-specific; addressed by other controls for protocols.			
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**		x	x	x
SC-20(1)	CHILD SUBSPACES	W: Incorporated into SC-20.			
SC-20(2)	DATA ORIGIN AND INTEGRITY				
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**		x	x	x
SC-21(1)	DATA ORIGIN AND INTEGRITY	W: Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**		x	x	x
SC-23	**Session Authenticity**			x	x
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT				
SC-23(2)	USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS	W: Incorporated into AC-12(1).			
SC-23(3)	UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS				
SC-23(4)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	W: Incorporated into SC-23(3).			
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES				
SC-24	**Fail in Known State**				x
SC-25	**Thin Nodes**				
SC-26	**Decoys**				
SC-26(1)	DETECTION OF MALICIOUS CODE	W: Incorporated into SC-35.			
SC-27	**Platform-Independent Applications**				
SC-28	**Protection of Information at Rest**			x	x
SC-28(1)	CRYPTOGRAPHIC PROTECTION			x	x
SC-28(2)	OFF-LINE STORAGE				
SC-28(3)	CRYPTOGRAPHIC KEYS				
SC-29	**Heterogeneity**				
SC-29(1)	VIRTUALIZATION TECHNIQUES				
SC-30	**Concealment and Misdirection**				
SC-30(1)	VIRTUALIZATION TECHNIQUES	W: Incorporated into SC-29(1).			
SC-30(2)	RANDOMNESS				
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS				
SC-30(4)	MISLEADING INFORMATION				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS				
SC-31	**Covert Channel Analysis**				
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY				
SC-31(2)	MAXIMUM BANDWIDTH				
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS				
SC-32	**System Partitioning**				
SC-32(1)	SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS				
SC-33	Transmission Preparation Integrity	W: Incorporated into SC-8.			
SC-34	**Non-Modifiable Executable Programs**				
SC-34(1)	NO WRITABLE STORAGE				
SC-34(2)	INTEGRITY PROTECTION AND READ-ONLY MEDIA				
SC-34(3)	HARDWARE-BASED PROTECTION				
SC-35	**External Malicious Code Identification**				
SC-36	**Distributed Processing and Storage**				
SC-36(1)	POLLING TECHNIQUES				
SC-36(2)	SYNCHRONIZATION				
SC-37	**Out-of-Band Channels**				
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION				
SC-38	**Operations Security**				
SC-39	**Process Isolation**		x	x	x
SC-39(1)	HARDWARE SEPARATION				
SC-39(2)	SEPARATE EXECUTION DOMAIN PER THREAD				
SC-40	**Wireless Link Protection**				
SC-40(1)	ELECTROMAGNETIC INTERFERENCE				
SC-40(2)	REDUCE DETECTION POTENTIAL				
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION				
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION				
SC-41	**Port and I/O Device Access**				
SC-42	**Sensor Capability and Data**				
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES				
SC-42(2)	AUTHORIZED USE				
SC-42(3)	PROHIBIT USE OF DEVICES				
SC-42(4)	NOTICE OF COLLECTION				
SC-42(5)	COLLECTION MINIMIZATION				
SC-43	**Usage Restrictions**				
SC-44	**Detonation Chambers**				
SC-45	**System Time Synchronization**				
SC-46	**Cross Domain Policy Enforcement**				
SC-47	**Communications Path Diversity**				
SC-48	**Sensor Relocation**				
SC-48(1)	DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES				
SC-49	**Hardware-Enforced Separation and Policy Enforcement**				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-50	**Software-Enforced Separation and Policy Enforcement**				
SC-51	**Operational and Internet-Based Technologies**				

872

3.19 SYSTEM AND INFORMATION INTEGRITY FAMILY

Table 3-19 provides a summary of the controls and control enhancements assigned to the System and Information Integrity Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-19: SYSTEM AND INFORMATION INTEGRITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-1	**Policy and Procedures**	x	x	x	x
SI-2	**Flaw Remediation**		x	x	x
SI-2(1)	CENTRAL MANAGEMENT				x
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS			x	x
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS				
SI-2(4)	AUTOMATED PATCH MANAGEMENT TOOLS				
SI-2(5)	AUTOMATIC SOFTWARE AND FIRMWARE UPDATES				
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE				
SI-3	**Malicious Code Protection**		x	x	x
SI-3(1)	CENTRAL MANAGEMENT			x	x
SI-3(2)	AUTOMATIC UPDATES	W: Incorporated into SI-3.			
SI-3(3)	NON-PRIVILEGED USERS	W: Incorporated into AC-6(10).			
SI-3(4)	UPDATES ONLY BY PRIVILEGED USERS				
SI-3(5)	PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
SI-3(6)	TESTING AND VERIFICATION				
SI-3(7)	NONSIGNATURE-BASED DETECTION	W: Incorporated into SI-3.			
SI-3(8)	DETECT UNAUTHORIZED COMMANDS				
SI-3(9)	AUTHENTICATE REMOTE COMMANDS				
SI-3(10)	MALICIOUS CODE ANALYSIS				
SI-4	**System Monitoring**		x	x	x
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM				
SI-4(2)	AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS			x	x
SI-4(3)	AUTOMATED TOOL AND MECHANISM INTEGRATION				
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC			x	x
SI-4(5)	SYSTEM-GENERATED ALERTS			x	x
SI-4(6)	RESTRICT NON-PRIVILEGED USERS	W: Incorporated into AC-6(10).			
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS				
SI-4(8)	PROTECTION OF MONITORING INFORMATION	W: Incorporated into SI-4.			
SI-4(9)	TESTING OF MONITORING TOOLS AND MECHANISMS				
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS				x
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES				
SI-4(12)	AUTOMATED ORGANIZATION-GENERATED ALERTS				x
SI-4(13)	ANALYZE TRAFFIC AND EVENT PATTERNS				
SI-4(14)	WIRELESS INTRUSION DETECTION				x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS				
SI-4(16)	CORRELATE MONITORING INFORMATION				
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS				
SI-4(18)	ANALYZE TRAFFIC AND COVERT EXFILTRATION				
SI-4(19)	RISK FOR INDIVIDUALS				
SI-4(20)	PRIVILEGED USERS				x
SI-4(21)	PROBATIONARY PERIODS				
SI-4(22)	UNAUTHORIZED NETWORK SERVICES				x
SI-4(23)	HOST-BASED DEVICES				
SI-4(24)	INDICATORS OF COMPROMISE				
SI-4(25)	OPTIMIZE NETWORK TRAFFIC ANALYSIS				
SI-5	**Security Alerts, Advisories, and Directives**		x	x	x
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES				x
SI-6	**Security and Privacy Function Verification**				x
SI-6(1)	NOTIFICATION OF FAILED SECURITY TESTS	W: Incorporated into SI-6.			
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING				
SI-6(3)	REPORT VERIFICATION RESULTS				
SI-7	**Software, Firmware, and Information Integrity**			x	x
SI-7(1)	INTEGRITY CHECKS			x	x
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS				x
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS				
SI-7(4)	TAMPER-EVIDENT PACKAGING	W: Incorporated into SR-9.			
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS				x
SI-7(6)	CRYPTOGRAPHIC PROTECTION				
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE			x	x
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS				
SI-7(9)	VERIFY BOOT PROCESS				
SI-7(10)	PROTECTION OF BOOT FIRMWARE				
SI-7(11)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	W: Moved to CM-7(6).			
SI-7(12)	INTEGRITY VERIFICATION				
SI-7(13)	CODE EXECUTION IN PROTECTED ENVIRONMENTS	W: Moved to CM-7(7).			
SI-7(14)	BINARY OR MACHINE EXECUTABLE CODE	W: Moved to CM-7(8).			
SI-7(15)	CODE AUTHENTICATION				x
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION				
SI-7(17)	RUNTIME APPLICATION SELF-PROTECTION				
SI-8	**Spam Protection**			x	x
SI-8(1)	CENTRAL MANAGEMENT			x	x
SI-8(2)	AUTOMATIC UPDATES			x	x
SI-8(3)	CONTINUOUS LEARNING CAPABILITY				
SI-9	**Information Input Restrictions**	W: Incorporated into AC-2, AC-3, AC-5, AC-6.			
SI-10	**Information Input Validation**			x	x
SI-10(1)	MANUAL OVERRIDE CAPABILITY				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-10(2)	REVIEW AND RESOLVE ERRORS				
SI-10(3)	PREDICTABLE BEHAVIOR				
SI-10(4)	TIMING INTERACTIONS				
SI-10(5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS				
SI-10(6)	INJECTION PREVENTION				
SI-11	**Error Handling**			x	x
SI-12	**Information Management and Retention**	x	x	x	x
SI-12(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x			
SI-12(2)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	x			
SI-12(3)	INFORMATION DISPOSAL	x			
SI-13	**Predictable Failure Prevention**				
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES				
SI-13(2)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	W: Incorporated into SI-7(16).			
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS				
SI-13(4)	STANDBY COMPONENT INSTALLATION AND NOTIFICATION				
SI-13(5)	FAILOVER CAPABILITY				
SI-14	**Non-Persistence**				
SI-14(1)	REFRESH FROM TRUSTED SOURCES				
SI-14(2)	NON-PERSISTENT INFORMATION				
SI-14(3)	NON-PERSISTENT CONNECTIVITY				
SI-15	**Information Output Filtering**				
SI-16	**Memory Protection**			x	x
SI-17	**Fail-Safe Procedures**				
SI-18	**Personally Identifiable Information Quality Operations**	x			
SI-18(1)	AUTOMATION				
SI-18(2)	DATA TAGS				
SI-18(3)	COLLECTION				
SI-18(4)	INDIVIDUAL REQUESTS	x			
SI-18(5)	NOTICE OF COLLECTION OR DELETION				
SI-19	**De-identification**	x			
SI-19(1)	COLLECTION				
SI-19(2)	ARCHIVING				
SI-19(3)	RELEASE				
SI-19(4)	REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS				
SI-19(5)	STATISTICAL DISCLOSURE CONTROL				
SI-19(6)	DIFFERENTIAL PRIVACY				
SI-19(7)	VALIDATED SOFTWARE				
SI-19(8)	MOTIVATED INTRUDER				
SI-20	**Tainting**				
SI-21	**Information Refresh**				
SI-22	**Information Diversity**				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-23	**Information Fragmentation**				

879

3.20 SUPPLY CHAIN RISK MANAGEMENT FAMILY

Table 3-20 provides a summary of the controls and control enhancements assigned to the Supply Chain Risk Management Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate.

TABLE 3-20: SUPPLY CHAIN RISK MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SR-1	**Policy and Procedures**		x	x	x
SR-2	**Supply Chain Risk Management Plan**		x	x	x
SR-2(1)	ESTABLISH SCRM TEAM		x	x	x
SR-3	**Supply Chain Controls and Processes**		x	x	x
SR-3(1)	DIVERSE SUPPLY BASE				
SR-3(2)	LIMITATION OF HARM				
SR-4	**Provenance**				
SR-4(1)	IDENTITY				
SR-4(2)	TRACK AND TRACE				
SR-4(3)	VALIDATE AS GENUINE AND NOT ALTERED				
SR-5	**Acquisition Strategies, Tools, and Methods**		x	x	x
SR-5(1)	ADEQUATE SUPPLY				
SR-5(2)	ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE				
SR-6	**Supplier Reviews**			x	x
SR-6(1)	PENETRATION TESTING AND ANALYSIS				
SR-7	**Supply Chain Operations Security**				
SR-8	**Notification Agreements**		x	x	x
SR-9	**Tamper Resistance and Detection**				x
SR-9(1)	MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE				x
SR-10	**Inspection of Systems and Components**		x	x	x
SR-11	**Component Authenticity**		x	x	x
SR-11(1)	ANTI-COUNTERFEIT TRAINING		x	x	x
SR-11(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR		x	x	x
SR-11(3)	COMPONENT DISPOSAL		x	x	x
SR-11(4)	ANTI-COUNTERFEIT SCANNING				

REFERENCES

LAWS, POLICIES, INSTRUCTIONS, STANDARDS, GUIDELINES, AND INTERNAL REPORTS

LAWS	
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
POLICIES AND INSTRUCTIONS	
[CNSSI 1253]	Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSP 22]	Committee on National Security Systems Policy No. 22, *Cybersecurity Risk Management Policy*, August 2016. https://www.cnss.gov/CNSS/issuances/Policies.cfm
[DODI 8510.01]	Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf
[OMB A-130]	Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
STANDARDS, GUIDELINES, AND INTERNAL REPORTS	
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53] Joint Task Force Transformation Initiative (2019) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5.

[SP 800-59] Barker W (2003) Guideline for Identifying an Information System as a National Security System. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-59. https://doi.org/10.6028/NIST.SP.800-59

[SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[IR 8011 v1]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal (NISTIR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1
[IR 8062]	Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (NISTIR) 8062. https://doi.org/10.6028/NIST.IR.8062
MISCELLANEOUS PUBLICATIONS AND WEBSITES	
[DSB 2017]	Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf
[NIST CSRC]	National Institute of Standards and Technology Computer Security Resource Center (CSRC). https://csrc.nist.gov
[SCOR]	Security Control Overlay Repository (SCOR). https://csrc.nist.gov/Projects/Risk-Management/scor

889

APPENDIX A

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix A provides definitions for terminology used in NIST SP 800-53B. Sources for terms used in this publication are cited as applicable. Where no citation is noted, the source of the definition is SP 800-53.

agency [OMB A-130]	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. See *executive agency*.
assignment statement	A control parameter that allows an organization to assign a specific, organization-defined value to the control or control enhancement (e.g., assigning a list of roles to be notified or a value for the frequency of testing). See *organization-defined control parameters* and *selection statement*.
assurance	Grounds for justified confidence that a [security or privacy] claim has been or will be achieved. *Note 1:* Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims), and the claims themselves may be interrelated. *Note 2:* Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.
authorizing official [OMB A-130]	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
availability [44 USC 3552]	Ensuring timely and reliable access to and use of information.
capability	A combination of mutually reinforcing security and/or privacy controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.
common control [OMB A-130]	A security or privacy control that is inherited by multiple information systems or programs.
common control provider [SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security or privacy controls inheritable by systems).

compensating controls	The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization.
confidentiality [44 USC 3552]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
control baseline [FIPS 200, Adapted]	The set of security and privacy controls defined for a low-impact, moderate-impact, or high-impact system or selected based on the privacy selection criteria that provide a starting point for the tailoring process.
control enhancement	Augmentation of a security or privacy control to build in additional but related functionality to the control, increase the strength of the control, or add assurance to the control.
control inheritance	A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *common control*.
environment of operation [OMB A-130]	The physical surroundings in which an information system processes, stores, and transmits information.
high-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.
hybrid control [OMB A-130]	A security or privacy control that is implemented for an information system, in part as a common control and in part as a system-specific control.
impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
impact value [FIPS 199]	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high.
information [OMB A-130]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

information security [OMB A-130]	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [OMB A-130]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
integrity [44 USC 3552]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
low-impact system [FIPS 200]	A system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.
moderate-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a potential impact value of high.
national security system [OMB A-130]	Any system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure, including federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements.
organization-defined control parameter	The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a pre-defined list provided as part of the control or control enhancement. See *assignment statement* and *selection statement*.

overlay [OMB A-130]	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. See *tailoring*.
personally identifiable information [OMB A-130]	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS Publication 199 low), a serious adverse effect (FIPS Publication 199 moderate), or a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privacy control [OMB A-130]	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
privacy impact assessment [OMB A-130]	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.
privacy plan [OMB A-130]	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
privacy program plan [OMB A-130]	A formal document that provides an overview of an agency'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.

processing [IR 8062]	Operation or set of operations performed upon PII that can include but is not limited to the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of PII.
risk [OMB A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
risk assessment [SP 800-39]	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses and analyses of privacy problems arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with *risk analysis*.
risk management [OMB A-130]	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time.
scoping considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security and privacy controls in the control baselines. Considerations include policy or regulatory, technology, physical infrastructure, system component allocation, public access, scalability, common control, operational or environmental, and security objective.
security category [OMB A-130]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.
security control [OMB A-130]	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
security control baseline [OMB A-130]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

security functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
security functions	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
security objective [FIPS 199]	Confidentiality, integrity, or availability.
security plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems. See *system security plan*.
security requirement [FIPS 200, Adapted]	A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. *Note:* Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
selection statement	A control parameter that allows an organization to select a value from a list of pre-defined values provided as part of the control or control enhancement (e.g., selecting to either restrict an action or prohibit an action). See *assignment statement* and *organization-defined control parameter*.
senior agency official for privacy [OMB A-130]	The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.
system owner (or program manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

system security plan	See *security plan*.
system-specific control [OMB A-130]	A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.
tailored control baseline	A set of controls resulting from the application of tailoring guidance to a control baseline. See *tailoring*.
tailoring	The process by which security and privacy control baselines are modified by identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating controls, assigning specific values to organization-defined control parameters, supplementing baselines with additional controls or control enhancements, and providing additional specification information for control implementation.

896

897 APPENDIX B

898 # ACRONYMS

899 COMMON ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CSRC	Computer Security Resource Center
DoD	Department of Defense
DoDI	Department of Defense Instruction
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
IT	Information Technology
ITL	Information Technology Laboratory
JTF	Joint Task Force
MOD	Moderate
NIST	National Institute of Standards and Technology
O/S	Organization or Information System
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMF	Risk Management Framework
SAOP	Senior Agency Official for Privacy
SP	Special Publication

900

APPENDIX C

OVERLAYS

ADDITIONAL CUSTOMIZATION OPTIONS FOR CONTROL BASELINES

In certain situations, it may be beneficial for organizations to apply the tailoring guidance to develop a set of controls for particular communities of interest or to address specialized requirements, technologies implemented, or unique missions or environments of operation. An organization may decide to establish a set of controls for specific applications or use cases, including for example: cloud-based services that could be applied to organizations procuring or implementing such services; industrial control systems generating or transmitting electric power or controlling environmental systems in facilities; systems processing, storing, or transmitting classified information; or systems controlling the safety of transportation systems. In these examples, overlays can be developed for each sector, technology area, unique circumstances, or environments and promulgated to large communities of interest—thus achieving standardized security and privacy capabilities, consistency of implementation, and cost-effective security and privacy solutions.

To address the need for specialized sets of controls for communities of interest, systems, and organizations, the concept of *overlay* is introduced. An overlay is a fully specified set of controls, control enhancements, and other supporting information (e.g., parameter values) derived from the application of tailoring guidance to control baselines.[39] Overlays[40] complement and further refine the initial control baselines by providing an opportunity for the community of interest to add, modify, or eliminate controls; providing control applicability and interpretations for specific technologies, computing paradigms, environments of operation, types of systems, types of missions/operations, operating modes, industry sectors, and statutory/regulatory requirements; and establishing parameter values for assignment and/or selection statements in controls and control enhancements agreeable to communities of interest. Organizations use the overlay concept when there is divergence from the basic assumptions used to create the initial control baselines. In many ways, overlays function like alternative control baselines and may require tailoring like the baselines in Chapter Three. Using an overlay is not a substitute for the full tailoring process. The overlay concept is only applicable to groups of like systems, technologies, or communities of interest (i.e., the overlay concept is not appropriate for an individual system since the tailoring process is used to adapt control baselines for individual systems).

The full range of tailoring activities can be employed by organizations to provide a structured approach for developing overlays that support the areas described above. Overlays provide an opportunity to build consensus across communities of interest and develop security and privacy plans for systems and organizations that have broad-based support for specific circumstances, situations, or conditions. Categories of overlays that may be useful include:

[39] Control baselines can include the federal baselines in Chapter Three; baselines developed by State, local, or tribal governments; or baselines developed by private sector organizations (e.g., manufacturers, consortia, trade associations, industry and critical infrastructure sectors).

[40] Tailored control baselines may also be referred to as *overlays*. An organizationally tailored control baseline is analogous to an organization-wide overlay since an overlay is a tailored baseline that services a community of interest, in this case, the organization.

- Communities of interest, industry sectors, or coalitions/partnerships, such as healthcare, law enforcement, intelligence, financial, manufacturing, transportation, energy, and allied collaboration/sharing
- Information technologies and computing paradigms, such as virtualized systems, cloud, mobile, smart grid, and cross-domain solutions
- Environments of operation, such as space, tactical, or sea
- Types of systems and operating modes, such as industrial/process control systems, weapons systems, single-user systems, standalone systems, IoT devices and sensors
- Types of missions/operations, such as counterterrorism, first responders, research, development, test, and evaluation
- Statutory/regulatory requirements, such as Foreign Intelligence Surveillance Act, Health Insurance Portability and Accountability Act, FISMA, and Privacy Act

Overlays provide uniformity and efficiency of control selection by presenting tailoring options developed by security and privacy experts and other subject matter experts to information system owners responsible for implementing and maintaining such systems. There are many options that can be used to construct overlays, depending on the specificity desired by the overlay developers. Some overlays may be very specific with respect to the hardware, firmware, and software that form the key components of the information system and the environment in which the system operates. Other overlays may be more abstract in order to be applicable to a large class of systems that may be deployed in different operational environments.

PUBLICATION OF OVERLAYS

Overlays can be published independently in a variety of venues and publications, including OMB policies, CNSS Instructions, NIST Special Publications, industry standards, and sector-specific guidance. The Security Control Overlay Repository (SCOR) provides stakeholders with a platform for voluntarily sharing security control overlays. To learn more about the repository, including instructions on how to submit an overlay, and to obtain a list of published overlays, see [SCOR].

Organizations may use the following outline when developing overlays.[41] The outline is provided as an example only. Organizations may use any format based on specific organizational needs and the type of overlay being developed. The level of detail included in the overlay is at the discretion of the organization initiating the overlay but should be of sufficient breadth and depth to provide an appropriate justification and rationale for the overlay, including any risk-based decisions made during the overlay development process. The example overlay outline includes the following sections:

[41] While organizations are encouraged to use the overlay concept to tailor control baselines, the development of widely divergent overlays on the same topic may prove to be counterproductive. The overlay concept is most effective when communities of interest work together to create consensus-based overlays that are not duplicative.

- Identification
- Overlay characteristics
- Applicability
- Overlay summary
- Overlay control specifications
- Tailoring considerations
- Terms and definitions
- Additional information or instructions

Identification

Organizations identify the overlay by providing a unique name for the overlay, a version number and date, the version of [SP 800-53] used to create the overlay, other documentation used to create the overlay, author or authoring group and point of contact, and type of organizational approval received. Organizations define how long the overlay is to be in effect and any events that may trigger an update to the overlay other than changes to [SP 800-53] or organization-specific guidance. If there are no unique events that can trigger an update for the overlay, this section provides that notation.

Overlay Characteristics

Organizations describe the characteristics that define the intended use of the overlay in order to help potential users select the most appropriate overlay for their missions or business functions. This may include, for example:

- Describing the physical environment where the information system will be used or operate (e.g., inside a guarded building within the continental United States, in an unmanned space vehicle, while traveling for business to a foreign country that is known for attempting to gain access to sensitive or classified information, or in a mobile vehicle that is in close proximity to hostile entities)
- The type of information that will be processed, stored, or transmitted by the system (e.g., personal identity and authentication information, financial management information, facilities, fleet, and equipment management information, defense and national security information, system development information)
- The functionality within the information system or the type of system (e.g., standalone system, industrial/process control system, or cross-domain system)
- Other characteristics related to the overlay that help protect organizational missions/business functions, information systems, information, or individuals from a specific set of threats that may not be addressed by the assumptions described in Section 2.3.

Applicability

Organizations provide criteria to assist potential users of the overlay in determining whether or not the overlay applies to a particular information system or environment of operation. Typical

formats may include a list of questions or a decision tree based on the description of the characteristics of the system (including associated applications) and its environment of operation at the level of specificity appropriate to the overlay.

Overlay Summary

Organizations provide a brief summary of the characteristics of the overlay. The summary may include the controls and control enhancements that are affected by the overlay; an indication of which controls and control enhancements are selected or not selected based on the specific characteristics and assumptions in the overlay, the tailoring guidance provided in Section 2.4, or any organization-specific guidance; the selected controls and control enhancements including parameter values; and references to applicable laws, Executive Orders, directives, instructions, regulations, policies, or standards.

Overlay Control Specifications

Organizations provide a comprehensive expression of the controls and control enhancements in the overlay as part of the tailoring process. This may include the justification for selecting or not selecting a specific control or control enhancement; modifications to the control discussion section that address the characteristics of the overlay and the environments in which the overlay is intended to be used; unique parameter values for control selection or assignment statements; specific statutory and/or regulatory requirements (above and beyond FISMA) that are met by a control or control enhancement; recommendations for compensating controls, as appropriate; and guidance that extends the capability of the control or control enhancement by specifying additional functionality, altering the strength of mechanism, or adding or limiting implementation options.

Tailoring Considerations

Organizations provide information to system owners and authorizing officials to consider during the tailoring process when determining the set of controls and control enhancements applicable to their specific information systems. This is especially important for overlays that are used in an environment of operation different from the one assumed by the control baselines in Chapter Three. In addition, organizations can provide guidance on the use of multiple overlays applied to a control baseline and address any potential conflicts that may arise between the controls in the baselines and overlay specifications.

Terms and Definitions

Organizations provide any terms and associated definitions that are unique and relevant to the overlay. If there are no unique terms or definitions for the overlay, that is stated in this section.

Additional Information or Instructions

Organizations provide any additional information or instructions relevant to the overlay not covered in the previous sections.