The Office of Management and Budget (OMB) is proposing to revise Circular No. A-130, *Managing Information as a Strategic Resource*, (hereinafter, Circular A-130, or the Circular) to incorporate new statutory requirements and enhanced technological capabilities, as well as address current and evolving technical and personnel security threats.

Historically, it has been the policy of the United States Government to support the development and use of efficient and effective information technology and information policy approaches that, when adopted by Federal agencies, can address important administrative, regulatory, procurement, and policy objectives. Today, more than ever, individuals, groups, and Federal agencies rely on information technology to carry out a wide range of missions and business functions. This reliance on information technology means that information systems developed and deployed to support Federal applications and operations must be dependable despite a growing number of threats including cybersecurity attacks, natural disasters, structural failures, and errors of omission and commission. To ensure that Federal agencies can successfully carry out their assigned missions and business operations in an environment of sophisticated and complex threats (including advanced persistent threats), they must deploy systems that are both trustworthy and resilient.[1] Trustworthy and resilient systems can help significantly reduce the susceptibility to threats and ensure mission/business continuity and survivability. While it is impossible to know all potential threats and to stop all anticipated threats, the architecture and design of information systems and use of commercial technologies can significantly increase the "built-in" protection capability of those systems and make them inherently less vulnerable. Moreover, the effects of many system attacks can be reduced by the application of the principles, concepts, and best practices that are proposed in this revised policy.

OMB is revising Circular A-130 to provide guidance to support agency missions and operations in a dynamic and increasingly interconnected, information-resources environment that must increasingly contend with information technology vulnerabilities and information security and other threats that could put the confidentiality, integrity and availability of Federal information systems at risk. Agencies shall incorporate this guidance into their policies, understanding that the subject nature of this document will demand agencies continually reassess, reexamine, and reevaluate their information resources management policies and strategies.

This Circular establishes general policy for the acquisition and management of information technology equipment, funds, personnel, and other resources. The requirements of this Circular apply to all information resources in any medium (unless otherwise noted), including both paper and electronic information. In the appendices to the document, it also includes a discussion of agency responsibilities for managing personally identifiable information, provides guidance on the use of electronic transactions, and provides guidance on the protection of Federal information resources. Although this Circular touches on many specific issues such as privacy, confidentiality, information quality, dissemination, and statistical policy, those topics are covered

[1] Refers to information systems that: (1) are believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation; and (2) include the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption.

more fully in other OMB policies, which are available on the OMB website at https://www.whitehouse.gov/omb.

In this notice, OMB is seeking comment on proposed revisions to Circular A-130.

In the main body of the Circular, OMB has replaced the Background section of the main body with an Introduction section (Section 1) that discusses the importance of ensuring trustworthiness and resilience of information systems. OMB also proposes additional language on the purpose of the Circular (Section 2) and amends the Authorities section (now Section 9) to more fully cover existing statutes.

In the Applicability section (Section 3) of the main body, OMB has simplified the reference to national security systems by removing "Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472" and replacing it with "For national security systems, agencies should follow applicable statutes, Executive Orders, and directives."

Section 4, Basic Considerations and Section 5, Policy have been revised to incorporate both policy and statute changes since the Circular was last revised.

Specific changes to the Policy section (Section 5) include the replacement of outdated requirements with new requirements covering planning and budgeting, governance, leadership and workforce, information technology management, privacy and information security, next generation Internet, records management, and information management and access.

Section 6 of the Circular designates government-wide responsibilities for specific agencies. The section incorporates additional statutory requirements enacted since the last revision of the Circular in 2000.

In the Definitions Section of the main body (Section 10), OMB has proposed several changes.

OMB is proposing to delete the following definitions – "audiovisual production," "full costs," "Information Technology Resources Board," "information processing services organization," and "service recipient," as they are no longer needed for the purposes of this Circular.

The term "government information" has been removed because it is not used in this Circular. The term "Federal information" has been added to the Definitions section because it is a commonly used term in statute and is used throughout this Circular.

Several new definitions are proposed for inclusion in the main body of the Circular including – "enterprise architecture," "Federal information system," "information security," "information technology resources," "interagency agreement," "major information technology investment," "open data," "personally identifiable information," "senior agency official for privacy," and "senior agency official for records."

The Circular also proposes to modify the definitions for "agency," "capital planning and investment control process," "information," "information resources," "information resources

management," "information system," "information system life cycle," "information technology," "the CIO Council," "dissemination," and "major information system" to be consistent with current OMB policy and Federal statute.

Appendix I, previously titled *Federal Agency Responsibilities for Maintaining Records About Individuals*, is being revised to provide guidance to Federal agencies on their responsibilities for managing information resources that involve personally identifiable information (PII). The previous version of Appendix I described agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, as amended (5 U.S.C. § 552a). This information is being revised and reconstituted as OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. The revised Appendix I, titled *Responsibilities for Management of Personally Identifiable Information*, provides guidance on Federal agencies' responsibilities for protecting personally identifiable information (PII) – including PII collected for statistical purposes under a pledge of confidentiality – and describes a set of fair information practice principles (FIPPs) that Federal agencies should incorporate when managing information resources that involve PII. It also discusses requirements for designating a Senior Agency Official for Privacy (SAOP) and conducting Privacy Impact Assessments. Finally, Appendix I requires Federal agencies to implement the privacy controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* Additional guidance on implementing the NIST SP 800-53 privacy controls is provided in Appendix III, *Responsibilities for Protecting Federal Information Resources.*

Appendix II, previously titled *Implementation of the Government Paperwork Elimination Act*, is being revised to reference requirements of the Electronic Signatures in Global and National Commerce Act (E-Sign Act). The Government Paperwork Elimination Act (GPEA) and E-Sign Act are both important tools to improve customer service and governmental efficiency through the use of information technology. In addition to highlighting the E-Sign Act and more recent guidance, such as the "Federal Chief Information Officers' Council *Use of Electronic Signatures in Federal Organization Transactions*" (dated January 2013), this appendix has been significantly pared down. For example, the OMB M-00-10 attachment entitled "*OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act*" has been removed and included as a reference. The Background section has been revised to make the information more current and remove historical information not relevant to the current update. For example, summaries of public comments received on OMB's draft GPEA guidance of 2000 have been removed, as well as outdated references to GAO and NIST publications.

Appendix III, previously titled *Security of Federal Automated Information Resources*, is being revised to establish new requirements for information security and privacy management, to incorporate new mandates in the Federal Information Security Modernization Act of 2014, and to ensure consistency with OMB policies and NIST Federal Information Processing Standards and 800-series publications. In short, the revised Appendix III provides guidance on how agencies should take a coordinated approach to information security and privacy when protecting Federal information resources. As a result, the title of the Appendix has been changed to *Responsibilities for Protecting Federal Information Resources*. The proposed revisions provide guidance on agency information security and privacy management, including the transition from the current periodic point-in-time authorization process to a more dynamic continuous monitoring and

ongoing authorization process for information systems and common controls. Examples of additional requirements included in the revised Appendix III focus on incident response, encryption, inclusion of security requirements in contracts, oversight of contractors, protecting against insider threats, protecting against supply chain risks, prohibiting unsupported software and system components, and holding personnel accountable. A number of new definitions, consistent with definitions in NIST standards and guidelines, have also been included.

In addition, the revised Appendix III clarifies the role of the SAOP in the NIST Risk Management Framework. In accordance with existing OMB policies, the Appendix explains that the SAOP has overall responsibility and accountability for implementing privacy protections and ensuring that all privacy requirements are met. Accordingly, the SAOP is responsible for developing and implementing a privacy continuous monitoring strategy, reviewing and approving the categorization of information systems, designating privacy controls, reviewing and approving the privacy plan, conducting privacy control assessments, and reviewing authorization packages for information systems.

CIRCULAR NO. A-130

Proposed

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction

Information and information technology resources are widely recognized as one of the engines that drives the U.S. economy—giving industry a competitive advantage in the global marketplace, enabling the Federal government to provide quality services to citizens, and facilitating greater productivity as a nation. The deeply embedded nature of information technology in all Federal agency missions and business processes reflects the rapid transformation to a fully "digital" world. This transformation has provided significant opportunities for agencies through modern computing architectures, cloud technologies, and agile development techniques, to acquire and rapidly deploy highly efficient and cost-effective applications, services, and solutions. Today, agencies depend heavily on information technology to successfully carry out their missions and business functions, thus the information technology environment, including the information systems, system components, and supporting business processes must be dependable and survivable. Information systems must have the necessary levels of trustworthiness and resilience to be able to process, store, manage access to, and transmit Federal information in a timely, efficient, and secure manner and to be able to operate under adverse conditions, when necessary, to provide essential services.

To provide the necessary levels of trustworthiness and resilience while maximizing advanced computing technologies, Federal information systems must be built to anticipate the modern threat space—that is, the systems should employ technologies that can significantly increase the "built-in" protection capability of those systems and make them inherently less vulnerable. This requires building trustworthiness and resilience in all layers of the information technology "stack" including the networks, systems, applications, and data, as well as hardware, firmware, operating systems, middleware, and software that comprise them. Increasing trustworthiness and resilience is a significant undertaking that requires a substantial investment in architectural design and development. The ultimate objective is to acquire and deploy more trustworthy, and resilient applications, systems, and services that are fully capable of supporting the Federal government's missions and business operations commensurate with its risk tolerance.

2. Purpose

This Circular establishes the general policy for the planning, budgeting, governance, acquisition, and management of personnel, equipment, funds, and information technology resources that support the quality, integrity, design, collection, processing, editing, compilation, storage, transmission, analysis, release, dissemination, accessibility, maintenance, security, cataloguing, sharing, and disposition of Federal information and supporting infrastructure and services. It also includes responsibilities for managing personally identifiable information, requirements for implementing the Government Paperwork Elimination Act and related electronic documentation statutes, and policy on protecting Federal information resources as appendices. Although this Circular touches on many specific issues such as privacy, confidentiality, information quality, dissemination, and statistical policy, those topics are covered more fully in other Office of Management and Budget (OMB) policies, which are available on the OMB website.

3. Applicability

The requirements of this Circular apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government. The requirements of this Circular apply to management activities concerning all information resources in any medium (unless

otherwise noted), including paper and electronic information. When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements of this Circular is not shifted (to the service provider). Agencies shall describe the responsibilities of service providers in relevant agreements with the service providers. Agencies are not required to apply this Circular to national security systems (defined in 44 U.S.C. § 3542). For national security systems, agencies should follow applicable statutes, Executive Orders, directives, and internal agency policies.

4. Basic Considerations

a. Federal information is both a strategic asset and a valuable national resource. It enables the performance of effective government missions and programs and provides the public with knowledge of the government, society, economy, and environment – past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain and enhance the healthy performance of the economy, as well as the general public health and a healthy social and physical environment.

b. Government agencies have a responsibility to be open, transparent, and accountable to the public. Promoting openness and interoperability, subject to applicable legal and policy requirements increases operational efficiencies, reduces costs, improves services, supports mission needs, safeguards personally identifiable information, and increases public access to valuable Federal information.

c. The open and efficient exchange of scientific and technical Federal information, subject to applicable security and privacy controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

d. Making information resources easy to find, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves the lives of Americans and contributes significantly to job creation.

e. Federal information must be protected like the strategic asset and valuable national resource that it is. Agencies must have information security programs that consider the risks and range of threats to information assets and implement controls to mitigate those risks to acceptable levels.

f. Protecting an individual's privacy is of utmost importance. Privacy must be considered and protected throughout the information life cycle in Federal information activities.

g. Information quality is a key parameter of information utility. Quality standards provide established means to evaluate rigor.

h. The rigor of information collection design should be consistent with the likely use of the information, and the utility of information should be balanced against the burden imposed on the public and the cost of the collection.

i. When the Federal Government disseminates information to the public, it must be accompanied with sufficient detail about the collection design and resulting quality parameters (e.g., response rates) for the public to determine the fitness of the information for a given use.

j. Systematic attention to the management of Federal Government records from creation to disposition is an essential component of sound information resources management that ensures public accountability. Together with records preservation, it protects the Government's historical record and safeguards the legal and financial rights of the Government and the public.

k. The Nation can benefit from Federal information disseminated by diverse non-Federal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations.

l. State, local, tribal, and territorial governments are important producers and consumers of information for many areas such as health, social welfare, labor, transportation, national security, public safety, homeland defense, and education. Consequently, the Federal Government should cooperate with these entities in the management of information resources.

5. Policy

Agencies are required to establish a comprehensive approach to improve the acquisition and management of their information resources, by: performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner; focusing information resources planning to support their strategic missions; implementing a IT investment management process that links to and supports budget formulation and execution; and rethinking and restructuring the way work is performed before investing in new information systems.

a. Planning and Budgeting

Agencies shall establish agency-wide planning and budgeting processes in accordance with OMB guidance. As discussed below, important components of planning and budgeting consist of developing and maintaining an Agency Information Strategy, as well as ensuring effective collaboration between agency leadership on budget activities.

1) Strategic Planning

In support of agency missions and business needs, and as part of the agency's overall strategic and performance planning processes, agencies shall develop and maintain an Agency Information Strategy that describes the agency's technology and information resources goals, including but not limited to the processes described in this Circular. The Agency Information Strategy shall support the goals of the Agency Strategic Plan required by the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act). The Agency Information Strategy shall demonstrate how these goals map to the agency's mission and organizational priorities. These goals should be specific, verifiable, and measurable, so that progress against these goals can be tracked. The agency should review its Agency Information Strategy annually alongside the Annual Performance Plan reviews, required by the GPRA Modernization Act, to determine if there are any performance gaps or changes to mission needs, priorities, or goals. As part of the planning and maintenance of an effective Information Strategy, agencies shall consider the following, in addition to all other requirements in this Circular:

a) Taking explicit account of information resources and information technology (IT) assets, personnel, and policies when planning, budgeting, and executing Federal programs and services;

b) Maintaining an inventory of the agency's major information systems, holdings, and dissemination products; a description of the agency's major information and record locator systems; an inventory of the agency's other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency's information resources); and an online resource for persons to obtain public information from the agency;[2]

c) Regularly assess throughout the life of each information system, the inventory of the physical and software assets associated with the system, the maintainability and supportability of the information resources and infrastructure supporting the system, and actively determine when significant upgrades, replacements and/or disposition is required to effectively support agency missions or business functions and/or adequately protect agency assets;

d) Ensuring the terms and conditions of contracts involving the processing, storage, access to, transmission, and destruction of Federal information are sufficient to enable agencies to meet their policy and legal requirements;

e) Ensuring that all resources planning and management activities consider information security, privacy, and supply chain security issues throughout the system development life cycle and that the risks associated with those issues are appropriately managed; and

f) Ensuring that CIOs are made aware of information systems and components that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement.[3]

2) Business Continuity Planning

Agencies shall develop a Business Continuity Plan.[4] A Business Continuity plan to continue agency operations during times of services disruption is essential. Therefore, recovery strategies should be developed so services and/or access can be restored in time to meet the mission needs. Manual workarounds should be part of the plan so business can continue while information systems are being restored. For additional information on business continuity planning, refer to Ready.gov.

[2] Pursuant to the Paperwork Reduction Act (44 U.S.C. § 3506(b)(4) and 3511) and Freedom of Information Act (5 U.S.C. § 552(g)).

[3] Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST Special Publication 800-53 provides additional guidance on unsupported software components.

[4] The Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. For additional information related to continuity planning and contingency planning, please see Appendix III.

3) Planning, Programming, and Budgeting

Agencies shall, in accordance with FITARA and related OMB policy:

a) Ensure that information technology resources are distinctly identified and separated from non-information technology resources during the planning, programming, and budgeting process in a manner that affords agency CIOs appropriate visibility and specificity to provide effective management and oversight of information technology resources. The manner should be jointly determined by Program leadership, the Chief Financial Officer (CFO) and Chief Information Officer (CIO).

b) Ensure the agency-wide budget development process includes the CFO, Chief Acquisition Officer (CAO), and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily IT oriented). The agency head, in consultation with the CFO, CIO, and program leadership, shall define the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:

   i. Weighing potential and ongoing investments and their underlying capabilities against other proposed and ongoing investments in the portfolio; and

   ii. Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and identifying strategies and time frames to close such gaps.

c) Ensure the CIO approves the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. Agencies shall also ensure the CIO is included in the internal planning processes for how the agency uses IT resources to achieve its objectives at all points in their lifecycle, including operations and disposition or migration.

d) Ensure that agency budget justification materials, in their initial budget submission to OMB, include a statement that affirms:

   i. The CIO has reviewed and approves the major IT investments portion of the budget request;

   ii. The CFO and CIO jointly affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and

   iii. The IT Portfolio (formerly Exhibit 53) includes appropriate estimates of all IT resources included in the budget request.

e) Ensure the CFO, CAO, and CIO define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

b. Governance

In support of agency missions and business needs, and in coordination with program managers, agencies shall:

1) Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance.

2) Ensure that the CIO defines the development processes, milestones, review gates, and the overall policies for all strategy, business alignment, and investment planning, enterprise architecture, project management and reporting for information technology resources. The CIO should ensure that such processes and policies address IT resources appropriately. At a minimum, these processes and policies shall ensure:

   a) The CIO certifies that IT systems are appropriately implementing incremental development;

   b) IT resources across the portfolio use appropriate measurements to evaluate the cost variance, schedule variance, and overall performance of their activities as a part of portfolio-wide processes such as IT investment management, enterprise architecture, and other agency information technology or performance management processes. When an Earned Value Management System (EVMS) or other budgeting practices are used, the standard definitions of cost variance and schedule variance will be used to measure progress;[5]

   c) There are agency-wide policies and procedures for conducting investment reviews, operational analyses, or other applicable performance reviews to evaluate IT resources, including projects in development and ongoing activities;

   d) Data and information needs are met through agency-wide data governance policies which clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships between IT strategy, data strategy, and agency programs and business objectives; and

   e) All IT systems and services operate only vendor-supported solutions, and planning and budgeting activities incorporate migration planning and resourcing to accomplish this requirement.

3) Ensure the CIO is a member of governance boards that inform investment decisions that include an IT component, including bureau Investment Review Boards (IRBs) to ensure early matching of appropriate IT with program objectives. The CIO may, in consultation with other senior agency officials, designate other agency officials to act as his or her representative to fulfill aspects of this responsibility in a rules-based manner—such as by a dollar threshold, type of planned IT activity, or by bureau—so long as the CIO retains accountability for the responsibility.

4) Ensure the CIO conducts TechStat reviews or uses other applicable performance measurements to evaluate the use of agency IT resources. The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations.

[5] The Federal Acquisition Streamlining Act of 1994 requires agencies to achieve, on average, ninety percent of the cost and schedule goals established for major and non-major acquisition programs of the agency without reducing the performance or capabilities of the items being acquired.

5) Ensure that the CIO establishes and maintains a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. It should be the CIO and program managers' shared responsibility to ensure that legacy and on-going IT investments are appropriately delivering customer value and meeting the business objectives of programs.

c. Leadership and Workforce

Agencies shall:

1) Ensure the CIO and CHCO develop a set of competency requirements for IT staff, including information security and IT leadership positions, and develop and maintain a current workforce planning process to ensure the agency can:

   a) Anticipate and respond to changing mission requirements,

   b) Maintain workforce skills in a rapidly developing IT environment, and

   c) Recruit and retain the IT talent needed to accomplish the mission.

2) Ensure the workforce related to acquiring, managing, maintaining, and using information resources has the appropriate knowledge and skill for facilitating the achievement of the performance goals established for the portfolio and evaluate the extent to which the executive-level workforce of the agency has appropriate information and technology related knowledge and skills.

3) Ensure the Chief Human Capital Officer (CHCO) and CIO jointly establish an agency-wide critical element (or elements) to be included in all bureau CIOs' performance evaluations. In addition, the CIO shall identify "key bureau CIOs" and provide input to the rating official for at least all "key bureau CIOs" at the time of the initial summary rating and for any required progress reviews. The rating official will consider the input from the CIO when determining the initial summary rating and discuss it with the bureau CIO during progress reviews.

4) Ensure the CIO is involved in the recruitment and approves the selection of any new bureau CIO (includes bureau leadership with CIO duties but not title). The title and responsibilities of current bureau CIOs may be designated or transferred to other agency personnel by the agency head or his or her designee as appropriate, and such decisions may take into consideration recommendations from the agency CIO.

5) Ensure the CIO, CHCO, and other hiring managers capitalize on flexible hiring authorities for specialized positions, as established by the Office of Personnel Management.

d. IT Investment Management

1) Acquisition of Information Technology and Services

   Agencies shall:

   a) Consistent with applicable Federal acquisition requirements, make use of adequate competition, analyze risks (including supply chain risks), associated with potential awards, allocate risk between government and contractor, and maximize return on investment (ROI) when acquiring information technology;

b) Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full lifecycle costs of IT products and services, including but not limited to planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements;[6]

c) Consider existing Federal contract solutions available to meet agency needs to avoid duplicative investments;

d) Structure acquisitions for major IT investments into useful segments with a narrow scope and brief duration in order to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;

e) To the extent practicable, award all contracts which include IT within 180 days after the solicitation is issued and, if this deadline is not reached, consider the cancellation of the work related to the contract, and the IT acquired should be delivered within 18 months after the solicitation resulting in award of the contract was issued (41 U.S.C. § 2308);

f) Ensure all acquisition strategies or acquisition plans (as described in FAR Part 7) or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the agency CIO. The CIO shall consider the following factors when reviewing acquisition strategies and acquisition plans:

i. Alignment with mission and program objectives in coordination with program leadership;

ii. Appropriateness with respect to the mission and business objectives supported by the IT strategic plan;

iii. Appropriateness of contract type for IT-related resources;

iv. Appropriateness of IT-related portions of statement of needs or statement of work;

v. Ability to deliver functionality in short increments; and

vi. Opportunities to migrate from end-of-life software and systems, and to retire those systems.

2) Investment Planning and Control

Agencies are responsible for establishing a decision-making process that provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of all major investments made by an agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the investments. Agencies shall designate IT

[6] Other acquisition planning provisions are set forth in Federal Acquisition Regulation (FAR) subpart 7.1, Acquisition Plans, and subpart 10, Market Research.

investments as major or non-major investments, or other categories, according to relevant statute, regulations and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide. At a minimum, agencies shall ensure that:

a) All IT resources (see "Information Technology Resources" definition) are included in IT investment planning documents or artifacts;

b) Significant decisions related to major IT investments are supported by business cases with appropriate evidence;

c) All IT investments appropriately implement incremental development and modular approaches as defined in OMB guidance;

d) IT investments support and enable core mission and operational functions and processes related to the agency's missions and business requirements;

e) Decisions to improve, enhance, or modernize existing information technology investments or to develop new information technology investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options and the most advantageous option to the government has been selected;

f) Qualitative and quantitative research methods are used to determine the goals, needs, and behaviors of current and prospective managers and users of the service to strengthen the understanding of requirements;

g) Priority in the selection of information system technologies and services, should be given in the following order: First, to the use of available and suitable existing Federal information systems, software, technologies, and shared services and/or information processing facilities; Second, to the acquisition of commercially available off-the-shelf components and/or software-as-a-service solutions; and Third, to custom developed software and technologies. All proposed solutions should be merit-based and consider factors such as performance, cost, security, interoperability, ability to share or re-use, and availability of quality support. Decisions to acquire or develop custom or duplicative solutions must be justified based on comparative analysis conducted in a technology neutral manner that is merit-based and considers factors such as performance, cost, security, interoperability, ability to share or re-use, and availability of quality support, analysis of overall cost-effectiveness of the solution throughout the life cycle, the ability to meet acceptable levels of security, and the ability to meet specific and high-priority mission or operational requirements. To the degree possible, any custom software development activity or custom software acquisition should include contractual rights for re-use throughout the Federal government;

h) Information technology needs are met through acquiring scalable, provisioned IT services[7] when it is cost-effective to do so rather than the agency developing its own information system or equipment;

i) Information systems security levels are commensurate with the impact that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information consistent with NIST 800-series guidelines;

j) Information systems should be built in a way that maximizes interoperability and in a manner that provides access to information through documented, scalable, and continuously available application programming interfaces (APIs). Agencies should maintain data asset inventories, and provide for active and inactive data governance within the agency with attention focused on maintaining appropriate information safeguards;

k) Information technology investments must facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and telecommunications platforms;

l) Information systems and processes must support interoperability and access to information, maximize the usefulness of information, minimize the burden on the public, and preserve the appropriate integrity, usability, availability, confidentiality, and disposition of information throughout the life cycle of the information.[8]

m) Information systems and processes must facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and information technology accessibility requirements commonly known as "section 508" requirements (29 U.S.C. § 794d);

n) Records management functions and retention requirements are incorporated into the design, development, and implementation of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service; and

o) Investments use an EVMS and Integrated Baseline Review (IBR), when appropriate, as required by Federal Acquisition Regulation Subpart 34.2 or, when an EVMS is not required, implement a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance.

[7] Provisioned IT services are considered subcategories of Development, Modernization and Enhancement (DME) and Operations and Maintenance (O&M). Examples of Provisioned IT Services may include the purchase of E-Gov Line of Business from another Federal Agency, or the purchase of software-as-a-service (SaaS), platform as a Service (PaaS), infrastructure-as-a-service (IaaS) from a private service provider, or the purchase of shared services or cloud services. Provisioned IT Service excludes Software Licenses but includes both Intra and Inter Shared Services.

[8] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35); Federal Records Act of 1950, as amended, codified (44 U.S.C. chapters 21, 29, 31, 33); and the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35).

3) Enterprise Architecture

Agencies shall develop an actionable enterprise architecture (EA) that describes the baseline architecture, target architecture, and a plan to get to the target architecture. The EA shall also address agency plans for significant upgrades, replacements and/or disposition of information systems when the systems can no longer effectively support missions or business functions or adequately protect agency needs. The intent is to align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state to the desired future state, helps agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens.

e. Privacy and Information Security

Although this section includes requirements for protecting Federal information resources, this area is covered more fully in the Appendices to this Circular.

1) Privacy

To ensure proper safeguards, agencies shall:

a) Designate a senior agency official for privacy (SAOP) who has overall agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide governance and privacy program to ensure compliance with all applicable statues, regulations, and policies regarding the collection, use maintenance, dissemination, and disposal of PII by programs and information systems;

b) Limit the collection of information such as personally identifiable information, to that which is legally authorized and reasonably deemed necessary for the proper performance of agency functions;

c) Only maintain personally identifiable information that is relevant and reasonably deemed necessary to accomplish a legally authorized purpose;

d) Limit the disclosure of personally identifiable information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

e) Comply with all applicable requirements of the Privacy Act[9] and ensure that system of records notices are published, revised, and rescinded, as required;

f) Ensure that all records with personally identifiable information are maintained in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration;

[9] Agencies should also consult OMB policies on privacy, and OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

g) Conduct privacy impact assessments when developing, procuring, or using information technology, in accordance with the E-Government Act,[10] and make the assessments available to the public in accordance with OMB policy; and

h) Maintain and post privacy policies on all agency websites, in accordance with OMB policy.

2) Information Security

To ensure proper safeguards, agencies shall:

a) Ensure the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014;

b) Ensure that information is protected commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information;

c) Implement security policies issued by the Office of Management and Budget (OMB) and Office of Personnel Management, as well as requirements issued by the Department of Commerce, Department of Homeland Security, and General Services Administration. This includes applying the standards and guidelines contained in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), NIST Special Publications (SPs) (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).[11]

f. Next Generation Internet

In a global and connected economy it is essential for the U.S. and the U.S. Government to ensure that Internet based technologies remain competitive. The Internet and our network infrastructure need to continue to lead in innovation, contribute to the free flow of information, participate an open and available market and do this in a scalable, secure and, when necessary, private Internet. Networking demands, escalating with the continued emergence of connecting technologies has grown well beyond initial capabilities. The use of IPv6 is an essential part of accomplishing these goals and to ensure the network infrastructure can meet our needs for growing capacity, security and privacy and keep the U.S. competitive in the ever escalating global electronic economy. Therefore, agencies shall implement agency-wide processes requiring that Internet Protocol Version 6 (IPv6) compliant products be included in all new information technology acquisitions using Internet Protocol (IP).[12] Agencies must also ensure that all public facing Internet services and

[10] Agencies should also consult OMB policies on privacy, including Appendix I to this Circular.

[11] NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience.

[12] When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g) of the Federal Acquisition Regulation. For additional information, refer to https://www.acquisition.gov/.

enterprise networks fully support the next generation Internet protocol, IPv6, as required by OMB policy.

g. Records Management

Agencies shall:

1) Designate a senior agency official for records management (SAORM) who has overall agency-wide responsibility for records management.

2) Ensure that records management programs provide adequate and proper documentation of agency activities.

3) Ensure the ability to access, retrieve, and manage records throughout their life cycle regardless of form or medium.

4) Establish and obtain the approval of the Archivist of the United States for retention schedules for Federal records in a timely fashion.

5) Ensure the proper and timely disposition of Federal records in accordance with a retention schedule approved by the Archivist of the United States.

6) Provide training and guidance, as appropriate, to all agency officials and employees and contractors regarding their Federal records management responsibilities.

h. Information Management and Access

1) Agencies shall incorporate in planning, budgeting, governance, and other policies appropriate steps to ensure that:

a) Information is managed throughout its life cycle to promote openness and interoperability, and to safeguard systems and information; this includes all stages through which the information passes, including: creating or collection, processing, maintenance, storage, use, sharing, dissemination, and disposition; and

b) Information is managed with a presumption in favor of proactively making information accessible, discoverable, and usable by the public to the extent permitted by statute and subject to existing terms and conditions, privacy, security, and other valid restrictions pertaining to access, use, and dissemination; and

c) Information is managed with clearly designated roles and responsibilities to promote effective and efficient design and operation of information resources management processes within their agency.

2) Agencies shall use these practices to:

a) Collect or create information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public, where appropriate, by:

i. Creating or collecting all new information electronically by default, in machine-readable open formats, using relevant data standards, that upon creation includes standard extensible metadata identifying any restrictions to access, use, and dissemination in accordance with OMB guidance; and

ii. For all instances where new Federal information creation or collection does not fall squarely within the public domain as U.S. government work, agencies shall include appropriate provisions in contracts to meet objectives of open data while recognizing that contractors may have proprietary interests in such information, and that protection of such information may be necessary to encourage qualified contractors to participate in and apply innovative concepts to government programs.

b) Ensure that the public has timely and equitable online access to the agency's public information using a manner that is informed directly by public engagement and balanced against the costs of dissemination or accessibility improvements and demonstrate usefulness of the information.

3) Agencies shall ensure that the public can appropriately discover, and provide feedback about disseminated information and unreleased information by:

a) Ensuring that data, wherever possible and legally permissible, are released to the public in ways that make the data easy to find, accessible, and usable; and

b) Developing other aids as necessary to assist the public in locating agency information including catalogs and directories, site maps, search functions, and other means.

4) Agencies shall ensure that the public can appropriately use disseminated information by:

a) Publishing information online in a, machine-readable open format that can be retrieved, downloaded, indexed, and searched by commonly used web search applications and is public, accessible, described, reusable, complete, timely. This includes providing such information in a format(s) accessible to employees and members of the public with disabilities.[13]

b) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with allowing the agency to disseminate its information on a timely and equitable basis. In certain cases, it may be appropriate to engage in time-limited restrictions or exclusively in cases where the agency, due to resource constraints, would otherwise be unable to provide the information to the public on its own;

c) Avoid establishing unnecessary restrictions, including charging of fees or royalties, on the reuse, resale, or re-dissemination of Federal information by the public;[14]

d) Recovering only the cost of dissemination if fee and user charges are necessary. They must exclude from calculation the costs associated with original collection and processing of the information. Exceptions to this policy are:

i. Where statutory requirements are at variance with the policy;

[13] Pursuant to Section 508 of the Rehabilitation Act of 1973 (as amended (29 U.S.C. § 794d).

[14] Pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35).

ii. Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;

iii. Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing the agency's functions, including reaching members of the public whom the agency has a responsibility to inform; or

iv. Where the Director of OMB determines an exception is warranted.

e) Ensuring that government publications are made available to depository libraries through the Government Publishing Office.[15]

f) Taking advantage of all dissemination channels, including Federal, State, local, tribal, territorial governments, libraries, nonprofit, and private sector entities, in discharging agency information dissemination responsibilities.

5) Agencies shall manage information in accordance with the following principles:

a) Providing notice of Federal agency practices for the collection, use, maintenance, disclosure, dissemination, and destruction of records, as appropriate;

b) Providing adequate notice when initiating, substantially modifying, or terminating dissemination of significant information that the public may be using;

c) Identifying the source of the information disseminated to the public, if from outside the agency where practicable;

d) Considering target audiences of Federal information when determining format, frequency of update, and other information management decisions;

e) Considering the impact of decisions and actions in each stage of the information life cycle on other stages;

f) Considering the effects of information management actions on members of the public and State, local, tribal and territorial governments and their access to Federal information and ensure consultation with the public and those governments as appropriate;

g) Ensuring that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made;

h) Seeking to satisfy new information needs through interagency or intergovernmental sharing of information, or through nongovernmental sources, where lawful and appropriate, before creating or collecting new information;

i) Complying with all applicable statutes governing the disclosure of information, including those related to the quality, privacy, confidentiality, security, and other valid access, use, and dissemination restrictions; and

[15] Pursuant to the Depository Library Act of 1962 (44 U.S.C. Part 19).

j) If not public domain, provide details on the license status to potential data users to help these potential users understand whether there are any restrictions on copying, publishing, distributing, transmitting, adapting, or otherwise using the information for commercial or non-commercial purposes.

6. Government-wide Responsibilities

a. Department of Commerce

The Secretary of Commerce shall:

1) Develop and issue Federal Information Processing Standards (FIPS) and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology, while taking into consideration the recommendations of the agencies and the CIO Council;[16]

2) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;[17]

3) Conduct studies and evaluations concerning telecommunications technology, and the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;[18]

4) Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting Federal information activities;[19]

5) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;[20] and

[16] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35) and the National Institute of Standards and Technologies Act (15 U.S.C. § 271 et seq.).

[17] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35) and the National Institute of Standards and Technologies Act (15 U.S.C. § 271 et seq.).

[18] Pursuant to the National Telecommunications and Information Administration (NTIA) Organization Act, as amended (47 U.S.C. 901 et seq.); cited in 47 U.S.C. 902 (b)(2)(F).

[19] Pursuant to the NTIA Organization Act, as amended (47 U.S.C. 901 et seq.); cited in 47 U.S.C. 902 (b)(2)(G).

[20] Pursuant to the National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. §3701 et seq.), the National Institute of Standards and Technology Organic Act (15 USC § 273, 275a, and 278b), and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

6) Ensure the Federal Government is represented in the development of national and international (in consultation with the Secretary of State) information technology standards, and advise the Director of OMB on such activities.[21]

b. Department of Homeland Security

The Secretary of Homeland Security shall:[22]

1) Monitor and assist agencies with the implementation of information security policies and practices for information systems;

2) Assist OMB in carrying out its information security oversight and policy responsibilities;

3) Develop and oversee the implementation of binding operational directives that reinforce the policies, principles, standards, and guidelines developed by OMB, that focus on:

   a) Requirements for the mitigation of exigent risks to information systems;

   b) Requirements for reporting incidents to the Federal information security incident center; and

   c) Other operational requirements, as deemed necessary by OMB;

4) Coordinate the development of binding operational directives and the oversight of the implementation of such directives with OMB and NIST to ensure consistency with OMB policies and NIST standards and guidelines;

5) Consult with the Director of NIST regarding any binding operational directives that implement or affect the standards and guidelines developed by NIST;

6) Convene meetings with senior agency officials to help ensure effective implementation of information security policies and procedures;

7) Coordinate government-wide efforts on information security policies and practices, including consultation with the CIO Council and NIST;

8) Manage government-wide information security programs and provide and operate Federal information security shared services, as directed by OMB;

9) Provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security. This includes:

   a) Operating the Federal information security incident center;

   b) Deploying technology to assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities, with or without reimbursement and at the request of the agency;

   c) Compiling and analyzing data on agency information security; and

[21] Pursuant to the America Competes Act (33 U.S.C. 893), National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. §3701 et seq.), and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

[22] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35).

781 d) Developing and conducting targeted operational evaluations, including threat and
782 vulnerability assessments, on information systems.

783 10) Provide agencies with current, timely and actionable intelligence about cyber threats,
784 vulnerabilities, and incidents for risk assessments;

785 11) Consult with OMB to determine what other actions may be necessary to support
786 implementation of effective government-wide information security programs;

787 12) Provide the public with timely notice and opportunities for comment on proposed
788 information security directives and procedures to the extent that such directives and
789 procedures affect the public or communication with the public; and

790 13) Solicit and consider the recommendations of the Information Security Privacy Advisory
791 Board, established by the National Institute of Standards and Technology Act.

792 c. General Services Administration

793 The Administrator of General Services shall:

794 1) Manage a single government-wide network contract (formally referred to as the FTS
795 2000 program) that leverages shared solutions for many agencies;[23]

796 2) Manage the Acquisition Services Fund in accordance with the General Services
797 Administration Modernization Act;

798 3) Administer the E-Government fund to support projects approved by the Office of
799 Management and Budget;[24]

800 4) Assist OMB in setting strategic direction for electronic government and overseeing
801 government-wide implementation, and recommend changes relating to government-wide
802 strategies and priorities;[25]

803 5) Promote innovative uses of information technology by agencies, particularly initiatives
804 involving multiagency collaboration, through support of pilot projects, research,
805 experimentation, and the use of innovative technologies;[26]

806 6) Provide support and assistance to the CIO Council;[27] and

807 7) Implement accessibility standards under section 508 of the Rehabilitation Act of 1973, in
808 coordination with the Department of Justice and U.S. Access Board.[28]

809

[23] Pursuant to the Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (40 U.S.C. § 11101-11704).

[24] Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3604).

[25] Pursuant to the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36).

[26] Pursuant to the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36).

[27] Pursuant to the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36).

[28] Pursuant to the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36).

d. National Archives and Records Administration

The Archivist of the United States shall:

1) Administer the Federal Records Act and National Archives and Records Administration regulations (36 CFR Subchapter B—Records Management);

2) Develop requirements relating to electronic records management in consultation with OMB;

3) Work with agencies to ensure the transfer of permanent Federal electronic records to the National Archives of the United States in digital or electronic form to the greatest extent possible;[29] and

4) Ensure agency compliance with records management requirements, provide records management training, and facilitate public access to high-value government records.[30]

e. Office of Personnel Management

The Office of Personnel Management shall:[31]

1) Analyze on an ongoing basis, the workforce needs of the Federal Government related to information technology and information resources management, in conjunction with relevant agencies;

2) Identify where current information technology and information resources management training does not satisfy the needs of the Federal Government related to information technology;

3) Oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs related to information technology and information resources management; and

4) Assess the training of employees in information technology disciplines in order to ensure that information resources management needs are addressed.

7. Effectiveness

This Circular is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

[29] Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. chapters 21, 29, 31, 33).

[30] Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. chapters 21, 29, 31, 33).

[31] Pursuant to the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36).

8. Oversight

The Director of OMB shall use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.

9. Authorities

OMB issues this Circular pursuant to the following statutes:[32]

a. America Competes Act (33 U.S.C. § 893);

b. Budget and Accounting Procedures Act of 1950, as amended (31 U.S.C. § Chapter 11);

c. Chief Financial Officers Act (31 U.S.C. § 3512 *et seq*.);

d. Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (40 U.S.C. § 11101-11704);

e. Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) (44 U.S.C. § 3501 note);

f. Depository Library Act of 1962 (44 U.S.C. Part 19)

g. Digital Accountability and Transparency Act of 2014 (Pub. L. 113-101);

h. E-Government Act of 2002 (44 U.S.C. chapters 35 and 36);

i. Economy Act of 1933 (38 U.S.C. § 701);

j. Federal Acquisition Streamlining Act of 1994 (Pub. L. 103-355);

k. Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35);

l. Federal Information Technology Acquisition Reform Act (FITARA) (Pub. L. 113-291);[33]

m. Federal Property and Administrative Services Act of 1940, as amended (40 U.S.C. §§ 101-18304);

n. Federal Records Act of 1950, as amended, codified (44 U.S.C. chapters 21, 29, 31, 33);

o. Freedom of Information Act (5 U.S.C. § 552);

[32] OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default.

[33] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291. Further references in the text that refer to "FITARA" refer to these sections.

p. General Services Administration Modernization Act (40 U.S.C. § 101);

q. Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504);

r. Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRM) of 2010 (5 U.S.C. § 306 and 31 U.S.C. §§ 1115 *et seq.*);

s. Information Quality Act (44 U.S.C. §§ 3504(d)(1) and 3516);

t. National Institute of Standards and Technologies Act (15 U.S.C. § 271 *et seq.*);

u. National Institute of Standards and Technology Organic Act (15 USC § 273, 275a, and 278b),

v. National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. §3701 et seq.),

w. National Telecommunications and Information Administration (NTIA) Organization Act, as amended (47 U.S.C. 901 et seq.); cited in 47 U.S.C. 902 (b)(2)(F).

x. Office of Federal Procurement Policy Act (41 U.S.C. chapter 7);

y. Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35);

z. Presidential and Federal Records Act Amendments of 2014 (Pub. L. 113-187);

aa. Privacy Act of 1974, as amended (5 U.S.C. § 552a);

bb. Section 508 of the Rehabilitation Act of 1973 (as amended (29 U.S.C. § 794d); and

cc. Other relevant statutes and Executive Orders.[34]

10. Definitions

a. 'Accessibility' or 'Accessible' means that any information technology product or service is in full compliance with the United States Architectural and Transportation Barriers Compliance Board (Access Board) Information and Communication Technology (ICT) Standards and Guidelines for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794 d), as amended by the Workforce Investment Act of 1998 (29 U.S.C. § 2801, *et seq.*), and its guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934 (47 U.S.C. § 151, *et seq.*).

b. 'Agency' means 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.

[34] Executive Orders can be located at https://www.whitehouse.gov.

c. 'Agency Information Strategy' means a strategy that demonstrates how information resources management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.[35]

d. 'Agency Strategic Plan' means plan that provides general and long-term goals the agency aims to achieve, the actions the agency will take to realize those goals, the strategies planned, how the agency will deal with challenges and risks that may hinder achieving result, and the approaches it will use to monitor its progress.[36]

e. 'Business Continuity Plan' means a plan that focuses on sustaining an organization's mission/business processes during and after a disruption, and may be written for mission/business processes within a single business unit or may address the entire organization's processes.[37]

f. 'Chief Information Officer' (CIO) means the senior official that, pursuant to the Clinger-Cohen Act, provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals.

g. 'Chief Information Officers Council' (CIO Council) means the Council codified in the E-Government Act of 2002 (44 U.S.C § 101).

h. 'Controlled Unclassified Information' (CUI) means Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

i. 'Dissemination' means the government-initiated distribution of information to a nongovernment entity, including the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees, intra- or interagency use or sharing of Federal information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act (5 U.S.C. § 552a).

j. 'Enterprise architecture' (a) means – (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (b) includes – (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan (44 U.S.C. § 3601).

---

[35] The Agency Information Strategy is referred to as Information Resource Management Strategic Plan in the Paperwork Reduction Act (44 U.S.C. 3506 (b)(2)).

[36] For additional information, refer to the Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRM) of 2010 (5 U.S.C. § 306 and 31 U.S.C. §§ 1115 *et seq.*); and OMB Circular A-11, Preparation, Submission and Execution of the Budget.

[37] The Federal Information Security Modernization Act (44 U.S.C. chapter 35) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

k. ‘Executive agency’ has the meaning defined in Title 41, Public Contracts section 133 (41 U.S.C. § 133).

l. ‘Federal information’ means information created, collected, processed, maintained, disseminated, or disposed of by or for the Federal Government, in any medium or form.

m. ‘Federal information system’ means an information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.

n. ‘Government publication’ means information that is published as an individual document at government expense, or as required by law, in any medium or form (44 U.S.C. § 1901).

o. ‘Incident’ means an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

p. ‘Information’ means 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.

q. ‘Information dissemination product’ means any recorded information, regardless of physical form or characteristics, disseminated by an agency, or contractor thereof, to the public.

r. ‘Information life cycle’ means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

s. ‘Information management’ means the planning, budgeting, manipulating, controlling, and processing of information throughout its life cycle. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

t. ‘Information resources’ means information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. § 3502).

u. ‘Information resources management’ means the process of managing information resources to accomplish agency missions. The term encompasses an agency’s information and the related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. § 3502).

v. ‘Information security’ means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) Availability, which means ensuring timely and reliable access to and use of information (44 U.S.C. § 3542).

w. ‘Information system’ means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. § 3502).

x. ‘Information system life cycle’ means all phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing. See also OMB A-11 Part 7 “Capital Programming Guide” and OMB Circular A-131 “Value Engineering” for more information regarding the costs and management of assets through their complete life cycle.

y. ‘Information technology’ means any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment is used by an agency if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use (40 U.S.C. § 11101).

z. ‘Information technology investment’ means an expenditure of information technology resources to address mission delivery and management support. This may include a project or projects for the development, modernization, enhancement, or maintenance of a single information technology asset or group of information technology assets with related functionality, and the subsequent operation of those assets in a production environment. These investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment’s most current alternatives analysis if applicable.

aa. ‘Information Technology Investment Management’ means a decision-making process that, in support of agency missions and business needs, provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of all major capital investments made by an agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the investments. The CPIC process has three distinct phases: Select, Control, and Evaluate. See 40 U.S.C § 11302 and the Clinger-Cohen Act of 1996 for statutory requirements.

bb. ‘Information technology resources’ means all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements which include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include

grants which establish or support information technology not operated directly by the Federal Government.

cc. 'Interagency agreement' means, for the purposes of this document, a written agreement entered into between two Federal agencies that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency), including assisted acquisitions as described in OMB Memorandum: *Improving the Management and Use of Interagency Acquisitions* and other cases described in Federal Acquisition Regulation (FAR) Part 17.

dd. 'Major information system' means a system that is part of an investment that requires special management attention as defined in OMB guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources.

ee. 'Major information technology investment' means an investment that requires special management attention as defined in OMB guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a major acquisition as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources.

ff. 'National security system' means any information 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: 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 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 (44 U.S.C. § 3542).

gg. 'Open data' means publicly available data structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are public, accessible, machine-readable, described, reusable, complete, timely, and managed in manners consistent with OMB guidance defining these terms, including relevant privacy, security, and other valid access, use, and dissemination restrictions.

hh. 'Personally identifiable information' (PII) means 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.

ii. 'Privacy Impact Assessment' (PIA) means 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 collecting, maintaining, and disseminating information in identifiable form in an electronic information systems; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.

jj. 'Provisioned IT Service' means an IT service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency on an as-needed basis.

kk. 'Public information' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public (44 U.S.C. chapter 35).

ll. 'Records' means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them (44 U.S.C. § 3301).

mm. 'Records management' means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. § 2901(2)).

nn. 'Senior Agency Official for Privacy' (SAOP) means the senior official, designated by the head of each agency, who has overall agency-wide responsibility for information privacy, including implementation of information privacy protections, compliance with Federal laws, regulations, and policies relating to information privacy, and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

oo. 'Senior Agency Official for Records Management' (SAORM) means the senior official who has direct responsibility for ensuring the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy, and OMB policy.

pp. 'TechStat' means a face-to-face, evidence-based accountability review of an IT investment that enables the Federal government to intervene to turn around, halt or terminate IT projects that are failing or are not producing results for the American people.

11. Inquires

All questions or inquiries should be addressed to the Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-0379 or (202) 395-3785 or Email: A130@omb.eop.gov.

Appendix I to OMB Circular No. A-130
Responsibilities for Management of Personally Identifiable Information

1. Purpose

This Appendix outlines some of the general responsibilities for Federal agencies managing information resources that involve personally identifiable information (PII). The requirements of this Appendix apply to PII in any medium, including both paper and electronic information. For more specific requirements, agencies should consult specific OMB guidance documents, which are available on the OMB website.

Previous versions of this Appendix included information about the reporting and publication requirements of the Privacy Act of 1974[38] ("Privacy Act") and additional OMB guidance. This information has been revised and reconstituted as OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.[39]

This Appendix does not extend or interpret the Privacy Act, including agency requirements under the Privacy Act.

2. Responsibilities for Protecting PII

The Federal Government necessarily collects, creates, uses, disseminates, and maintains PII to carry out the missions mandated by Federal statute. The term PII, as defined in the main body of this Circular, refers to 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. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, agencies must perform an assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-identifiable information can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.[40]

Once the agency determines that an information system contains PII, the agency must conduct an analysis of the information and the information system to determine which privacy requirements may apply. The determination of which privacy controls and safeguards should be applied to an information system will depend on more than an assessment of whether the information system contains PII. Rather, the agency must also consider the sensitivity level of the PII and the potential risk to individual privacy from the collection, creation, use, dissemination, and maintenance of that PII.[41] Agencies should evaluate the sensitivity of each individual data element that is PII, as well as all of the data elements together. The sensitivity level of the PII

[38] 5 U.S.C. § 552a.

[39] OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. This Circular was rescinded by OMB Circular No. A-130.

[40] *See, e.g.*, National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[41] *See id.*

will depend on the context, including the purpose for which the PII is collected, used, disseminated, or maintained. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other data associated with the list, the intended use of the data, how the data will be processed and shared, and the ability to access the data.

Agencies must begin to consider the effect on individual privacy during the earliest planning and development stages of any actions and policies. Moreover, agencies must continue to account for privacy implications during each stage of the life cycle of PII. Agencies must regularly review their holdings of PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete, and must reduce their holdings of PII to the minimum necessary for the proper performance of authorized agency functions.

3. Designation of Senior Agency Official for Privacy

Agencies are required to designate a Senior Agency Official for Privacy (SAOP) who has overall agency-wide responsibility and accountability for ensuring the agency's implementation of all privacy requirements. The SAOP must have a central policy-making role and must ensure that the agency considers the privacy impact of all agency actions and policies that involve PII. The SAOP's review of privacy implications should begin at the earliest planning and development stages of agency actions and policies that involve PII, and should continue through the life cycle of the information.

The SAOP must ensure that the agency complies with all applicable privacy requirements in statute, regulation, and policy. Relevant authorities include, but are not limited to, the Privacy Act, the Paperwork Reduction Act of 1995,[42] the E-Government Act of 2002,[43] *Privacy Act Implementation: Guidelines and Responsibilities*,[44] *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988*,[45] and *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.[46]

4. Privacy Impact Assessments

As a general matter, an agency must conduct a privacy impact assessment (PIA) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section, when the agency develops, procures, or uses information technology to collect, maintain, or disseminate PII.[47] A PIA is an analysis of how PII is handled to ensure that handling conforms

[42] 44 U.S.C. chapter 35.

[43] 44 U.S.C. § 3501 note.

[44] Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf

[45] Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25,818 (June 19, 1989), available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf

[46] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22

[47] *See* 44 U.S.C. § 3501 note.

to all applicable privacy requirements, determine the risks of activities involving PII, and evaluate protections and processes for handling PII to mitigate potential privacy risks.

A PIA is one of the most valuable tools Federal agencies use to ensure that privacy is sufficiently analyzed and addressed. Agencies must conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle. In order to conduct a meaningful PIA, the agency's SAOP must work closely with the program managers, system owners, information technology experts, security officials, counsel, and other relevant agency officials.

In addition to serving as an important analytical tool for agencies, a PIA also serves as notice to the public regarding the agency's practices with respect to privacy and information technology. All PIAs must be drafted in plain language and must be posted on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information. Moreover, a PIA is a living document that agencies are required to update whenever changes to the information technology or the agency's practices substantively alter the privacy risks associated with the use of such information technology.

5. Responsibilities for Protecting PII Collected for Statistical Purposes under a Pledge of Confidentiality

The Nation relies on the flow of credible statistics to support the decisions of individuals, households, governments, businesses, and other organizations. Any loss of trust in the relevance, accuracy, objectivity, or integrity of the Federal statistical system and its products can foster uncertainty about the validity of measures our Nation uses to monitor and assess performance, progress, and needs.

Given the importance of robust and objective official Federal statistics, agencies and components charged with the production of these statistics are assigned particular responsibility. Specifically, information acquired by an agency or component under a pledge of confidentiality[48] and for exclusively statistical purposes cannot be used for any non-statistical purpose, such as an administrative, enforcement, or regulatory purpose. As defined in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),[49] statistical purpose refers to the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that compose such groups; it includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support such purposes. These agencies and components must protect

[48] The term "confidentiality" can have multiple meanings. For example, in the context of general information security the term means "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." *See* 44 U.S.C. § 3542. However, for the purposes of section 5 of Appendix I to this Circular, the term "confidentiality" refers to the requirement that "data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent." *See* 44 U.S.C. § 3501 note.

[49] 44 U.S.C. § 3501 note.

the integrity and confidentiality of this information against unauthorized access, use, modification, or deletion throughout the life cycle of the information. Further, these agencies and components must adhere to legal requirements and should follow best practices for protecting the confidentiality of data, including training their employees and agents, and ensuring the physical and information system security of confidential information.

Relevant authorities include, but are not limited to, Title V of the E-Government Act of 2002, the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),[50] *Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002* (CIPSEA Implementation Guidance),[51] and *Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units*.[52]

6. Fair Information Practice Principles

In addition to the specific requirements in statute, regulation, and policy, agencies should use the Fair Information Practice Principles (FIPPs) when managing information resources that involve PII. The FIPPs are a collection of widely accepted principles that agencies should use when evaluating systems, processes, programs, and activities that affect individual privacy. The FIPPs are not OMB requirements; rather they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements.

Rooted in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," the FIPPs are reflected in Federal statute and the laws of many U.S. states and foreign nations, as well as incorporated in the policies of many organizations around the world. The precise expression of the FIPPs has varied over time and in different contexts. However, the FIPPs retain a consistent set of core principles that are broadly relevant to agencies' information management practices. For purposes of this Circular, the FIPPs are as follows:

a. *Access and Amendment*. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.[53]

b. *Accountability*. Agencies should be accountable for complying with these principles and all applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

---

[50] *Id*.

[51] Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002, 72 Fed. Reg. 33362 (June 15, 2007), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/proposed_cispea_guidance.pdf

[52] Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units, 79 Fed. Reg. 71610 (Dec. 2, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-05-21/pdf/2014-11735.pdf

[53] The Access and Amendment principle is included as part of the "Individual Participation" control family in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems. OMB is including Access and Amendment as a standalone principle in this Circular to emphasize the importance of allowing individuals to access and amend their information when appropriate.

c. *Authority*. Agencies should only collect, create, use, disseminate, or maintain PII if they have authority to do so, and should identify this authority in the appropriate notice.[54]

d. *Minimization*. Agencies should only collect, create, maintain, and use PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.[55]

e. *Quality and Integrity*. Agencies should collect, create, use, disseminate, and maintain PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. *Individual Participation*. Agencies should involve the individual in the decision-making process regarding the collection, creation, use, dissemination, and maintenance of PII and, to the extent practicable, seek individual consent for these activities. Agencies should also establish procedures to receive and address individuals' privacy-related complaints.

g. *Purpose Specification and Use Limitation*. Agencies should provide notice of the specific purpose for which PII is collected and should only use, disseminate, or maintain PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected.

h. *Security*. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, or dissemination.

i. *Transparency*. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding collection, creation, use, dissemination, and maintenance of PII.[56]

7. Privacy Controls for Federal Information Systems and Organizations

It is essential for agencies to take a coordinated approach to identifying and addressing privacy and security requirements. Information security and privacy are independent and separate disciplines and a coordinated approach allows agencies to more effectively consider the breadth of privacy and security requirements that may overlap in concept and in implementation within Federal information systems and technology, programs, and organizations.

---

[54] The Authority principle is included as part of the "Purpose Specification" control family in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems. OMB is including Authority as a standalone principle in this Circular to emphasize the importance of identifying a specific authority for collecting, creating, using, disseminating, or maintaining PII.

[55] In some versions of the FIPPs, the minimization principle is referred to under a different name, such as "collection limitation." *See* National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[56] In some versions of the FIPPs, the transparency principle is referred to under a different name, such as "openness." *See* National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Agencies are expected to implement the security and privacy controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.[57] NIST SP 800-53 establishes privacy controls that are designed to help agencies satisfy statutory privacy requirements and privacy-related OMB policies. The privacy controls are based on the FIPPs and outline the administrative, technical, and physical safeguards that agencies should apply to protect and ensure proper handling of PII. Agencies should implement the privacy controls in a manner that is consistent with their authorities, missions, and operational needs.

The requirement to implement security and privacy controls is described in more detail in Appendix III to this Circular, *Responsibilities for Protecting Federal Information Resources.* Appendix III clarifies the role of the SAOP with respect to the NIST Risk Management Framework. While agencies should refer to Appendix III for the details and definitions of terms, a brief summary of the SAOP's responsibilities in this area is provided below.

SAOP Responsibilities in the Risk Management Framework for Federal Information Systems

SAOP Responsibility	Description	Citation
Overall agency-wide responsibility for privacy	The SAOP has overall agency-wide responsibility and accountability for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the collection, use, maintenance, dissemination, and disposal of PII by programs and information systems.	Appendix III, § 5(e)
Develop and maintain a privacy continuous monitoring strategy	The SAOP shall develop and maintain a privacy continuous monitoring strategy to address privacy risks and requirements across the organizational risk management tiers.	Appendix III, § 5(e)(1)
Establish and maintain a privacy continuous monitoring program	The SAOP shall establish and maintain a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable requirements and to adequately protect PII.	Appendix III, § 5(e)(2)
Review IT capital investment plans and budgetary requests	The SAOP shall review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included.	Appendix III, § 5(e)(3)
Review and approve the categorization of systems	The SAOP shall review and approve, in accordance with NIST FIPS Publication 199 and Special Publication 800-60, the categorization of information systems that collect, process, store, maintain, or disseminate PII.	Appendix III, § 5(e)(4)

[57] National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

SAOP Responsibility	Description	Citation
Designate privacy controls for systems	The SAOP shall designate system-specific, hybrid, and common privacy controls.	Appendix III, § 5(e)(5)
Review and approve the privacy plans for systems	The SAOP shall review and approve the privacy plans for organizational information systems prior to authorization, reauthorization, or ongoing authorization.	Appendix III, § 5(e)(6)
Conduct assessments of privacy controls for systems	The SAOP shall conduct privacy control assessments to ensure that privacy controls are implemented correctly, operating as intended, and effective in satisfying privacy requirements.	Appendix III, § 5(e)(7)
Review authorization packages for systems	The SAOP shall review authorization packages and determine that all applicable privacy requirements are met and the risk to PII is sufficiently addressed prior to authorizing officials making risk determination and acceptance decisions.	Appendix III, § 5(e)(8)
Maintain formal incident response capabilities	The SAOP shall maintain formal privacy incident response capabilities to include breach notification, shall implement formal privacy incident policies, and shall provide adequate training and awareness for employees and contractors on how to report and respond to privacy incidents.	Appendix III, § 5(f)(1)-(3)
Develop and maintain agency-wide privacy training	The SAOP shall develop and maintain mandatory agency-wide privacy training for all employees and contractors, including role-based training, and shall establish enforceable rules of behavior.	Appendix III, § 5(g)(1)-(8)

1263

Appendix II to OMB Circular No. A-130
Guidance on Electronic Transactions

1. Summary

The Office of Management and Budget (OMB) provides procedures and guidance to implement the Government Paperwork Elimination Act (GPEA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN).

GPEA requires Federal agencies to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and for agencies to maintain records electronically, when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal Government use of a range of electronic signature alternatives.

E-SIGN promotes the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between: contracts written on paper and contracts in electronic form; pen-and-ink signatures and electronic signatures; and other legally required written documents (termed "records") and the same information in electronic form.

E-SIGN applies broadly to commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and State Government.

In support of GPEA and E-SIGN, the General Services Administration and the National Institute of Standards and Technology, in coordination with the Federal CIO Council, maintains guidance on use of Electronic Signatures (E-Signatures) in Federal organization transactions. This guidance expands upon OMB guidance.

2. Background

This document provides agencies the guidance required under sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), Public L. 105-277, Title XVII, signed into law on October 21, 1998, and the Electronic Signatures in Global and National Commerce Act (E-SIGN), Public L. 106-229, signed into law on June 30, 2000. GPEA and E-SIGN are important tools to improve customer service and governmental efficiency through the use of information technology.

As public awareness of electronic communications and Internet usage has increased, demand for on-line interactions with the Federal agencies has also increased. Moving to electronic transactions and electronic signatures can reduce transaction costs for the agency and its partners. Transactions are quicker and information access can be more easily tailored to the specific questions that need to be answered. As a result, data analysis by Federal agencies would be easier. In addition, reengineering the work process associated with transactions may improve efficiency of agency operations.

Public confidence in the security of the government's electronic information processes is essential as agencies make this transition. Electronic commerce, electronic mail, and electronic benefits transfer can require the exchange of sensitive information within government, between

the government and private industry or individuals, and among governments. Electronic systems must be able to protect the confidentiality and privacy of information, authenticate the identity of the transacting parties to the degree required by the transaction, guarantee that the information is not altered in an unauthorized way, and provide access when needed. A corresponding policy and management structure must support the infrastructure that delivers these services.

GPEA seeks to "preclude agencies or courts from systematically treating electronic documents and signatures less favorably than their paper counterparts," so that citizens can interact with the Federal Government electronically (S. Rep. 105-335). It required Federal agencies to provide individuals or entities that deal with agencies the option to submit information or transact with the agency electronically, and to maintain records electronically, when practicable. It also addresses the matter of private employers being able to use electronic means to store, and file with Federal agencies, information pertaining to their employees. GPEA states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal Government use of a range of electronic signature alternatives. This guidance implements GPEA and supports the continued transition to electronic government.

E-SIGN also eliminates barriers to electronic commerce, while also providing consumers with protections equivalent to those available in the world of paper-based transactions. The Act makes clear that no person is required to use electronic records, signatures, or contracts. E-SIGN requires that a consumer affirmatively consent to the use of electronic notices and records. Prior to consenting, the consumer must receive notice of their rights. Moreover, the consumer must provide the affirmative consent electronically, in a manner that reasonably demonstrates that the consumer can access the electronic records that are the subject of the consent.

E-SIGN applies broadly to Federal and State statutes and regulations governing private sector (including business-to-business and business-to-consumer) activities. It generally covers legal requirements that information be disclosed in private transactions. It also requires that agencies generally permit private parties to retain records electronically. The government may establish appropriate performance standards for the accuracy, integrity, and accessibility of records retained electronically, to ensure compliance with applicable statutes and to guard against fraud.

Agency activities and requirements that involve information, but do not relate to business, commercial, or consumer transactions, are not within the scope of E-SIGN. Instead they are addressed by GPEA. Certain statutes and regulations involve both GPEA and E-SIGN, especially with respect to record retention requirements in agency regulations that relate to business, consumer, and commercial transactions. Additionally, GPEA and E-SIGN guidance builds on the requirements and scope of the Paperwork Reduction Act (PRA) of 1995. All transactions that involve Federal information collections covered under the PRA are also covered under GPEA and E-SIGN. Guidance on implementing the requirements of these Acts is referenced below.

3. Guidance

Guidance and procedures on implementing the Government Paperwork Elimination Act and E-SIGN are set forth in the documents referenced below:

a. OMB Memoranda M-00-10, *Procedures and Guidance on Implementing the Government Paperwork Elimination Act,* April 25, 2000. https://www.whitehouse.gov/omb/memoranda_m00-10

b. OMB Memoranda M-00-15, *OMB Guidance on Implementing the Electronic Signatures,* September 25, 2000. https://www.whitehouse.gov/omb/memoranda_m00-15

c. Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (E-SIGN). https://www.whitehouse.gov/sites/default/files/omb/memoranda/esign-guidance.pdf

d. Department of Justice, *Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies*, November 2000. http://www.idmanagement.gov

e. Federal Chief Information Council, *Use of Electronic Signatures in Federal Organization Transactions*, January 2013. http://www.idmanagement.gov

Appendix III to OMB Circular No. A-130
Responsibilities for Protecting Federal Information Resources

Requirements

1. Introduction

Agencies of the Federal Government depend on the secure acquisition, processing, storage, transmission, and disposition of information to carry out their core missions and business functions. This allows diverse information resources ranging from large enterprise information systems (or systems of systems) to small mobile computing devices to collect, process, store, maintain, transmit, and disseminate this information. The information relied upon is subject to a range of threats that could potentially harm or adversely affect organizational operations (e.g., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. These threats include environmental disruptions, purposeful attacks, structural failures, human errors, and other threats that can compromise the confidentiality, integrity, or availability of information. Leaders at all levels of the Federal Government must understand their responsibilities and be held accountable for managing information security and protecting privacy.

Federal agencies must implement information security programs and privacy programs with the flexibility to meet current and future information management needs and the sufficiency to comply with Federal requirements. Emerging technologies and services may continue to shift the ways in which agencies acquire, develop, manage, and use information and technology. As technologies and services continue to change, so will the threat environment. Agency programs must have the capability to identify, respond to, and recover from current threats while protecting their information resources and the privacy of the individuals whose information they maintain. The programs must also have the capability to address new and emerging threats. To be effective, information security and privacy considerations must be part of the day-to-day operations of agencies. This is best accomplished by planning for the requisite security and privacy capabilities as an integral part of the agency strategic planning and risk management processes, not as a separate activity. This includes, but is not limited to, the integration of Federal information security and privacy requirements (and security and privacy controls) into the enterprise architecture, system development life cycle activities, systems engineering processes, and acquisition processes.

To ensure that Federal agencies can successfully carry out their assigned missions and business operations in an environment of sophisticated and complex threats, they must deploy systems that are both *trustworthy* and *resilient*. To increase the level of trustworthiness and resilience of Federal information systems, the systems should employ technologies that can significantly increase the built-in protection capability of those systems and make them inherently less vulnerable. This can require a significant investment in security architectures, and the application of systems security engineering concepts and principles in the design of Federal information systems.

As Federal agencies take advantage of emerging information technologies and services to obtain more effective mission and operational capabilities, achieve greater efficiencies, and reduce costs, they must also apply the principles and practices of risk management, information security,

and privacy to the acquisition and use of those technologies and services. While there are certain security requirements and associated controls that are mandatory, agencies are required to employ risk-based approaches and decision-making to ensure that security capabilities are sufficient to protect agency assets, operations, and individuals. Such risk-based approaches involve framing, assessing, responding to, and monitoring security risks on an ongoing basis. Risk-based approaches can also support potential performance improvements and cost savings when agencies make decisions about maintaining, modernizing, or replacing existing information technologies and services or implementing new technologies and services that leverage internal, other government, or private sector innovative and market-driven solutions. These responsibilities extend to the creation, collection, processing, storage, transmission, dissemination, and disposal of Federal information when such information is hosted by non-Federal entities on behalf of the Federal Government. Ultimately, agency heads remain responsible and accountable for ensuring that information management practices comply with all Federal requirements, and that Federal information is adequately protected commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information.

2. Purpose

This Appendix establishes minimum requirements for Federal information security programs, assigns Federal agency responsibilities for the security of information and information systems, and links agency information security programs and agency management control systems established in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. This Appendix also establishes requirements for Federal privacy programs, assigns responsibilities for privacy program management, and describes how agencies should take a coordinated approach to implementing information security and privacy controls.[58] This Appendix revises requirements contained in previous versions of Appendix III to OMB Circular No. A-130, and incorporates requirements of the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35), the E-Government Act of 2002 (44 U.S.C. chapters 35 and 36), and responsibilities assigned in Executive Orders and Presidential Directives.

3. General Requirements

a. Agencies shall ensure the requirements of the Federal Information Technology Acquisition Act (FITARA) are considered in establishing the responsibilities and accountability for the implementation of information and information security programs.

b. Agencies shall develop, implement, document, maintain, and oversee agency-wide information security and privacy programs including people, processes, and technologies to:

   1) Provide for agency information security and privacy policies, planning, budgeting, management, implementation, and oversight;

   2) Cost-effectively manage information security risk, which includes reducing such risk to an acceptable level;

[58] Agencies should consult OMB policies on privacy, including Appendix I to this Circular and OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

3) Ensure compliance with all applicable Federal privacy requirements, and use privacy impact assessments and other tools to analyze and address privacy risks;

4) Protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for their confidentiality, integrity, and availability;

5) Provide adequate security for all information, including PII, created, collected, processed, stored, transmitted/disseminated, or disposed of by or on behalf of the Federal Government, to include Federal information residing in contractor information systems and networks;

6) Employ systems security engineering concepts and techniques during the development of new or updated information systems to facilitate the trustworthiness and resilience of those systems;

7) Implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development lifecycle;

8) Provide information security safeguards and countermeasures commensurate with the risk from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency, or by a contractor of an agency or other organization on behalf of an agency;

9) Implement an agency-wide risk management approach that frames, assesses, responds to, and monitors information security risk across three organizational tiers (i.e., organization level, mission/business process level, and information system level);[59]

10) Implement a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems and environments of operation;

11) Ensure, for information systems and the environments in which those systems operate, that security and privacy controls are implemented correctly, operating as intended, and continually monitored and assessed; that procedures are in place to ensure that security and privacy controls remain effective over time; and that steps are taken to maintain risk at an acceptable level within organizational risk tolerance;

12) Ensure that, in a timely manner, agency CIOs are made aware of information systems and components that cannot be appropriately protected or secured and that such systems are given a high priority for upgrade, replacement, or retirement.

13) Implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide information security and privacy programs; and

[59] Refer to NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* for additional information.

14) Ensure that performance plans for all Federal employees include an element addressing the need to adhere to Federal and agency-specific requirements for the protection of information and information systems; and for individuals with significant security and privacy responsibilities, include requirements regarding their role in protecting information and information systems.

c. Agencies shall protect Controlled Unclassified Information (CUI) in accordance with requirements set forth by the National Archives and Records Administration.

d. Agencies shall limit the disclosure of proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists.

e. Agencies shall implement security and privacy policies issued by the Office of Management and Budget (OMB), and the Office of Personnel Management, as well as requirements issued by Department of Commerce, Department of Homeland Security, and General Services Administration. This includes applying the standards and guidelines contained in National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), NIST (800-series) Special Publications, and, where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).

f. Agencies shall ensure that all contracts, and other third-party agreements for services, incorporate all relevant information security and privacy requirements outlined in statute, OMB policy, Executive Orders, and Presidential Directives.

4. Specific Requirements[60]

a. Security Categorization

Agencies shall:

1) Identify authorization boundaries for information systems; and

2) Categorize information and information systems, in accordance with FIPS Publication 199 and NIST Special Publication 800-60, considering potential adverse security and privacy impacts to organizational operations and assets, individuals, other organizations, and the Nation.

b. Planning, Budgeting, and Enterprise Architecture

Agencies shall:

1) Identify and plan for the resources needed to implement information security and privacy programs;

2) Ensure that information security and privacy are addressed throughout the life cycle of each agency information system, and that security and privacy activities and costs are explicitly identified and included in IT investment capital plans and budgetary requests;

[60] The requirements in this section represent those areas deemed to be of fundamental importance to the achievement of effective agency information security programs and those areas deemed to require specific emphasis by OMB. The security programs developed and executed by agencies need not be limited to the aforementioned areas but can employ a comprehensive set of safeguards and countermeasures based on the principles, concepts, and methodologies defined in the suite of NIST standards and guidelines.

3) Plan and budget to upgrade, replace or retire any information systems for which security and privacy protections commensurate with risk cannot be effectively implemented;

4) Ensure that investment plans submitted to OMB as part of the budget process meet the information security and privacy requirements appropriate for the life cycle stage of the investment; and

5) Incorporate Federal information security and privacy requirements into the agency's enterprise architecture to ensure information systems and the environments in which those systems operate achieve the necessary levels of trustworthiness, protection, and resilience.

c. Plans, Controls, and Assessments

Agencies shall:

1) Develop and maintain information security program and privacy program plans that provide an overview of the organization-wide information security and privacy requirements and describe the program management controls and common controls in place or planned for meeting those requirements;

2) Employ a system life cycle process that incorporates the principles, concepts, methods, and techniques of systems security engineering as described in NIST Special Publication 800-160 to ensure the development of trustworthy and resilient information systems;

3) Develop supply chain risk management plans for all organizational tiers as described in NIST Special Publication 800-161 to ensure the integrity, security, resilience, and quality of information systems;

4) Implement a risk-based security control selection process for information systems and environments of operation that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST Special Publication 800-53, tailored as appropriate;

5) Implement a privacy control selection process for information systems and environments of operation that satisfies the privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular, OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, and NIST Special Publication 800-53;

6) Develop and maintain security and privacy plans for information systems and environments of operation to document which security and privacy controls have been selected and how those controls have been implemented;

7) Implement security controls and privacy controls in information systems and environments of operation using systems/security engineering principles, concepts, methods, practices, and techniques;

8) Deploy effective security controls to provide Federal employees and contractors with multifactor authentication, digital signature, and encryption capabilities that provide assurance of identity and are interoperable and accepted across all Executive Branch agencies;

9) Designate common controls in order to provide cost-effective security and privacy capabilities that can be inherited by multiple agency information systems;[61]

10) Assess all selected and implemented security and privacy controls in agency information systems (and environments in which those systems operate) prior to operation, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance;

11) Conduct and record the results of security control assessments and privacy control assessments in security and privacy assessments, respectively;

12) Use agency Plans of Action and Milestones (POA&Ms), and make available or provide access to OMB, DHS, Inspectors General, and the Government Accountability Office, upon request, to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in agency information systems and environments of operation; and

13) Obtain approval from the authorizing official for connections from the information system, as defined by its authorization boundary, to other information systems based on the risk to the agency's operations and assets, individuals, other organizations, and the Nation.

d. Authorization and Continuous Monitoring

Agencies shall:

1) Designate senior Federal officials to formally: authorize an information system to operate; and authorize agency-designated common controls for use based on a determination of, and explicit acceptance of, the information security and privacy risk to agency operations and assets, individuals, other organizations, and the Nation, and prior to operational status;

2) Complete an initial authorization for each information system and all agency-designated common controls;

3) Transition information systems and common controls to an ongoing authorization process when eligible for such a process and with the formal approval of the respective authorizing officials;

4) Reauthorize information systems and common controls as needed, on a time- or event-driven basis in accordance with agency risk tolerance;

[61] When common controls protect multiple agency information systems of differing impact levels, the controls shall be implemented with regard to the highest impact level among the systems. If such controls cannot be implemented at the highest impact level of the information systems, agencies shall factor this situation into their assessments of risk and take appropriate risk mitigation actions (e.g., adding security controls, changing assigned values of security control parameters, implementing compensating controls, changing certain aspects of mission/business processes, or separating the higher impact system into its own domain where it can be afforded appropriate levels of protection).

5) Develop and maintain an ISCM strategy and PCM strategy to address information security and privacy risks and requirements across the organizational risk management tiers (i.e., organization/governance tier, mission/business process tier, and/or information system tier);[62]

6) Implement and periodically update the ISCM strategy and PCM strategy to reflect: the effectiveness of deployed controls; significant changes to information systems and environments of operations; and adherence to Federal statutes, policies, directives, instructions, regulations, standards, and guidelines;

7) Ensure that all selected and implemented controls are addressed in the ISCM strategy and PCM strategy and are effectively monitored on an ongoing basis, as determined by the agency's ISCM and PCM programs;[63]

8) Establish and maintain an ISCM program that:

   a) Provides an understanding of agency risk tolerance and helps officials set priorities and manage information security risk consistently throughout the agency;

   b) Includes metrics that provide meaningful indications of security status at all organizational risk management tiers;

   c) Ensures the continued effectiveness of all security controls selected and implemented by monitoring controls with the frequencies specified in the ISCM strategy;

   d) Verifies compliance with information security requirements derived from missions/business functions, Federal statutes, directives, instructions, regulations, policies, and standards/guidelines;

   e) Is informed by all applicable agency IT assets to help maintain visibility into the security of those assets;

   f) Ensures knowledge and control of changes to information systems and environments of operation; and

   g) Maintains awareness of threats and vulnerabilities;

9) Establish and maintain a PCM program that:

   a) Ensures continued compliance with all applicable privacy requirements;

   b) Verifies the continued effectiveness of all Federal privacy controls selected and implemented across all organizational risk management tiers;

   c) Includes metrics to monitor the effective implementation of privacy requirements and privacy controls across all organizational risk management tiers;

   d) Monitors changes to information systems and environments of operation that collect, process, store, maintain, use, or disseminate PII; and

   e) Maintains adequate awareness of any threats and vulnerabilities that may affect PII and impact individual privacy;

[62] The ISCM strategy and PCM strategy may be integrated into one consolidated continuous monitoring strategy.

[63] The ISCM program and PCM program may be integrated into one consolidated continuous monitoring program.

10) Ensure that a robust ISCM program and PCM program are in place before agency information systems or common controls are eligible for ongoing authorization; and

11) Leverage available Federal shared services, where practicable and appropriate.

e. Privacy Controls for Federal Information Systems and Organizations

The senior agency official for privacy (SAOP) has overall agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide governance and privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the collection, use, maintenance, dissemination, and disposal of PII by programs and information systems. The SAOP shall:

1) Develop and maintain a PCM strategy to address privacy risks and requirements across the organizational risk management tiers (i.e., organization/governance tier, mission/business process tier, and/or information system tier);

2) Establish and maintain a PCM program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable requirements and to adequately protect PII;

3) Review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included;

4) Review and approve, in accordance with NIST FIPS Publication 199 and Special Publication 800-60, the categorization of information systems that collect, process, store, maintain, or disseminate PII;

5) Designate system-specific, hybrid, and common privacy controls;

6) Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization;

7) Conduct privacy control assessments to ensure that privacy controls are implemented correctly, operating as intended, and effective in satisfying privacy requirements; and

8) Review authorization packages and determine that all applicable privacy requirements are met and the risk to PII is sufficiently addressed prior to authorizing officials making risk determination and acceptance decisions.

f. Incident Detection, Response and Recovery

After agencies have selected and implemented the necessary security controls to protect their information and systems consistent with their understanding of agency operations and assets and management of information security risk, agencies shall subsequently ensure they can react appropriately to information security incidents.

Agencies shall:[64]

1) Develop and implement incident management policies and procedures that address incident detection, response, and recovery. This includes developing and implementing appropriate activities to identify the occurrence of an incident; developing and

[64] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35).

implementing appropriate activities to take action regarding a detected cybersecurity incident; and developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an incident;

2) Designate sensitive positions and execute commensurate security clearance levels for appropriate agency personnel;

3) Establish clear roles and responsibilities to ensure the oversight and coordination of incident response activities and that incidents are appropriately documented, reported, investigated and handled;

4) Periodically test incident response procedures to ensure effectiveness of such procedures;

5) Document lessons learned for incident response and update procedures annually and/or as required by OMB and/or DHS;

6) Ensure processes are in place to verify corrective actions;

7) Maintain formal security and privacy incident response capabilities and mechanisms to include breach notification and adequate training and awareness for employees and contractors on how to report and respond to security and privacy incidents;

8) Report security and privacy incidents to OMB, DHS, the SAOP, their respective Inspectors General and General Counsel, law enforcement, and Congress in accordance with procedures issued by OMB;

9) Implement formal security and privacy incident policies to include definitions, detection and analysis, containment, internal and external notification and reporting requirements, incident reporting methods, post-incident procedures, roles and responsibilities, and guidance on how to mitigate impacts to the agency and its respondents following an incident; and

10) Provide reports on incidents as required by FISMA, OMB policy, DHS binding operational directives, US-CERT guidelines, NIST guidelines, and agency procedures.

g. Contingency Planning

Agencies shall:

1) Develop contingency plans[65] for information systems that:

a) Identify essential missions and business functions and associated contingency requirements;

b) Provide recovery objectives, restoration priorities, and metrics;

[65] The Federal Information Security Modernization Act (44 U.S.C. chapter 35) requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

c) Address contingency roles and responsibilities; and

d) Address maintaining essential missions and business functions despite a disruption, compromise, or failure of information systems; and

2) Provide for the recovery and reconstitution of information systems to a known state after a disruption, compromise, or failure.

h. Awareness and Training

Agencies shall:

1) Develop, maintain, and implement mandatory agency-wide information security and privacy awareness and training programs for all employees and contractors;

2) Ensure that the security and privacy awareness and training programs are consistent with applicable standards and guidelines issued by OMB, NIST, and OPM;

3) Apprise agency personnel about available assistance and technical security and privacy products and techniques;

4) Provide foundational as well as more advanced levels of security and privacy awareness training to information system users (including managers, senior executives, and contractors) and ensure that measures are in place to test the knowledge level of information system users;

5) Provide role-based security and privacy training to personnel with assigned security and privacy roles and responsibilities before authorizing access to the information system or performing assigned duties;

6) Establish rules of behavior, that include consequences for violating rules of behavior, for personnel having access to agency information and information systems;

7) Ensure that agency personnel have read and agreed to abide by the rules of behavior for the information systems for which they require access prior to being granted access; and

i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems[66]

Agencies shall:

1) Implement a policy of least functionality by only permitting the use of networks, systems, applications, and data, as well as programs, functions, ports, protocols, and/or services that are necessary in meeting mission or business needs;

2) Implement policies of least privilege at multiple layers – network, system, application, and data so that users have role-based access to only the information and resources that are necessary for legitimate purpose;

3) Implement a policy of separation of duties to address the potential for abuse of authorized privileges and help to reduce the risk of malicious activity without collusion;

[66] NIST Special Publication 800-53 provides information on additional security safeguarding measures.

4) Isolate sensitive and/or critical information resources (e.g., information systems, system components, applications, databases, and information) into separate security domains with appropriate levels of protection based on the sensitivity/criticality of those resources;

5) Implement access control policies for information resources that ensure individuals have appropriate authorization and need, and that the appropriate level of identity proofing and/or background investigation is conducted prior to granting access;

6) Protect administrator, user, and system documentation related to the design, development, operation, maintenance, and security of the hardware, firmware, and software components of information systems;

7) Continuously monitor, log, and audit the execution of information system functions by privileged users to detect misuse and to help reduce the risk from insider threats;

8) Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement;[67]

9) Implement and maintain current updates and patches for all software and firmware components of information systems;[68]

10) For systems that promote public access, ensure that identity proofing, registration, and authentication processes provide assurance of identity consistent with security and privacy requirements, in accordance with Executive Order 13681,[69] OMB policy, and NIST standards and guidelines;

11) Require use of multifactor authentication for employees and contractors in accordance with government-wide identity management standards;

12) Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information: is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO;

13) Implement the current encryption algorithms and validated cryptographic modules in accordance with NIST standards and guidelines;

14) Ensure that only users with legitimate need for access have the ability to decrypt sensitive information.

[67] Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST Special Publication 800-53 provides additional guidance on unsupported software components.

[68] Security-relevant software and firmware updates include, for example, patches, service packs, hot fixes, device drivers, basic input output system (BIOS), and antivirus signatures.

[69] Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.

15) Develop and implement processes to support use of digital signatures for employees and contractors;[70]

16) Implement attribute-based access controls[71] to control and monitor access to Federal information; and

17) Ensure that all Federal systems and services identified in the Domain Name System are protected with Domain Name System Security (DNSSEC) and that all systems are capable of validating DNSSEC protected information.[72]

j. Contracts and Agreements

Organizations that collect or maintain information on behalf of a Federal agency or that operate or use information systems on behalf of a Federal agency, must comply with the requirements in the FISMA and OMB policies. Agencies shall ensure that terms and conditions in contracts, and other agreements involving the processing, storage, transmission, and destruction of Federal information, are sufficient to enable agencies to meet necessary security and privacy requirements concerning Federal information. For additional information and associated requirements pertaining to information technology acquisitions, refer to the Federal Acquisition Regulation.

k. Oversight of Non-Federal Entities

Agencies shall:

1) Provide oversight of information systems used or operated by contractors or other entities on behalf of the Federal government or that collect or maintain Federal information on behalf of the Federal government, to include:

a) Documenting and implementing policies and procedures for information security and privacy oversight, to include ensuring appropriate vetting and access control processes for contractors and others with access to systems containing Federal information;

b) Ensuring that security and privacy controls of such information systems and services are effectively implemented and comply with NIST standards and guidelines and agency requirements;

c) Maintaining and continuously updating an inventory of information systems and system components using automated reporting, cataloguing, and inventory tools;

d) Ensuring that the inventory identifies interfaces between these systems and organization-operated systems;

[70] Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use.

[71] NIST Special Publication 800-162 provides additional information on attribute-based access control.

[72] DNSSEC is a critical component of the Internet infrastructure. DNSSEC enables clients to cryptographically verify that each such translation is provided by a server with the authority to do so, and that the translation response from the server was not modified before reaching the client.

e) Ensuring that procedures are in place for incident response for these systems including timelines for breach notification;

f) Requiring agreements (e.g., Memorandum of Understandings, Interconnection Security Agreements, contracts) for interfaces between these systems and agency-owned and operated systems; and

g) Implementing policies, procedures, and verification methods to ensure, within the risk tolerance of the agency, that systems that are owned or operated by contractors or entities that contain Federal information are compliant with FISMA requirements, OMB policies, and applicable NIST standards and guidelines;

2) Collaborate with non-Federal entities and other agencies as appropriate to ensure that security and privacy requirements pertaining to these non-Federal entities, such as State, local, tribal, and territorial governments, are consistent to the greatest extent possible; and

3) Ensure that non-Federal entities protect CUI in accordance with NARA requirements and any associated NIST standards and guidelines.

l. Mitigation of Deficiencies and Issuance of Status Reports

Agencies must correct deficiencies that are identified through information security and privacy assessments, ISCM and PCM programs, or internal/external audits and reviews, to include OMB reviews. OMB Circular No. A-123, *Management's Responsibility for Internal Control*, provides guidance to determine whether a deficiency in controls is material when so judged by the agency head against other agency deficiencies. Material deficiencies must be included in the annual Federal Managers Financial Integrity Act (FMFIA) report, and remediation tracked and managed through the agency's POA&M process. Less significant deficiencies need not be included in the FMFIA report, but must be tracked and managed through the agency's POA&M process.

m. Reporting

Agencies shall provide FISMA reports in accordance with processes established by OMB and DHS in accordance with the Federal Information Security Modernization Act of 2014.

n. Cybersecurity Framework

The Cybersecurity Framework was developed by NIST in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The Framework describes five core cybersecurity functions (i.e., Identify, Protect, Detect, Respond, and Recover) that may be helpful in raising awareness and facilitating communication among agency stakeholders, including executive leadership. The Cybersecurity Framework may also be helpful in improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. The Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST Risk Management Framework and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs. NIST will provide additional guidance on how agencies can use the Cybersecurity Framework and in particular, how the

two frameworks can work together to help agencies develop, implement, and continuously improve their information security programs.

o. Independent Evaluations

Agencies shall:

1) Perform an independent evaluation of the information security programs and practices to determine the effectiveness of such programs and practices. The evaluation may include an evaluation of their privacy program and practices, as appropriate. Each evaluation must include:

   a) Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

   b) An assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

   c) Separate presentations, as appropriate, regarding information security relating to national security systems.

2) For each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section must be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency. For agencies in which the Inspector General Act of 1978 does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

5. Government-wide Responsibilities

a. Department of Commerce

The Secretary of Commerce shall:

1) Develop and issue standards and guidelines for the security and privacy of information in Federal information systems, and systems which create, collect, process, store, transmit/disseminate, or dispose of information on behalf of the Federal Government;

2) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense (DoD) and DHS;

3) Follow a transparent process that allows and addresses input from the agencies and the public when developing standards and guidelines; and

4) Solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by the National Institute of Standards and Technology Act.[73]

[73] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35).

b. Department of Homeland Security

The Secretary of Homeland Security shall:[74]

1) Monitor and assist agencies with the implementation of information security policies and practices for information systems;

2) Assist OMB in carrying out its information security oversight and policy responsibilities;

3) Develop and oversee the implementation of binding operational directives that reinforce the policies, principles, standards, and guidelines developed by OMB, that focus on:

   a) Requirements for the mitigation of exigent risks to information systems;

   b) Requirements for the mitigation of known or reasonably suspected information security threats, vulnerabilities, and risks;

   c) Requirements for reporting incidents to the Federal information security incident center; and

   d) Other operational requirements, as deemed necessary by OMB;

4) Coordinate the development of binding operational directives and the oversight of the implementation of such directives with OMB and NIST to ensure consistency with OMB policies and NIST standards and guidelines;

5) Consult with the Director of NIST regarding any binding operational directives that implement or affect the standards and guidelines developed by NIST;

6) Convene meetings with senior agency officials to help ensure the effective implementation of information security policies and procedures;

7) Coordinate government-wide efforts on information security policies and practices, including consultation with the CIO Council and NIST;

8) Manage government-wide information security programs and provide and operate Federal information security shared services, as directed by OMB;

9) Provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security. This includes:

   a) Operating the Federal information security incident center;

   b) Deploying technology to assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities, with or without reimbursement and at the request of the agency;

   c) Compiling and analyzing data on agency information security; and

   d) Developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on information systems;

10) Provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments and proactive mitigation;

[74] Pursuant to the Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35).

11) Consult with OMB to determine what other actions may be necessary to support implementation of effective government-wide information security programs;

12) Provide the public with timely notice and opportunities for comment on proposed information security directives and procedures to the extent that such directives and procedures affect the public or communication with the public; and

13) Solicit and consider the recommendations of the Information Security Privacy Advisory Board, established by the National Institute of Standards and Technology Act.

c. Department of Defense

The Secretary of Defense shall:

1) Provide technical advice and assistance to the Departments of Commerce and Homeland Security; and

2) Assist the Departments of Commerce and Homeland Security in evaluating the vulnerabilities of emerging information technologies.

d. General Services Administration

The Administrator of General Services shall:

1) When developing contract vehicles for agencies to use in the acquisition of information security products and services, or when providing government-wide services, ensure these contract vehicles and services are cost effective and provide for capabilities that are consistent with government-wide requirements;

2) Maintain a Federal public key infrastructure (FPKI) framework to allow efficient interoperability among agencies when using digital certificates; and

3) Ensure effective controls are in place to protect the confidentiality, integrity, and availability of the FPKI framework components managed and overseen by the agency, to include performing information security continuous monitoring of the FPKI.

e. Office of Personnel Management

The Director of the Office of Personnel Management shall determine the minimum investigative requirements for Federal employees and contractors requiring access to Federal facilities, information, and/or information systems.

Discussion of the Major Provisions in the Appendix

1. NIST Standards and Guidelines

NIST standards and guidelines associate each information system with an impact level. The standards and guidelines also provide a corresponding starting set of baseline security controls and tailoring guidance to ensure that the set of security controls in the security plan (approved by the authorizing official) and privacy controls in the privacy plan (approved by the SAOP), satisfy the information security, privacy, and mission/business protection needs of the agency.

For non-national security programs and information systems, agencies must apply NIST guidelines unless otherwise stated by OMB. Federal Information Processing Standards (FIPS) are mandatory. There is flexibility within NIST's guidelines (specifically in the 800-series) in

how agencies apply those guidelines. Unless specified by additional implementing policy by OMB, the concepts and principles described in NIST guidelines must be applied. However, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant with the guidelines.

For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems.

2. Risk Management Framework

The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF requires agencies to categorize each information system and the information processed, stored, and transmitted by that system based on a mission/business impact analysis. Agencies select an initial set of baseline security controls for the information system based on the security categorization and then tailor the security control baseline as needed, based on an organizational assessment of risk and local conditions. After implementing the security controls, agencies assess the controls using appropriate assessment methods as described in NIST Special Publication 800-53A to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The authorization to operate the system is based on a determination of the risk to agency operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the system and the decision by the authorizing official, that this risk is acceptable. Subsequent to the authorization decision and as part of an information security continuous monitoring strategy and program, agencies monitor the security controls in the system on an ongoing basis. Monitoring includes, but is not limited to, assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated agency officials on an ongoing basis.

An effective implementation of the RMF ensures that managing information system-related security risks is consistent with the agency's mission/business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function[75] as discussed in NIST Special Publication 800-37. It also ensures that the

[75] The *risk executive function* is an individual or group within an agency that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an agency-wide perspective with regard to the overall strategic goals and objectives of the agency in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the agency, reflects the agency's risk tolerance, and is considered along with other agency risks affecting its missions or business functions.

requisite security requirements and controls are integrated into the agency's enterprise architecture and system development life cycle processes. Finally, the RMF supports consistent, well-informed, and ongoing security authorization decisions, transparency of security and risk management information, reciprocity, and information sharing.

3. Security Control Baselines

It is important to achieve adequate security for Federal information and information systems and a consistent level of protection for such information and systems government-wide. To meet this objective, agencies must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in FIPS Publication 200. The security controls must include one of the three security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of their information systems. The security control baselines define the set of minimum security controls for a low-impact, moderate-impact, or high-impact information system and provide a starting point for the tailoring process. Agencies are required to tailor the security control baselines to customize their safeguarding measures for specific missions, business lines, and operational environments—and to do so in a cost-effective, risk-based manner. Tailoring allows agencies to designate common controls; apply scoping considerations; select compensating controls; assign specific values to agency-defined control parameters; supplement baselines with additional controls when necessary; and provide additional specification information for control implementation. Agencies must provide a justification for any tailoring actions that result in changes to the initial security control baselines. Agencies are not permitted to make changes to security control baselines when such changes result in control selections that are inconsistent with security requirements set forth in Federal statutes, Executive Orders, regulations, directives, or policies.

Agencies may also develop overlays as part of the security control selection process. Overlays provide a specification of security and/or privacy controls, control enhancements, supplemental guidance, and other supporting information as part of the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay may be more stringent or less stringent than the original security control baseline and can be applied to multiple systems. All selected security controls must be documented in a security plan and implemented. Agencies can use the priority code designations associated with each security control in NIST Special Publication 800-53 to assist in making sequencing decisions for control implementation. This prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling agencies to deploy controls in a more structured and timely manner in accordance with available resources. Independent evaluations, when conducted, should focus on the effectiveness of the security controls selected and implemented (as documented in agency security plans after all tailoring actions have been completed on the security control baselines) and the justification for any decisions to change the control baselines.

4. Security and Privacy Assessments

Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually. This general requirement to test and evaluate the effectiveness of information security and privacy policies, procedures, and practices does not imply that agencies must assess every selected and implemented security and privacy control at

least annually. Rather, agencies must continuously monitor all implemented security and privacy controls (i.e., system-specific, hybrid, and common controls) with a frequency determined by the agency in accordance with the ISCM and PCM strategies. These strategies will define the specific security and privacy controls selected for assessment during any one-year period (i.e., the annual assessment window) with the understanding that all controls may not be formally assessed every year. Rotational assessment of security and privacy controls is consistent with the transition to ongoing authorization and assumes the information system has completed an initial authorization where all controls were formally assessed for effectiveness.

Security and privacy control assessments should ensure that security and privacy controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying security and privacy requirements. The security of information may change over time based on changes in the threat, agency missions/business functions, personnel, technology, or environments of operation. Consequently, maintaining a capability for real-time or near real-time analysis of the threat environment and situational awareness following an information security incident is paramount. The type, rigor, and frequency of control assessments should be commensurate with the level of awareness necessary for effectively determining information security risk that is established by the agency's risk tolerance and risk management strategy. Technical security tools such as malicious code scanners, vulnerability assessment products (which look for known security weaknesses, configuration errors, and the installation of the latest patches), and penetration testing can assist in the ongoing assessment of information systems.

5. Authorizing Official

The authorizing official is a senior agency official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations and assets, individuals, other organizations, and the Nation. Authorizing officials have budgetary oversight for an information system or are responsible for the mission or business operations supported by the system. Through the authorization process, authorizing officials are responsible and accountable for the security risks associated with information system operations. Because information security is closely related to the individual privacy protections required for PII (see *Fair Information Practice Principles*), authorizing officials are also responsible and accountable for the privacy-related risks that arise from the operation of an information system. Accordingly, authorizing officials must be in management positions with a level of authority commensurate with understanding and accepting such information system-related *security* and *privacy* risks. Since the SAOP is the senior official, designated by the head of each agency, who has overall agency-wide responsibility for information privacy, agencies must consider inputs and recommendations submitted by the SAOP in the authorization decision. Additionally, the SAOP has responsibility for reviewing the authorization package to ensure that privacy risks are addressed prior to system authorization. In situations where the authorizing official and SAOP cannot reach a final resolution regarding the appropriate protection for the agency information and information system, the head of the agency must review the associated

risks and requirements and make a final determination regarding the issuance of the authorization to operate.[76]

Agencies can choose from several different approaches when planning for and conducting authorizations. These include an authorization with a single authorizing official, an authorization with multiple authorizing officials, or leveraging an existing authorization (see Section 8, *Joint and Leveraged Authorizations*). Agencies can, at their discretion, include the CIO or the SAOP as co-authorizing officials with other senior agency officials responsible for the mission or line of business supported by the system being authorized for operation. Regardless of the approach used, the role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only.

6. Authorization to Operate

The authorization to operate an information system and the authorization of agency-designated common controls granted by senior Federal officials provide an important quality control for agencies. The decision to authorize a system to operate should be based on a review of the authorization package and includes an assessment of compliance with applicable requirements and risk to agency operations and assets, individuals, other organizations, and the Nation. As stated above, the decision to authorize a system, or agency-defined common controls, should be made by the appropriate authorizing official – an agency official responsible for the associated missions, business functions, and/or supporting infrastructure. Since the security plan and privacy plan establish the security and privacy controls selected for implementation, those plans are a critical part of the authorization package and should form the basis for the authorization, supplemented by more specific information as needed.

7. Ongoing Authorization

Ongoing authorization[77] is a process whereby the authorizing official makes risk determination and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's risk tolerance and mission/business requirements. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the near real-time state of the information system and inherited common controls to determine whether or not all applicable security and privacy requirements have been satisfied and the mission/business risk is acceptable. Effective ongoing authorization requires robust ISCM and PCM strategies and effective operational ISCM and PCM programs. Agencies can move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process for information systems and common controls after having satisfied two

[76] The head of the agency is the highest-level senior official or executive within an agency with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation. It is possible for the head of the agency to serve as the Authorizing Official and, in those situations, the decision to authorize a system to operate is final.

[77] For additional information on Ongoing Authorization and its relationship to initial authorization and reauthorization, refer to NIST *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management.*

conditions: the system and/or common controls have been granted an initial authorization to operate by the designated authorizing official; and ISCM and PCM programs are in place to monitor all implemented security and privacy controls with the appropriate degree of rigor and at the appropriate frequencies in accordance with applicable ISCM and PCM strategies, OMB guidance and NIST guidelines.

Agencies must define and implement a process to specifically designate information systems and/or common controls that have satisfied the two conditions noted in the previous paragraph and have been transitioned to ongoing authorization. The process includes the means for the authorizing official to formally acknowledge that the information system and/or common controls are being managed under an ongoing authorization process and accept the responsibility for ensuring all necessary activities associated with the ongoing authorization process are performed. Until a formal approval is obtained from the authorizing official to transition to ongoing authorization, information systems (and common controls) remain under a static authorization process with specific authorization termination dates enforced by the agency.

8. Reauthorization

Reauthorization consists of a review of the information system similar to the review carried out during the initial authorization but conducted during the operations/maintenance phase of the system development life cycle rather than prior to that phase. In general, reauthorization actions may be time-driven or event-driven. However, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that increases information security risk above the previously agreed-upon agency risk tolerance. Event-driven reauthorization triggers can include, for example: new threat, vulnerability, or impact information; an increased number of findings, weaknesses, or deficiencies from continuous monitoring programs; new missions or business functions; new or modified security requirements; changes in authorizing officials; significant changes in risk assessment findings; significant changes to information systems, common controls, or environments of operation; exceeding agency-designated thresholds; and changes in Federal statutes, OMB policies, or NIST standards and guidelines. A significant change is defined as a change that is likely to affect the security state of an information system.

The reauthorization process differs from the initial authorization inasmuch as the authorizing official can initiate: a complete zero-base review of the information system or common controls; or a targeted review based on the type of event that triggered the reauthorization, the assessment of risk related to the event, the risk response of the agency, and the agency risk tolerance. Reauthorization is a separate activity from the ongoing authorization process, though security- and privacy-related information from the agency's ISCM and PCM programs may still be leveraged to support reauthorization. Note also that reauthorization actions may necessitate a review of and changes to the ISCM or PCM strategy, which may in turn affect ongoing authorization.

9. Joint and Leveraged Authorizations

Agencies are encouraged to use joint and leveraged authorizations whenever practicable.[78] Joint authorizations can be used when multiple agency officials either from the same agency or different agencies, have a shared interest in authorizing an information system or common controls. The participating officials are collectively responsible and accountable for the system and the common controls and jointly accept the information security risks that may adversely impact agency operations and assets, individuals, other organizations, and the Nation. Agencies choosing a joint authorization approach should work together on the planning and the execution of the Risk Management Framework tasks described in NIST Special Publication 800-37 and document their agreement and progress in implementing the tasks. The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization including, for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only as long as there is mutual agreement among authorizing officials and the authorization meets the requirements established by Federal and/or agency policies.

Leveraged authorizations can be used when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency based on the need to use the same information resources (e.g., information system and/or services provided by the system). The leveraging agency reviews the owning agency's authorization package as the basis for determining risk to the leveraging agency. The leveraging agency considers risk factors such as the time elapsed since the authorization results were produced, differences in environments of operation (if applicable), the impact of the information to be processed, stored, or transmitted, and the overall risk tolerance of the leveraging agency. The leveraging agency may determine that additional security measures are needed and negotiate with the owning agency to provide such measures. To the extent that a leveraged authorization includes an information system that collects, processes, stores, maintains, transmits, or disseminates PII, leveraging agencies must consult their SAOP. The SAOP, may determine that additional measures are required to protect PII prior to leveraging the authorization.

10. Continuous Monitoring

Agencies must develop ISCM and PCM and implement ISCM and PCM activities in accordance with applicable statutes, directives, policies, instructions, regulations, standards, and guidelines. Agencies have the flexibility to develop an overarching ISCM and PCM strategy (e.g., at the agency, bureau, or component level) that address all information systems, or continuous monitoring strategies that address each agency information system individually. The ISCM and PCM strategies must address all security and privacy controls selected and implemented by agencies, including the frequency of and degree of rigor associated with the monitoring process. ISCM and PCM strategies, which must be approved by the SAOP and appropriate agency authorizing official, must also include all common controls inherited by agency information systems.

[78] NIST Special Publication 800-37 provides guidance on joint and leveraged security authorizations.

11. Critical Infrastructure

Agencies that operate information systems that are part of the critical infrastructure must conduct risk assessment to ensure that security controls for those systems are appropriately tailored (including the deployment of additional controls, when necessary), thus providing the required level of protection for critical Federal missions and business operations. In addition, agencies must ensure that the privacy controls assigned to critical infrastructure meet all applicable requirements and adequately protect individual privacy. This includes the ongoing monitoring of deployed security and privacy controls in critical infrastructure systems to determine the ongoing effectiveness of those controls against current threats; improving the effectiveness of those controls, when necessary; managing associated changes to the systems and environments of operation; and satisfying specific protection and compliance requirements in statutes, Executive Orders, directives, and policies required for critical infrastructure protection.

12. Encryption

When the assessed risk indicates the need, agencies must encrypt Federal information at rest and in transit unless otherwise protected by alternative physical and logical safeguards implemented at multiple layers, including networks, systems, applications, and data. Encrypting information at rest and in transit helps to protect the confidentiality, integrity, and availability of such information by making it less susceptible to unauthorized disclosure or modification. Agencies must apply encryption requirements to Federal information categorized as either moderate or high impact in accordance with FIPS Publication 199 unless encrypting such information is technically unfeasible or would demonstrably affect their ability to carry out their respective mission, functions, or operations. In situations where the use of encryption is technically infeasible, for example, due to an aging legacy system, agencies must initiate the appropriate system or system component upgrade or replacement actions at the earliest opportunity to be able to accommodate such safeguarding technologies. Authorizing officials who choose to operate information systems without the use of required encryption technologies must carefully assess the risk in doing so and they must receive written approval for the exception from the agency CIO. For high impact information, access to unencrypted content should be managed separately from access to the networks, systems, and applications where the encrypted data resides. Only FIPS-validated and NSA-approved cryptography are approved for use in Federal information systems.

13. Digital Signatures

Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use. Additionally, digital signatures can help agencies streamline mission/business processes and transition manual processes to more automated processes to include, for example, online transactions. Because of the advantages provided by this technology, OMB expects agencies to implement digital signature capabilities in accordance with Federal Public Key Infrastructure (PKI) policy, and NIST standards and guidelines. For employees and contractors, agencies must require the use of the digital signature capability of Personal Identity Verification (PIV) credentials when the

capability is available.[79] For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures.

14. Identity Assurance

To streamline the process of citizens, businesses, and other partners[80] securely accessing government services online requires a risk-appropriate demand of identity assurance. Identity assurance, in an online context, is the ability of an agency to determine that a claim to a particular identity made by an individual can be trusted to actually be the individual's "true" identity. Citizens, businesses, and other partners that interact with the Federal Government need to have and be able to present electronic identity credentials to identify and authenticate themselves remotely and securely when accessing Federal information resources. An agency needs to be able to know, to a degree of certainty commensurate with the risk determination, that the presented electronic identity credential truly represents the individual presenting the credential before a transaction is authorized.[81] To transform processes for citizens, businesses, and other partners accessing Federal services online, OMB expects agencies to use a standards-based federated identity management approach that enables security, privacy, ease-of-use, and interoperability among electronic authentication systems.

15. Unsupported Information System Components

Unsupported information system components (e.g., when vendors are no longer providing critical software patches) provide a substantial opportunity for adversaries to exploit weaknesses discovered in the currently installed components. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. For such systems, agencies can establish in-house support, for example, by developing customized patches for critical software components or securing the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

16. FISMA Applicability to Non-Federal Entities

FISMA describes Federal agency security responsibilities as including "information collected or maintained by or on behalf of an agency" and "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." FISMA requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or

[79] NIST FIPS 201 provides additional information on use of Personal Identity Verification credentials.

[80] "Other partners" may include contractors not subject to the NIST FIPS 201 identity standard.

[81] NIST Special Publication 800-63 provides additional guidance on identity assurance.

managed by another agency, contractor, or other source." This includes services that are either fully or partially provided, including agency hosted, outsourced, and cloud-based solutions.

Additionally, because FISMA applies to Federal information and information systems, in certain circumstances, its requirements also apply to a specific class of information technology that the Clinger-Cohen Act of 1996 (40 U.S.C. § 1401(3)) did not include, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal information is used within incidentally acquired equipment, the agency continues to be responsible and accountable for ensuring that FISMA requirements are met for such information.

17. Other Requirements

Agencies must adhere to all other applicable information requirements such as the privacy requirements in accordance with the Privacy Act of 1974 and OMB guidance, the Confidential Information Protection and Statistical Efficiency Act of 2002 and OMB guidance, and to statutes and regulations pertaining to management of Federal records, and other relevant statutes, Executive Orders, Presidential Directives, and policies.

18. Authorities and References[82]

a. Privacy Act of 1974 (5 U.S.C. § 552a), December 1974.

b. E-Government Act of 2002 (44 U.S.C. chapters 35 and 36), December 2002.

c. Federal Information Security Modernization Act of 2014 (44 U.S.C. chapter 35), December 2014.

d. Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. § 401 note), December 2004.

e. Executive Order 13556, *Controlled Unclassified Information*, November 2010.

f. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.

g. Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.

h. Homeland Security Presidential Directive 20 (National Security Presidential Directive 51), National Continuity Policy, May 2007.

i. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, February 2008.

j. National Communications System (NCS) Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, July 2007.

[82] OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default. References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

k. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), *Standards for Security Categorization of Federal Information and Information Systems*.

l. National Institute of Standards and Technology Federal Information Processing Standards Publication 200 (as amended), *Minimum Security Requirements for Federal Information and Information Systems*.

m. National Institute of Standards and Technology Federal Information Processing Standards Publication 201 (as amended), *Personal Identity Verification of Federal Employees and Contractors*.

n. Committee on National Security Systems Instruction 1253 (as amended), *Security Categorization and Control Selection for National Security Systems*.

o. National Institute of Standards and Technology Special Publication 800-18 (as amended), *Guide for Developing Security Plans for Federal Information Systems*.

p. National Institute of Standards and Technology Special Publication 800-30 (as amended), *Guide for Conducting Risk Assessments*.

q. National Institute of Standards and Technology Special Publication 800-37 (as amended), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

r. National Institute of Standards and Technology Special Publication 800-39 (as amended), *Managing Information Security Risk: Organization, Mission, and Information System View*.

s. National Institute of Standards and Technology Special Publication 800-47 (as amended), *Security Guide for Interconnecting Information Technology Systems.*

t. National Institute of Standards and Technology Special Publication 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*.

u. National Institute of Standards and Technology Special Publication 800-53A (as amended), *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.

v. National Institute of Standards and Technology Special Publication 800-59 (as amended), *Guideline for Identifying an Information System as a National Security System*.

w. National Institute of Standards and Technology Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*.

x. National Institute of Standards and Technology Special Publication 800-63 (as amended), *Electronic Authentication Guideline*.

y. National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

z. National Institute of Standards and Technology Special Publication 800-137 (as amended), *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

aa. National Institute of Standards and Technology Special Publication 800-160 (as amended), *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*.

bb. National Institute of Standards and Technology Special Publication 800-161 (as amended), *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

cc. National Institute of Standards and Technology Special Publication 800-162 (as amended), *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.

dd. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (as amended).

ee. National Institute of Standards and Technology *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management* (as amended).

19. Definitions

a. The terms 'Agency', 'Executive Agency', 'Federal information,' 'Federal information system,' 'information resources management', 'information security,' 'personally identifiable information,' and 'senior agency official for privacy' are defined in the main body of this Circular.

b. 'Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

c. 'Authorization' means the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

d. 'Authorization boundary' means all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.[83]

e. 'Authorization official' means 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 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.

[83] Agencies have significant flexibility in determining what constitutes an information system and its associated boundary.

f. 'Authorization package' means the essential information that an authorizing official uses to determine whether or not to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

g. 'Breach' means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

h. 'Common control' means a security or privacy control that is inherited by multiple information systems.

i. 'Controlled unclassified information' means information that requires safeguarding or dissemination controls pursuant to and consistent with statutes, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

j. 'Critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters (42 U.S.C. § 5195c(e)).

k. 'Environment of operation' means the physical, technical, and organizational setting in which an information system operates.

l. 'Hybrid control' means a control that is implemented in an information system in part as a common control and in part as a system-specific control.

m. 'Information security architecture' means an embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, information security systems, personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

n. 'Information security continuous monitoring' means maintaining ongoing awareness of information security, vulnerabilities, and threats to support agency risk management decisions.[84]

o. 'Information security program plan' means a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. The information security program plan and the privacy program plan may be integrated into one consolidated document.

p. 'Information system resilience' means the ability of an information system: to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining

[84] The terms *continuous* and *ongoing* in this context mean that security controls and agency risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect agency information.

essential operational capabilities; and to recover to an effective operational posture in a time frame consistent with mission needs.

q. 'Initial authorization' means the initial (start-up) risk determination and risk acceptance decision based on a zero-base review of the information system conducted prior to its entering the operations/maintenance phase of the system development life cycle. The zero-base review includes an assessment of all security and privacy controls (i.e., system-specific, hybrid, and common controls) contained in a security plan or in a privacy plan and implemented within an information system or the environment in which the system operates.

r. 'National security system' means any information 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: 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 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 (44 U.S.C. § 3552).

s. 'Ongoing authorization' means the risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission/business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether or not the mission/business risk of continued system operation is acceptable.

t. 'Overlay' means a specification of security and/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" definition.)

u. 'Privacy continuous monitoring' means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable requirements and to adequately protect personally identifiable information.

v. 'Privacy control' means the administrative, technical, and physical safeguards employed within agencies to protect and ensure the proper handling of personally identifiable information or prevent activities that create privacy risk.

w. 'Privacy control assessment' means the testing or evaluation of privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the privacy requirements for an information system or organization.

x. ‘Privacy program plan’ means a formal document that provides an overview of the privacy requirements for an agency-wide privacy program and describes the program management controls and common controls in place or planned for meeting those requirements. The privacy program plan and the information security program plan may be integrated into one consolidated document.

y. ‘Privacy plan’ means a formal document that provides an overview of the privacy requirements for an information system or program and describes the privacy controls in place or planned for meeting those requirements. The privacy plan and the security plan may be integrated into one consolidated document.

z. ‘Reauthorization’ means the risk determination and risk acceptance decision that occurs after an initial authorization. In general, reauthorization actions may be time-driven or event-driven; however, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that drives information security or privacy risk above the previously agreed-upon agency risk tolerance.

aa. ‘Resilience’ means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

bb. ‘Risk’ means 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.

cc. ‘Risk management’ means the program and supporting processes to manage information security and privacy 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.

dd. ‘Risk response’ means accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.

ee. ‘Security category’ means 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.

ff. ‘Security control’ means 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.

gg. ‘Security control assessment’ means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

hh. ‘Security control baseline’ means the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

ii. ‘Security plan’ means a 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 security plan and the privacy plan may be integrated into one consolidated document.

jj. ‘Supply chain’ means a linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

kk. ‘Supply chain risk management’ means the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

ll. ‘System-specific control’ means a control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.

mm. ‘Systems security engineering’ means a specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that: satisfies stakeholder requirements; is seamlessly integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to stakeholders.

nn. ‘Tailoring’ means the process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls. (See “overlay” definition.)

oo. ‘Trustworthiness’ means the degree to which an information system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across a full range of threats.

pp. ‘Trustworthy information system’ means a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.