NIST Computer Security Division csrc.nist.gov

Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Kelley Dempsey
Computer Security Division
Information Technology Laboratory

Greg Witte
Doug Rike
G2, Inc.
Annapolis Junction, MD

February 19, 2014

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

Abstract

This white paper provides an overview of NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which was published April 30, 2013.

Keywords

assurance; computer security; FIPS Publication 199; FIPS Publication 200, FISMA; Privacy Act; Risk Management Framework; security controls; security requirements

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Computer Security Division programs, projects and publications, visit the Computer Security Resource Center, csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

Table of Contents

List of Figures

1 Introduction

In April, 2013, NIST published an update, Revision 4, to NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*. The guide was developed and is maintained by the Joint Task Force Transformation Initiative Interagency Working Group, part of an ongoing information security partnership among the U.S. Department of Defense, the Intelligence Community, the Committee on National Security Systems, the Department of Homeland Security, and U.S. federal civil agencies.

SP 800-53 Revision 4 has been updated to reflect the evolving technology and threat space. Example areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems. The revision also contains a new appendix of privacy controls, and related implementation guidance (Appendix J), based on the Fair Information Practice Principles (FIPPs), a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.

SP 800-53 Revision 4 is part of the NIST Special Publication 800-series that reports on the NIST Information Technology Laboratory's (ITL) computer security-related research, guidelines, and outreach. The publication provides a comprehensive set of security controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs according to the organization's missions, environments of operation, and technologies used.

As the risk to an information system's confidentiality, integrity and/or availability increases, the need for additional controls to protect the system may also increase accordingly. SP 800-53 Revision 4 provides the security control baselines as the starting point for the security control selection process. The baselines are chosen based on the security category and associated impact level of information systems as described in Federal Information Processing Standard Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

A separate guideline, SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations,* provides specific guidelines that facilitate periodic assessment of security controls to ensure that controls have been implemented correctly, are operating as intended, and are meeting the organization's security requirements.

2 NIST SP 800-53 Revision 4 and the Risk Management Framework (RMF)

NIST SP 800-39, *Managing Information Security Risk*, defines risk management as "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, and reputation), organizational assets, individuals, other organizations, and the Nation". To integrate the risk management process throughout an organization and to address its mission and business concerns, a three-tiered approach is employed. The process is carried out across three tiers with the objective of continuous improvement in the organization's risk-related activities, with effective communication among tiers and stakeholders. Figure 1 illustrates the three-tiered approach to risk management.

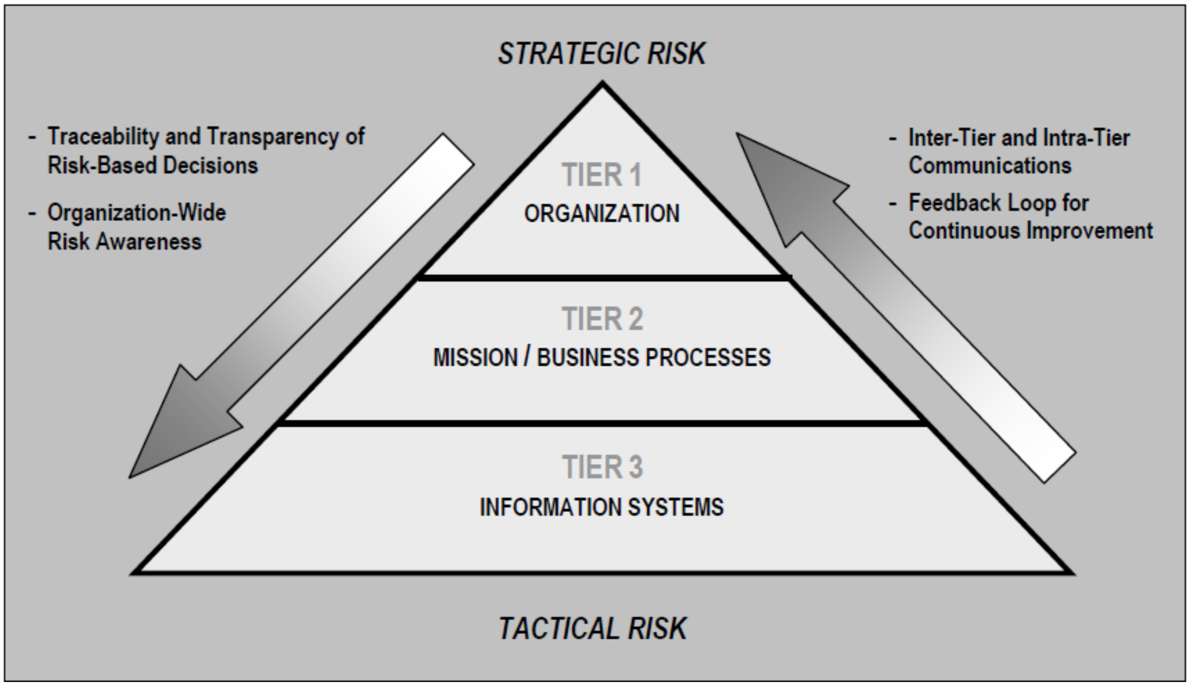
STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Figure 1: Risk Management 3-Tiered Approach

The NIST Risk Management Framework (RMF), described in NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach,* is a methodology for implementing risk management at the information systems tier. The RMF (depicted in Figure 2) identifies six distinct steps that provide a disciplined and structured process to integrate information security risk management activities into the system development life cycle. The RMF addresses security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate.

The security controls in SP 800-53 Rev. 4 support Step Two of the RMF, and a detailed catalog of these controls is provided in Appendix F. For ease of use in the security control selection and specification process, controls are organized into eighteen families, each containing security controls related to the general security topic of the family. Security controls involve aspects of policy, oversight, supervision, manual processes, individual actions, or automated mechanisms implemented by information systems/devices. The security control structure consists of the following components: (i) a control section; (ii) a supplemental guidance section; (iii) a control enhancements section; (iv) a references section; and (v) a priority and baseline allocation section.

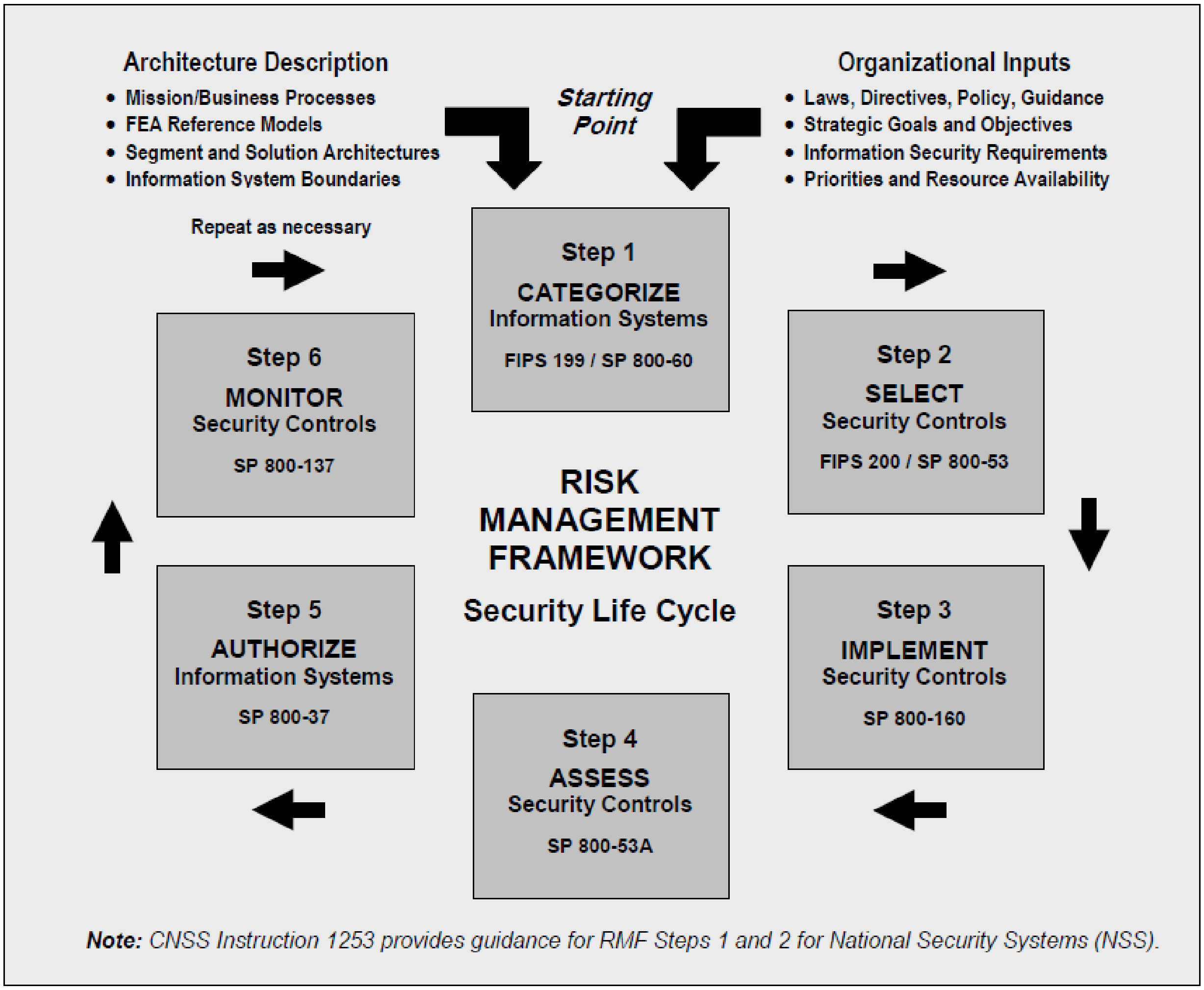
Architecture Description
• Mission/Business Processes
• FEA Reference Models
• Segment and Solution Architectures
• Information System Boundaries
Starting Point
Organizational Inputs
• Laws, Directives, Policy, Guidance
• Strategic Goals and Objectives
• Information Security Requirements
• Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORIZE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

Figure 2: The Risk Management Framework

3 Control Baselines and Tailoring

To assist organizations in making the appropriate selection of security controls for information systems, the concept of security control baselines is introduced. Security control baselines are the starting point for the security control selection process and are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS Publication 199 and FIPS Publication 200, respectively (Step One of the RMF). SP 800-53 Rev. 4 states that "the security controls and control enhancements listed in the initial baselines are not a minimum— but rather a proposed starting point from which controls and controls enhancements may be removed or added." Appendix D provides a listing of baseline security controls corresponding to the low-impact, moderate-impact, and high-impact information systems, using the high water mark defined in FIPS Publication 200.

The security control baselines address the security needs of a broad and diverse set of constituencies, and are developed based on a number of general assumptions, including common environmental, operational, and functional considerations. The baselines also assume typical threats facing common information systems. Articulating the underlying assumptions is a key element in the initial risk framing step of the risk management process described in NIST SP 800-39. To ensure that an appropriate set of controls is identified to provide security commensurate with risk, organizations tailor the controls to align with specific security needs. Organizations may perform tailoring at the organization level for all information systems, in support of a particular line of business or mission/business process, at the individual information system level, or by using a combination of the above. The tailoring process is comprised of several steps, as described in SP 800-53 Rev. 4 Section 3.2. These actions include:

- Identifying and designating common controls - controls that may be inherited by one or more information systems. If an information system inherits a common control, such as environmental controls within a data center, that system does not need to explicitly implement that control.
- Applying scoping considerations – these, when applied in conjunction with risk management guidance, can eliminate unnecessary security controls from the initial security control baselines and help ensure that organizations select *only* those controls needed to provide the appropriate level of protection for information systems. When scoping considerations are applied, compensating controls may need to be selected to provide alternative means to achieve security requirements.
- Supplementing baselines - additional security controls and control enhancements are selected if needed to address specific threats and vulnerabilities.

4 Documenting the Control Selection Process

To aid in review activities, security planning, and risk assessments, organizations document the relevant decisions taken during the security control selection process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for organizational information systems with respect to the potential impact on an organization's mission and business.

The resulting tailored baseline set of security controls and the supporting rationale for the selection decisions (including any information system use restrictions required by organizations) are documented in system security plans. Documenting significant risk management decisions in the security control selection process is imperative so that authorizing officials have access to necessary information to make informed authorization decisions for organizational information systems, as demonstrated in Figure 3.

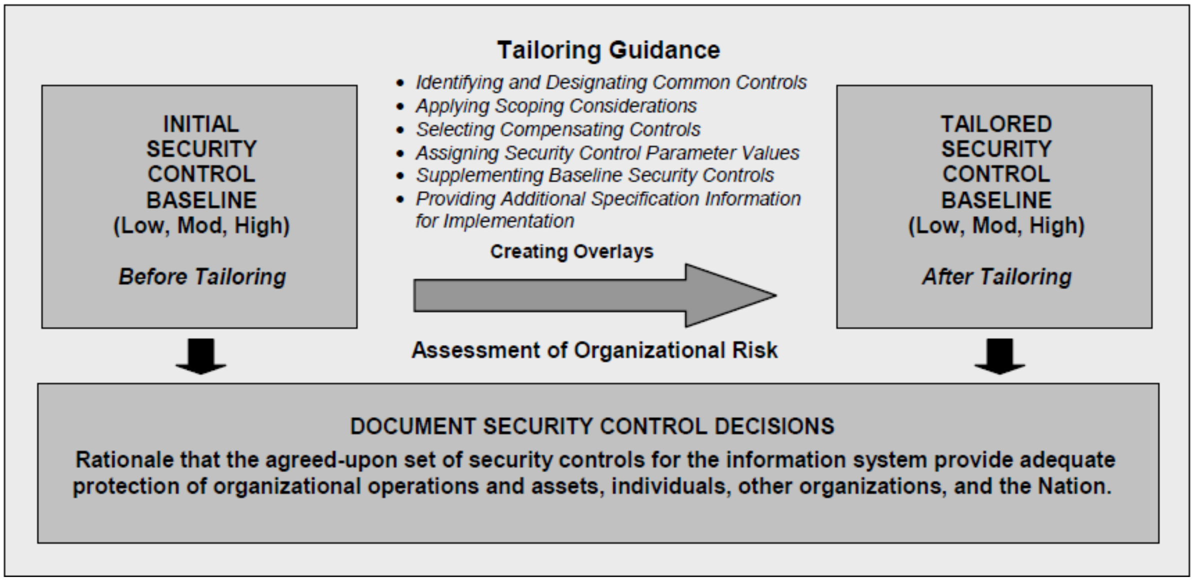
Tailoring Guidance
Identifying and Designating Common Controls
Applying Scoping Considerations
Selecting Compensating Controls
Assigning Security Control Parameter Values
Supplementing Baseline Security Controls
Providing Additional Specification Information for Implementation
Creating Overlays
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
DOCUMENT SECURITY CONTROL DECISIONS
Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

Figure 3: Security Control Selection Process

5 Assurance

Appendix E in SP 800-53 Revision 4 provides an update to guidance regarding security assurance. This section outlines methods for agencies to establish measures of confidence that the implemented security controls provide the security capability required to protect critical missions and business operations.

The criteria for whether a security control is assurance- or functionality-related is based on the overall characteristics of the control. In general, assurance-related controls are controls that: (i) define processes, procedures, techniques, or methodologies for designing and developing information systems and system components; (ii) provide supporting operational processes including improving the quality of systems, components, or processes; (iii) produce security evidence from developmental or operational activities; (iv) determine security control effectiveness or risk; or (v) improve personnel skills, expertise, and understanding.

Appendix E provides three tables that identify specific assurance-related controls that are included in the low-, moderate-, and high-impact baselines described in Appendix D. The controls described assist organizations in defining the controls needed to satisfy minimum assurance requirements. Where additional assurance is desired to achieve risk management objectives, Table E-4 provides additional security controls and control enhancements to achieve enhanced assurance. Implementers should note that designation of assurance-related controls is not intended to imply a greater level of importance for such controls. Achieving adequate security for organizational information systems requires the correct combination of both functionality- and assurance-related security controls.

6 Security Controls

Appendix F, the Security Control Catalog, provides a comprehensive range of countermeasures for organizations and information systems. The security controls are designed to be technology-neutral such that the focus is on the *fundamental* countermeasures needed to protect organizational information during processing, storage, or transmission. SP 800-53 Rev. 4, therefore, does not provide guidance on the application of security controls to specific technologies, environments of operation, or missions/business functions. These specific areas may be addressed using overlays (see below).

Control enhancements are included with many security controls and are selected in order to increase the strength of the base control. Control enhancements are intended to be implemented only in conjunction with implementation of the base control.

Some security controls and control enhancements include one or more *assignment* and *selection* statements. These are variable parameters that organizations define, providing them with the ability to tailor security controls based on specific security requirements, environments of operation, and organizational risk tolerance. Parameters assigned and/or selected by organizations for a given base control also apply to all control enhancements associated with that control.

The first security control in each family (referred to as the dash-1control) addresses policies and procedures needed for effective implementation of all the other controls within each family. Therefore, requirements to develop policies and procedures are not repeated in individual controls.

Many security controls and enhancements include supplemental guidance. The supplemental guidance provides additional information about a control or enhancement to help organizations define, develop, and/or implement security controls but does not include any additional requirements.

SP 800-53 Rev. 4 includes many changes from SP 800-53 Rev. 3 – 295 controls and control enhancements were added while approximately 100 controls and control enhancements were withdrawn or incorporated into others. Of the eighteen security control families in SP 800-53 Rev. 4, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

One additional family, the Program Management (PM) family, provides controls for information security programs themselves. This family is described in Appendix G of SP 800-53 Rev. 4. While it is not specifically referenced in FIPS 200, the PM section provides security controls at the organization level rather than the information system level. The PM controls are typically implemented at the organization level and not directed at individual organizational information systems. They complement the security controls in Appendix F and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Tailoring guidance can be applied to the program management controls in a manner similar to how the guidance is applied to security controls in Appendix F.

7 International Information Security Standards

Many organizations use well-known international information security standards as the basis or as a supplemental source of security controls for risk management. To aid in selection and comparison, SP 800-53 Rev. 4 provides mapping tables to provide organizations with a general indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements* and ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security*. ISO/IEC 27001 applies to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. ISO/IEC 15408 (also known as the Common Criteria) provides functionality and assurance requirements for developers of information systems and information system components (i.e., information technology products). Since many of the technical security controls defined in Appendix F are implemented in hardware, software, and firmware components of information systems, organizations can obtain significant benefit from the acquisition and employment of information technology products evaluated against the requirements of ISO/IEC 15408. The use of such products can provide evidence that certain security controls are implemented correctly, operating as intended, and producing the desired effect in satisfying stated security requirements.

8 Overlays

To help ensure that selected and implemented controls are sufficient to adequately mitigate risks to organizational operations and assets, SP 800-53 Rev. 4 introduces the concept of *overlays.* An overlay provides a set of security controls, control enhancements, and supplemental guidance for community-wide use or to address specialized requirements, technologies, or unique missions and environments of operation. For example, the federal government may decide to establish a government-wide set of security controls and implementation guidance for public key infrastructure (PKI) systems that could be uniformly applied to information systems.

Multiple overlays can be applied to a single security control baseline. The tailored baselines that result from the overlay development process may be more or less stringent than the original security control baselines. Risk assessments provide information necessary to determine if the risk from implementing the tailored baselines falls within the risk tolerance of the organizations or communities of interest developing the overlays.

General guidance on overlays is provided in section 3.3 and an overlay template is provided in Appendix I. The template is included as an example only—organizations may choose to use other formats or modify the format in this appendix based on 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 rationale and justification for the resulting tailored baseline developed, including any risk-based decisions made during the overlay development process.

The sample overlay template consists of eight sections:

- Identification;
- Overlay Characteristics;
- Applicability;
- Overlay Summary;
- Detailed Overlay Control Specifications;
- Tailoring Considerations;
- Definitions; and
- Additional Information or Instructions.

9 Privacy

Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight new families of privacy controls that are based on the internationally accepted Fair Information Practice Principles (FIPPs). The proliferation of social media, Smart Grid, mobile, and cloud computing, as well as the transition from structured to unstructured data and metadata environments, have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality.

The families of controls are described in a similar manner to those of Appendix F (Security Controls) and Appendix G (Information Security Programs Organization-Wide Information Security Program Management Controls). SP 800-53 Rev. 4 reminds readers to view the privacy controls in Appendix J from the same perspective as the Program Management controls in Appendix G—that is, the controls are implemented for each organizational information system irrespective of the FIPS 199 categorization for that system. Appendix J defines controls, control enhancements, guidance, and references for the following new families:

- Authority and Purpose (AP);
- Accountability, Audit, and Risk Management (AR);
- Data Quality and Integrity (DI);
- Data Minimization and Retention (DM);
- Individual Participation and Redress (IP);
- Security (SE);
- Transparency (TR); and,
- Use Limitation (UL).

The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Organizations should decide when to apply control enhancements to support their particular missions and business functions. Specific overlays for privacy can also be considered to facilitate the tailoring of the security control baselines in Appendix D with the requisite privacy controls to ensure that both security and privacy requirements can be satisfied by organizations.