CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction

Information and information technology (IT) resources are critical to the U.S. social, political, and economic well-being. They enable the Federal Government to provide quality services to citizens, generate and disseminate knowledge, and facilitate greater productivity and advancement as a Nation. It is important for the Federal Government to maximize the quality and security of Federal information systems, and to develop and implement uniform and consistent information resources management policies in order to inform the public and improve the productivity, efficiency, and effectiveness of agency programs. Additionally, as technology evolves, it is important that agencies manage information systems in a way that addresses and mitigates security and privacy risks associated with new information technologies and new information processing capabilities.

These new information technologies and information processing capabilities also provide significant opportunities for agencies. The deeply embedded nature of IT in all Federal agency missions and business processes, and the emergence of the digital economy, combined with the increasing interconnection of technology and public services, has changed the way we share information, changed the way we use and view technology, and has forever changed Americans' expectations. To meet expectations of the American people and facilitate innovation, the Federal Government must continue to transform itself to embrace and respond to the digital revolution by developing and maintaining a top-notch workforce and delivering secure, world-class digital services that serve the public. With IT at the core of nearly everything the Federal Government does, agencies must continually identify ways to apply new and emerging technologies that can fundamentally improve the way Government works and delivers services to the American people in the most cost-effective way possible. Delivering world-class digital services requires the Federal Government to change its approach to buying, building, and delivering IT and information. This Circular is designed to help drive the transformation of the Federal Government and the way it builds, buys, and delivers technology by institutionalizing more agile approaches intended to facilitate the rapid adoption of changing technologies, in a way that enhances information security, privacy, and management of information resources across all Federal programs and services.

2. Purpose

This Circular[1] establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. The appendices to this Circular also include responsibilities for protecting Federal information resources and managing personally identifiable information (PII). While it is the responsibility of all agency leadership, program managers, and staff to implement the requirements of this Circular, agency heads have ultimate

[1] Although this Circular touches on many specific information resources management 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. Agencies shall implement the policies in this Circular and those in other OMB policy guidance in a mutually consistent fashion.

responsibility for ensuring that the requirements of this Circular are implemented for their agency.

3. Applicability

The requirements of this Circular apply to the information resources management activities of all agencies[2] 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. § 3552), but are encouraged to do so where appropriate. For national security systems, agencies shall follow applicable statutes, executive orders, directives, and internal agency policies.

4. Basic Considerations

Federal information is both a strategic asset and a valuable national resource. It enables the Government to carry out its mission and programs effectively. It provides the public with knowledge of the Government, society, economy, and environment – past, present, and future. Federal information is also a means to ensure the accountability of Government, to manage the Government's operations, and to maintain and enhance the performance of the economy, the public health, and welfare. Appropriate access to Federal information significantly enhances the value of the information and the return on the Nation's investment in its creation. The following considerations reflect these principles:

a. The free flow of information between the Government and the public is essential to a democratic society. Therefore, the management of Federal information resources shall protect the public's right of access to Federal information;

b. Government agencies shall 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, and increases public access to valuable Federal information;

c. Making Federal information discoverable, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves the lives of Americans, and contributes significantly to national stability and prosperity, and fosters public participation in Government;

d. The Federal Government shall provide members of the public with access to public information on Government websites. This responsibility includes taking affirmative steps to ensure and maximize the quality, objectivity, utility, and integrity of Federal information prior to public dissemination, and maintaining processes for addressing requests for correction of information disseminated publicly;

[2] '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.

e. 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 resources;

f. Federal information is a strategic asset subject to risks that must be managed to minimize harm;

g. Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle;

h. While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements;

i. The design of information collections shall be consistent with the intended use of the information, and the need for new information shall be balanced against the burden imposed on the public, the cost of the collection, and any privacy risks;

j. It is essential that the Federal Government minimize the Federal information collection burden on the public, minimize the costs of its information activities, and maximize the usefulness of Government information; and

k. Attention to the management of Federal Government records from creation to disposition is an essential component of sound information resources management that promotes public accountability. Together with records preservation, it helps protect the Federal Government's historical record and safeguards the legal and financial rights of the Federal Government and the public.

5. Policy

Agencies shall 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 missions; implementing an 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 a strategy for managing and maintaining their information resources, referred to as the Information Resource Management (IRM) Strategic Plan, 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 IRM Strategic Plan that describes the agency's technology and information resources

goals, including but not limited to, the processes described in this Circular. The IRM Strategic Plan must support the goals of the Agency Strategic Plan required by the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act). The IRM Strategic Plan shall demonstrate how the technology and information resources goals map to the agency's mission and organizational priorities. These goals shall be specific, verifiable, and measurable, so that progress against these goals can be tracked. The agency shall review its IRM Strategic Plan 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 meet the following requirements, in addition to all other requirements in this Circular:

a) Inventories

Agencies shall:

i. Maintain an inventory[3] of the agency's major information systems,[4] information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; and

ii. Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.[5]

b) Information Management

Agencies shall:

i. Continually facilitate adoption of new and emerging technologies, and regularly assess the following throughout the life of each information system: the inventory of the physical and software assets associated with the system[6]; the maintainability and sustainability of the information resources and infrastructure supporting the system; and actively determine when significant upgrades,

[3] The inventory of agency information resources shall include an enterprise-wide data inventory that accounts for data used in the agency's information systems.

[4] The inventory of major information systems is required in accordance with 44 U.S.C. § 3505(c). All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system.

[5] This inventory may be combined with the agency's inventory of information systems, as described above.

[6] Agencies shall ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried initially when obtained and updated on an ongoing basis.

replacements, or disposition is required to effectively support agency missions or business functions and adequately protect agency assets;[7] and

ii. Ensure the terms and conditions of contracts and other agreements involving the processing, storage, access to, transmission, and disposition of Federal information are linked to the IRM strategic plan goals, and are sufficient to enable agencies to meet their policy and legal requirements.

c) Risk Management

Agencies shall:

i. Consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed;

ii. Develop plan, in consultation with Chief Information Officers (CIOs), Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement;[8]

iii. Regularly review and address risk regarding processes, people, and technology; and

iv. Consult National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) (e.g., 500, 800, and 1800 series guidelines).

2) Enterprise Architecture

Agencies shall develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. The EA should 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 to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

[7] The assessment process is described in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations.*

[8] 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 SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* provides additional guidance on unsupported software components.

3) Planning, Programming, and Budgeting

Agencies shall, in accordance with the Federal Information Technology Acquisition Reform Act (FITARA) and related OMB policy:[9]

a) Ensure that IT resources are distinctly identified and separated from non-IT resources during the planning, programming, and budgeting processes in a manner that affords agency CIOs appropriate visibility and specificity to provide effective management and oversight of IT resources;

b) Ensure that the agency-wide budget development process includes the CFO, CAO, and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily information- and technology-oriented);

c) The agency head, in consultation with the CFO, CAO, 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 IT investments and their underlying capabilities against other proposed and ongoing IT investments in the portfolio; and

   ii. Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and developing a corrective action plan to close such gaps;

d) Ensure that 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 that the CIO is included in the internal planning processes for how the agency uses information resources to achieve its objectives at all points in their life cycle, including operations and disposition or migration;

e) 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 IT investments portion of the budget request;

   ii. The SAOP has reviewed the IT investments portion of the budget request to ensure that privacy requirements, as well as any associated costs, are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

[9] OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default. The Department of Defense (DoD), the Intelligence Community, and portions of other agencies that operate systems related to national security are subject to only certain portions of Federal Information Technology Acquisition Reform (FITARA) (Pub. L. 113-291), as provided for in the statute.

iii. 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

iv. The IT Portfolio includes appropriate estimates of all IT resources included in the budget request;

f) Ensure that 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.

4) Business Continuity Planning

Agencies shall develop a Business Continuity Plan.[10] A Business Continuity Plan to continue agency operations during times of service disruption is essential. Therefore, agencies shall develop continuity strategies in order to ensure services and access can be restored in time to meet the mission needs. Manual workarounds shall be part of the plan so business can continue while information systems are being restored.

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) Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately. At a minimum, these processes and policies shall require that:

a) Investments and projects in development are evaluated to determine the applicability of agile development;[11]

b) Open data standards are used to the maximum extent possible when implementing IT systems;

c) Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances[12] of IT projects across the portfolio leveraging processes such

[10] The Federal Information Security Modernization Act of 2014 (FISMA) (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, see Appendix I.

[11] This evaluation shall be conducted as part of the acquisition planning process and involve staff from the CIO of the department, the implementing program managers, the appropriate contracting office representatives, and other applicable agency officials;

[12] Standard definitions from budget or performance management practices, such as earned value management, shall be used for cost variance and schedule variance to measure progress.

as IT investment management, enterprise architecture, and other agency IT or performance management processes;[13]

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

e) Data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives;[14] and

f) Unsupported information systems and system components[15] are phased out as rapidly as possible, and planning and budgeting activities for all IT systems and services incorporate migration planning and resourcing to accomplish this requirement;

3) Ensure that the CIO is a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives. The CIO may designate, in consultation with other senior agency officials, other agency officials to act as their representative to fulfill aspects of this responsibility so long as the CIO retains accountability;

4) Require that information security and privacy be fully integrated into the system development process;

5) Conduct TechStat reviews, led by the CIO, or use other applicable performance measurements to evaluate the use of agency information 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;

6) Establish and maintain a process for the CIO to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. It shall be the CIO and program managers' shared responsibility to ensure that legacy and ongoing IT investments are appropriately delivering customer value and meeting the business objectives of the agency and the programs that support the agency; and

7) Measure performance in accordance with the GPRA Modernization Act and OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*.

---

[13] The Federal Acquisition Streamlining Act of 1994 (Pub. L. 103-355) 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.

[14] In accordance with the information management responsibilities outlined in 44 U.S.C. § 3506(b).

[15] Includes hardware, software, or firmware components no longer supported by developers, vendors, manufacturers, or communities through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

c. Leadership and Workforce

Agencies shall:

1) Require that the Chief Human Capital Officer (CHCO), CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions, and develop and maintain a current workforce planning process to ensure that 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 that the workforce, which supports the acquisition, management, maintenance, and use of information resources, has the appropriate knowledge and skills to facilitate the achievement of the portfolio's performance goals and, further, evaluate the extent to which the agency's executive-level workforce has appropriate information and technology-related knowledge and skills;

3) Implement innovative approaches and track performance of workforce development training, including cross-functional training, rotational development and assignments, and effective training and education used by the private sector, to maintain and enhance skills or obtain additional skills;

4) Ensure that the CHCO and CIO jointly establish an agency-wide critical element (or elements) to be included in all component or bureau CIOs' performance evaluations. In addition, the CIO shall identify key component or bureau CIOs and provide input to the rating official for these component or 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 component or bureau CIO during progress reviews;

5) Ensure that the CIO is involved in the recruitment, approves the selection, and provides input for the performance review of any component or bureau CIO, which includes any component or bureau leader who holds CIO duties but not necessarily the "CIO" title. The title and responsibilities of current component or bureau CIOs should be designated or transferred to other agency personnel by the agency head or their designee as appropriate, and such decisions should take into consideration recommendations from the agency CIO;

6) Ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy; and

7) Ensure that the CIO, CHCO, SAOP, and other hiring managers take advantage of flexible hiring authorities for specialized positions, as established by the Office of Personnel Management (OPM).

d. IT Investment Management

1) Acquisition of Information Technology and Services

Agencies shall:

a) Make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between Government and contractor when acquiring IT;

b) Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full life cycle 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;[16]

c) Consider existing Federal contract solutions or shared services when developing planned information systems, available within the same agency, from other agencies, or from the private sector to meet agency needs to avoid duplicative IT investments;

d) Acquire IT products and services in accordance with Government-wide requirements;[17]

e) Ensure that decisions to improve existing information systems with custom-developed solutions or develop new information systems are initiated only when no existing alternative private sector or governmental source can efficiently meet the need, taking into account long-term sustainment and maintenance;

f) 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;

g) To the extent practicable, modular contracts for IT, including orders for increments or useful segments of work, should be awarded within 180 days after the solicitation is issued. If award cannot be made within 180 days, agencies shall consider cancelling the solicitation. The IT acquired should be delivered within 18 months after the solicitation resulting in award of the contract was issued;[18]

h) Align IT procurement requirements with larger agency strategic goals;

i) Promote innovation in IT procurements, including conducting market research in order to maximize utilization of innovative ideas; and

j) Include security, privacy, accessibility, records management, and other relevant requirements in solicitations.

2) Agency Approval

Agencies shall ensure that all acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support

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

[17] For information regarding Government-wide requirements, refer to OMB policy and the Federal Acquisition Regulation. For the acquisition of Personal Identity Verification (PIV) and public key infrastructure (PKI) products and services, also refer to the FIPS 201 Evaluation Program at https://www.idmanagement.gov.

[18] Pursuant to Public Contracts statute (41 U.S.C. § 2308).

purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO. These approvals shall consider the following factors:

a) Alignment with mission and program objectives in coordination with program leadership;

b) Appropriateness with respect to the mission and business objectives supported by the IRM Strategic Plan;

c) Inclusion of innovative solutions;

d) Appropriateness of contract type for IT-related resources;

e) Appropriateness of IT-related portions of statement of needs or statement of work;

f) Ability to deliver functionality in short increments;

g) Inclusion of Government-wide IT requirements, such as information security; and

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

3) Investment Planning and Control

Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT 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) Decisions related to major IT investments are supported by business cases with appropriate evidence;

c) IT investments implement an agile development approach, as appropriate;[19]

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

e) IT capital investment plans and budgetary requests are reviewed to ensure that Government-wide requirements, as well as any associated costs, are explicitly identified and included, with respect to any IT resources. This includes IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and

[19] For additional information, refer to OMB memoranda at https://www.whitehouse.gov/omb/memoranda_default.

f) Decisions to improve, enhance, or modernize existing IT investments or to develop new IT 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 option representing the best value to the Government has been selected.

4) Selection Criteria and Requirements

Agencies shall consider the following factors when analyzing IT investments:

a) 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;

b) All decisions concerning the selection of information system technologies and services – including decisions to acquire or develop custom or duplicative solutions – shall be merit-based and consider factors such as, but not limited to, ability to meet operational or mission requirements, total life cycle cost of ownership, performance, security, interoperability, privacy, accessibility, ability to share or reuse, resources required to switch vendors, and availability of quality support. Consistent with the FAR, contracts for custom software development are to include contractual provisions that reaffirm the right to reuse the software throughout the Federal Government;

c) Agencies shall consider use of suitable existing Federal information technology resources and commercially-available solutions in order to ensure effective management of Federal resources. Consistent with law and regulation, agencies should consider and evaluate the suitability of existing Federal information technologies and related services, including software, Federal shared services, and commercially-available solutions before embarking upon new developments of software and information technologies; and

d) 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 standards and guidelines.

5) IT Investment Design and Management

Agencies shall implement the following requirements:

a) Information systems and processes must support and maximize interoperability and access to information, where appropriate, by using documented, scalable, and continuously available application programming interfaces and open machine-readable formats;

b) IT investments must facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and communications platforms;

c) Information systems, technologies, and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and

IT accessibility requirements commonly known as "section 508" requirements (29 U.S.C. § 794d);

d) Records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning 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

e) IT investments use an Earned Value Management System (EVMS) and Integrated Baseline Review, when appropriate, as required by FAR Subpart 34.2. When an EVMS is required, agencies must have a documented process for accepting a contractor's EVMS. Agencies are encouraged to share information about their acceptance process with other agencies and to consider recognizing each other's acceptance of an EVMS so that a contractor is not required to complete a duplicative process. When an EVMS is not required, implement a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance.

e. Information Management and Access

1) Agencies shall incorporate the following steps, as appropriate, in planning, budgeting, governance, and other policies:

a) Federal information is properly managed throughout its life cycle, including all stages through which the information passes, such as: creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition;

b) Federal information is managed by making information accessible, discoverable, and usable by the public to the extent permitted by law and subject to privacy, security (which includes confidentiality), or other valid restrictions pertaining to access, use, dissemination, and disclosure;

c) Federal information is managed consistent with applicable records retention and disposition requirements;

d) Federal information and information systems are managed in a manner that identifies and mitigates privacy and security risks; and

e) Federal 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 have a responsibility to provide information to the public consistent with their missions and subject to Federal law and policy. Agencies will discharge this responsibility by:

a) Publishing public information online in a manner that promotes analysis and reuse for the widest possible range of purposes, meaning that the information is publicly accessible, machine-readable, appropriately described, complete, and timely. This

includes providing such public information in a format(s) accessible to employees and members of the public with disabilities;[20]

b) Avoiding establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the agency's ability to disseminate its public information on a timely and equitable basis;

c) Avoiding charging fees or royalties for public information or establishing unnecessary restrictions on the resale or re-dissemination of public information by the public. Agencies shall not, unless specifically authorized by statute, establish fees that exceed the cost of dissemination to the public, restrict or regulate the use, resale, or re-dissemination of public information by the public; or establish any mechanism that interferes with the timely and equitable availability of public information to the public;[21]

d) As appropriate, making Government publications available to depository libraries through the Government Publishing Office regardless of format;[22]

e) Taking advantage of all dissemination channels, including Federal, State, local, tribal, and territorial governments, libraries and educational institutions, for-profit and nonprofit organizations, and private sector entities, in discharging agency information dissemination responsibilities; and

f) Considering the impact of providing agency information and services over the Internet for individuals who do not own computers or lack Internet access and, to the extent practicable, pursuing additional or alternative modes of delivery to ensure that such information and services are accessible to, and their availability is not diminished for, such individuals.

3) Agencies shall establish policies, procedures, and standards that enable data governance so that information is managed and maintained according to relevant statute, regulations, and guidance.

4) Agencies shall collect or create information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public, where appropriate, by 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 in accordance with OMB guidance.

5) Agencies shall include appropriate provisions in contracts, and other agreements, to encourage recipients of Federal funding to maximize access to data developed under an award and to prepare data management plans that describe data to be created in funded programs and approaches for long-term preservation and access to created data.

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

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

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

6) Agencies shall ensure that there is a mechanism for the public to provide feedback about public information.

7) Agencies shall manage information in accordance with the following principles as appropriate:

   a) Providing notice of Federal agency practices for the creation, collection, use, processing, preservation, storage, maintenance, disclosure, dissemination, and disposal of information, 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) 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; and

   h) Complying with all applicable statutes and policies governing the disclosure or dissemination of information, including those related to the quality, privacy, security, accessibility, and other valid access, use, and dissemination restrictions.

f. Privacy and Information Security[23]

   1) Privacy

      Agencies shall:

      a) Establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks;[24]

      b) Designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to

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

[24] When considering privacy risks, privacy programs shall consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of their PII.

ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency;[25]

c) Monitor Federal law, regulation, and policy for changes that affect privacy;

d) Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions;

e) To the extent reasonably practicable, ensure that PII is accurate, relevant, timely, and complete, and reduce all PII to the minimum necessary for the proper performance of authorized agency functions;

f) Take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier;

g) Comply with all applicable privacy-related laws, including the requirements of the Privacy Act,[26] and ensure that the Privacy Act system of records notices are published, revised, and rescinded, as required;

h) Maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration (NARA);

i) Conduct privacy impact assessments when developing, procuring, or using IT, in accordance with the E-Government Act,[27] and make the privacy impact assessments available to the public in accordance with OMB policy;

j) Maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy; and

k) Ensure that the SAOP and the agency's privacy personnel closely coordinate with the agency CIO, senior agency information security officer, and other agency offices and officials, as appropriate.

[25] The SAOP shall be designated by the head of the agency, pursuant to Executive Order 13719, *Establishment of the Federal Privacy Council* (2016), and OMB guidance.

[26] Agencies should also consult OMB policies on privacy, and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.*

[27] Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under that section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

2) Information Security

To provide proper safeguards, agencies shall:

a) Ensure that 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 (FISMA);

b) Protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information; and

c) Implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).[28]

g. Electronic Signatures[29]

To support the transition to electronic government, agencies shall:

1) 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. Electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form;[30]

2) Promote 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; and [31]

[28] NISTIRs describe research of a technical nature of interest to a specialized audience.

[29] In support of Government Paperwork Elimination Act (GPEA) and Electronic Signatures in Global and National Commerce Act (E-Sign), the Federal Chief Information Officers Council maintains guidance on use of Electronic Signatures (E-Signatures) in Federal organization transactions. The Federal Chief Information Officers Council guidance, *Use of Electronic Signatures in Federal Organization Transactions*, can be located at https://www.idmanagement.gov. This guidance expands upon OMB guidance.

[30] Pursuant to the Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504).

[31] Pursuant to E-Sign (15 U.S.C. Chapter 96). 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.

3) Develop and implement processes to support use of digital signatures, a form of electronic signature, for employees and contractors.[32]

h. Records Management

Agencies shall:

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

2) Institute records management programs that provide documentation of agency activities;[33]

3) Manage electronic records in accordance with Government-wide requirements. This includes:

a) Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format; and

b) Managing all email records electronically and retaining them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed;

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

5) Ensure agency records managed by the SAORM are treated as information resources and follow the requirements in this Circular;

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

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

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

i. Leveraging the Evolving Internet

In a global and connected economy, it is essential for the United States and the Federal Government to strive to ensure that Internet-based technologies remain competitive. The Federal Government needs to continue to lead in innovation, contribute to the free flow of information, participate in an open and available market, and do this in a way that is scalable and secure. Networking demands, escalating with the continued emergence of connecting technologies, has grown well beyond initial capabilities. The use of the newest Internet Protocol (currently, Internet Protocol Version 6 [IPv6]) is an essential part of accomplishing

[32] Digital signatures can help agencies streamline mission or business processes and transition manual processes to more automated processes to include, for example, online transactions.

[33] Additional information regarding adequate and proper documentation is available in 36 C.F.R. § 1222.22.

these goals and ensuring that the network infrastructure can meet our needs for growing capacity, security, and privacy, and keep the United States competitive in the ever-escalating global electronic economy. Therefore, agencies shall:

1) Implement agency-wide processes requiring that all IT acquisitions using Internet Protocol conform to the FAR; and[34]

2) Ensure that all public-facing Internet services and enterprise networks fully support the newest version of Internet Protocol as required by OMB policy.

6. 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;[35]

2) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of IT;[36]

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;[37]

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;[38]

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;[39]

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

[35] National Institute of Standards and Technologies (NIST) Act, 15 U.S.C. § 278g-3.

[36] Pursuant to the NIST Act (15 U.S.C. § 278g-3).

[37] Pursuant to the National Telecommunications and Information Administration (NTIA) Organization Act, as amended (47 U.S.C. § 902(b)(2)(F)).

[38] Pursuant to the NTIA Organization Act, as amended (47 U.S.C. §902(b)(2)(G)).

[39] Pursuant to the NIST Act, 15 U.S.C. §§ 272(b), 278g-3, and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

6) Ensure that the Federal Government is represented in the development of national and international (in consultation with the Secretary of State) IT standards, and advise the Director of OMB on such activities;[40]

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

8) Solicit and consider the recommendations of the Information Security and Privacy Advisory Board regarding such standards and guidelines;[41] and

9) Lead the development of a Cybersecurity Framework to reduce cyber risks to critical infrastructure pursuant to Executive Order 13636, Improving Critical Infrastructure Cybersecurity.

b. Department of Homeland Security

The Secretary of Homeland Security shall:[42]

1) Perform its responsibilities under FISMA, including assisting OMB in carrying out its statutory authorities and functions of information security oversight and policy responsibilities;[43]

2) Develop and oversee the implementation of binding operational directives pursuant to FISMA;[44]

3) Monitor agency implementation of information security policies and practices;

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

5) Coordinate Government-wide efforts on information security policies and practices, including consultation with the Federal Chief Information Officers Council, and the Director of NIST;

6) Provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under 40 U.S.C. § 11331, including by:

a) Operating the Federal information security incident center established under 44 U.S.C. § 3556;

b) Upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate cyber threats and vulnerabilities, with or without reimbursement;

[40] Pursuant to NIST Act, 15 U.S.C. §§ 272(b), 273, 278g–3 and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

[41] Pursuant to the National Institute of Standards and Technology Act (15 U.S.C. §278g–4).

[42] Pursuant to FISMA (44 U.S.C. § 3553).

[43] FISMA, 44 U.S.C. § 3553(b)(1).

[44] FISMA, 44 U.S.C. § 3553(b)(2).

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

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

7) Consult with the Director of NIST regarding any binding operational directives that implements the standards and guidelines developed by NIST;

8) Coordinate the development of binding operational directives and the oversight of the implementation of such directives with OMB to ensure consistency with OMB policies;

9) Ensure that binding operational directives do not conflict with the guidelines issued under 40 U.S.C. § 11331;

10) Take other actions as the Director of OMB or the Secretary, in consultation with the Director of OMB, may determine necessary to carry out the implementation of effective agency information security policies and practices for information systems;

11) Manage Government-wide information security programs and provide and operate Federal information security shared services, in coordination with OMB and in accordance with OMB policies;

12) Provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under FISMA;[45] and

13) Solicit and consider the recommendations of the Information Security Privacy Advisory Board, established by the National Institute of Standards and Technology Act (NIST Act).[46]

c. Federal Chief Information Officers Council (Federal CIO Council)

Pursuant to the E-Government Act of 2002, the Federal CIO Council shall:[47]

1) Develop recommendations for OMB on Government information resources management policies and requirements;

2) Share experiences, ideas, best practices, and innovative approaches related to information resources management;

3) Assist OMB in the identification, development, and coordination of multiagency projects and other innovation initiatives to improve Federal Government performance through use of IT;

4) Promote the development and use of common performance measures for agency information resources management, as further described in statute;

[45] 44 U.S.C. § 3556(a)(4).

[46] Pursuant to DHS current practices.

[47] E-Government Act of 2002 (44 U.S.C. § 3603).

5) Work as appropriate with NIST and OMB to develop recommendations on IT standards developed under the NIST Act and promulgated under section 11331 of title 40, and maximize the use of commercial standards, as further described in statute;

6) Work with OPM to assess and address the hiring, training, classification, and professional development needs of the Federal Government related to information resources management;

7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities; and

8) Solicit perspectives from the Chief Financial Officers Council, Federal Acquisition Officers Council, Chief Human Capital Officers' Council, Budget Officers Advisory Council, and other key groups in the Federal Government, as well as industry, academia, and other Federal, State, local, tribal and territorial governments, on matters of concern to the Council as appropriate.

d. Federal Privacy Council

Pursuant to Executive Order 13719, the Federal Privacy Council shall:[48]

1) Develop recommendations for OMB on Federal Government privacy policies and requirements;

2) Coordinate and share ideas, best practices, and approaches for protecting privacy and implementing appropriate privacy safeguards;

3) Assess and recommend how best to address the hiring, training, and professional development needs of the Federal Government with respect to privacy matters;

4) Perform other privacy-related functions, consistent with law, as designated by the Chair of the Federal Privacy Council; and

5) In performing its duties, engage in appropriate coordination as described in Executive Order 13719.[49]

[48] Executive Order 13719, *Establishment of the Federal Privacy Council* (2016).

[49] Executive Order 13719, *Establishment of the Federal Privacy Council (2016)*at § 4(d), "Coordination":

(i) The Chair and the Privacy Council shall coordinate with the Federal Chief Information Officers Council (CIO Council) to promote consistency and efficiency across the executive branch when addressing privacy and information security issues. In addition, the Chairs of the Privacy Council and the CIO Council shall coordinate to ensure that the work of the two councils is complementary and not duplicative.

(ii) The Chair and the Privacy Council should coordinate, as appropriate, with such other interagency councils and councils and offices within the Executive Office of the President, as appropriate, including the President's Management Council, the Chief Financial Officers Council, the President's Council on Integrity and Efficiency, the National Science and Technology Council, the National Economic Council, the Domestic Policy Council, the National Security Council staff, the Office of Science and Technology Policy, the Interagency Council on Statistical Policy, the Federal Acquisition Regulatory Council, and the Small Agency Council.

e. General Services Administration

The Administrator of General Services shall:

1) Provide a Government-wide network services contract that leverages shared solutions for many agencies;[50]

2) Ensure that contract vehicles and services made available to agencies are cost-effective and provide for capabilities that are consistent with Government-wide requirements;[51]

3) Assist OMB in setting strategic direction for electronic government and overseeing Government-wide implementation, and recommend changes relating to Government-wide strategies and priorities;[52]

4) Promote innovative uses of IT by agencies, particularly initiatives involving multiagency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies;[53]

5) Maintain a Federal public key infrastructure (PKI) framework to allow efficient interoperability among agencies when using digital certificates;[54] and

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

f. National Archives and Records Administration

The Archivist of the United States shall:

1) Administer the Federal Records Act and NARA regulations (36 CFR Subchapter B—Records Management);[55]

2) Develop regulations relating to electronic records management;[56]

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;[57]

---

[50] Pursuant to the Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (40 U.S.C. § 11314(b)).

[51] Pursuant to the Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (40 U.S.C. §§ 11302, 11314(a)).

[52] Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3602).

[53] Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3602).

[54] Federal PKI provides the government with a common infrastructure to administer digital certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

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

[56] Pursuant to the Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapters 31 and 33).

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

4) Ensure agency compliance with records management requirements, provide records management training, and facilitate public access to high-value Government records;[58] and

5) Serve as the Executive Agent for the Controlled Unclassified Information (CUI) program.[59]

g. Office of Personnel Management

The Administrator of the Office of Personnel Management shall:[60]

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

2) Identify training needs of the Federal Government workforce related to IT and information resources management;

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

4) Assess the training of employees in IT disciplines to address information resources management needs.

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.

8. Oversight

The Director of OMB shall use IT planning reviews, fiscal budget reviews, information collection 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.

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

[59] Pursuant to Executive Order 13556, *Controlled Unclassified Information*.

[60] Pursuant to the E-Government Act of 2002 (44 U.S.C. § 3501 note; Pub. L. 107–347, § 209(b)(1)).

9. Authority

OMB issues this Circular pursuant to the Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (40 U.S.C. § 11101-11704); E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36); Federal Information Security Modernization Act of 2014 (44 U.S.C. Chapter 35, Subchapter II); Federal Information Technology Acquisition Reform Act (FITARA) (Pub. L. 113-291)[61]; Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); Privacy Act of 1974, as amended (5 U.S.C. § 552a); Digital Accountability and Transparency Act of 2014 (Pub. L. 113-101); Electronic Signatures in Global and National Commerce Act (E-Sign) (15 U.S.C. Chapter 96); Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504); Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRA Modernization Act) of 2010 (5 U.S.C. § 306 and 31 U.S.C. §§ 1115 et seq.); Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); Budget and Accounting Procedures Act of 1950, as amended (31 U.S.C. Chapter 11); Chief Financial Officers Act (31 U.S.C. § 3512 et seq.); and Executive Order 13719, Establishment of the Federal Privacy Council (2016).

10. Definitions

a. The following definitions are applicable within this policy:

1) 'Accessibility' means information technology products or services that are in full compliance with the standards of section 508 of the Rehabilitation Act of 1973.[62]

2) '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.

3) '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.

4) 'Agency Strategic Plan' means a plan that provides general and long-term goals that the agency aims to achieve, the actions the agency will take to realize those goals, the

[61] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. 113-291. Further references in the text that refer to "FITARA" refer to these sections.

[62] The United States Architectural and Transportation Barriers Compliance Board's (Access Board) Information and Communication Technology Standards and Guidelines for information and communications technologies (ICT), known as the Section 508 Standards. The 508 standards apply to ICT developed, procured, maintained, or used by Federal agencies covered by section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d), as amended. Accessibility also refers to the 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*.).

strategies planned, how the agency will deal with challenges and risks that may hinder achieving results, and the approaches it will use to monitor its progress.[63]

5) 'Agile Development' means a development methodology that uses an iterative approach to deliver solutions incrementally through close collaboration and frequent reassessment.

6) 'Authorization to Operate' 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.

7) 'Authorization boundary' means all components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.[64]

8) 'Authorization package' means the essential information that an authorizing official uses to determine whether 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 information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

9) 'Authorizing 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.

10) 'Binding Operational Directive' means a compulsory direction from the Department of Homeland Security to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director (44 U.S.C. § 3552).

11) 'Business Continuity Plan' means a plan that focuses on sustaining an organization's mission or business processes during and after a disruption, and may be written for

[63] For additional information, refer to the Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRA Modernization Act) 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*.

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

mission or business processes within a single business unit or may address the entire organization's processes.[65]

12) 'Chief Information Officer' means the senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT 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; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.

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

14) 'Common control' means a security or privacy control that is inherited by multiple information systems or programs.[66]

15) 'Controlled Unclassified Information' means information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

16) '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)).

17) 'Cybersecurity' means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

18) 'Dissemination' means the government-initiated distribution of information to a nongovernment entity, including the public. The term 'dissemination,' as used within this Circular, does not include distribution limited to Federal 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).

19) '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

[65] The Federal Information Security Modernization Act (44 U.S.C. § 3554(b))) 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.

[66] A control is inherited by an information system when the control is selected for the system but the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system.

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).

20) 'Environment of operation' means the physical surroundings in which an information system processes, stores, and transmits information.

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

22) 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

23) 'Federal information system' means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

24) 'Federal Privacy Council' means the Council established by Executive Order 13719.[67]

25) '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).

26) 'Hybrid control' means a security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control.

27) 'Incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (44 U.S.C. § 3552).

28) '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.

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

30) '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.

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

32) 'Information resources' means information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. § 3502).

[67] Executive Order 13719, *Establishment of the Federal Privacy Council* (2016).

33) ‘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).

34) ‘Information Resource Management 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 (44 U.S.C. 3506 (b)(2)).

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

    a) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

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

    c) Availability, which means ensuring timely and reliable access to and use of information (44 U.S.C. § 3552).

36) ‘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.

37) ‘Information security continuous monitoring’ means maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.[68]

38) ‘Information security continuous monitoring program’ means the compendium of methods, tools, and techniques necessary to implement the agency information continuous monitoring strategy in a way that is sufficient to inform risk-based decisions and maintain operations within established risk tolerances. The program includes determining monitoring metrics, establishing monitoring frequencies, and developing a monitoring architecture.

39) ‘Information security continuous monitoring strategy’ means a comprehensive plan to address monitoring requirements and activities at each organizational tier (organization, mission or business process, and information system).

40) ‘Information system security plan’ means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.[69]

[68] 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.

[69] The information system security plan and the privacy plan may be integrated into one consolidated document.

41) ‘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.

42) ‘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).

43) ‘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.)

44) ‘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 essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

45) ‘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 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).

46) ‘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 shall 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.

47) ‘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 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.[70]

48) '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 that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants that establish or support information technology not operated directly by the Federal Government.

49) 'Initial authorization' means the initial risk determination and risk acceptance decision based on a zero-base review[71] of the information system conducted prior to its entering the operations or 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 an information system security plan or in a privacy plan and implemented within an information system or the environment in which the system operates.

50) 'Interagency agreement' means, for the purposes of this document, a written agreement entered into between two or more 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(s) (the requesting agency), including assisted acquisitions as described in OMB Memorandum: *Improving the Management and Use of Interagency Acquisitions* and other cases described in FAR Part 17.

51) 'Major information system' means a system that is part of an investment that requires special management attention as defined in OMB guidance[72] 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.[73]

52) '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

[70] See the Clinger Cohen Act of 1996 (40 U.S.C. § 11302) for statutory requirements.

[71] A zero-base review of an information system is the first complete security assessment performed in order to provide the authorizing official with a comprehensive set of security-related information to facilitate making an appropriate risk determination.

[72] For example, an information system requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

[73] All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system.

defined in the OMB Circular A-11, *Capital Programming Guide*, consisting of information resources.

53) '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).

54) '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 or 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 the mission or business risk of continued system operation is acceptable.

55) 'Open data' means publicly available data that are made available consistent with relevant privacy, confidentiality, security, and other valid access, use, and dissemination restrictions, and are structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are consistent with principles, explained in OMB guidance, of such data being public, accessible, machine-readable, described, reusable, complete, timely, and managed post-release.

56) 'Overlay' means a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. (See "tailoring" definition.)

57) 'Personally identifiable information' 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.

58) 'Privacy continuous monitoring' means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

59) 'Privacy continuous monitoring program' means an agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to

information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.

60) 'Privacy continuous monitoring strategy' means a formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

61) 'Privacy control' means the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

62) 'Privacy control assessment' means the assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.

63) 'Privacy impact assessment' 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 creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

64) 'Privacy program plan' means a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

65) 'Privacy plan' means a formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.[74]

66) 'Program management control' means, in the context of information security and privacy, a control that is generally implemented at the agency level, independent of any

[74] The privacy plan and the information system security plan may be integrated into one consolidated document.

particular information system, and essential for managing information security or privacy programs.

67) 'Provisioned IT Service' means an information technology service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency.

68) '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).

69) '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 risk above the previously agreed-upon agency risk tolerance.

70) '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).

71) '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)).

72) '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.

73) '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.[75]

74) 'Risk management' means the program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

75) 'Risk management strategy' means the description of how an agency intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk

[75] Risk can include both information security and privacy risks.

perceptions that organizations routinely use in making both investment and operational decisions.

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

77) ‘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.

78) ‘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.

79) ‘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.

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

81) ‘Senior Agency Official for Privacy’ means the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency’s development and evaluation of legislative, regulatory, and other policy proposals.

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

83) ‘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.

84) ‘Supply chain risk’ means risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

85) ‘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.

86) ‘System-specific control’ means a security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.

87) ‘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.

88) ‘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.)

89) ‘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.

90) ‘Trustworthy information system’ means an information 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.

b. Terms that are not specifically defined in this section are assumed to have standard dictionary meanings, or are defined in other OMB policy.

11. Inquiries

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 A-130
Responsibilities for Protecting and Managing Federal Information Resources

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 Federal information resources. Personnel at all levels of the Federal Government must understand how to manage information security and protect 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 and manage risks. 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 can best be 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 appropriate architectures and the application of systems 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 and privacy requirements and associated controls that are mandatory, agencies are

required to employ risk-based approaches and decision making to ensure that security and privacy capabilities are sufficient to protect agency assets, operations, and individuals. Such risk-based approaches involve framing, assessing, responding to, and monitoring security and privacy 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, use, processing, storage, maintenance, dissemination, disclosure, 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, that information security and privacy programs are appropriately managed, 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 A-123, *Management's Responsibility for Enterprise Risk Management and Internal Controls*. This Appendix also establishes requirements for Federal agency privacy programs, assigns responsibilities for privacy program management, and describes how agencies should take a coordinated approach to implementing information security and privacy controls. Additionally, this Appendix incorporates requirements of statute, such as FISMA (44 U.S.C. Chapter 35), the E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36), the Paperwork Reduction Act (44 U.S.C. Chapter 35), and the Privacy Act of 1974, and responsibilities assigned in executive orders and Presidential directives.

3. General Requirements

a. Agencies shall implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security and privacy risk on an ongoing basis across the three organizational tiers (i.e., organization level, mission or business process level, and information system level).[76]

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;

[76] NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, provides additional information on risk management processes and strategies. See also Section 5.b of this Appendix.

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

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

4) Cost-effectively manage information security and privacy risks, which includes reducing such risks to an acceptable level;

5) 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;

6) Implement security and privacy controls, and verify that they are operating as intended, and continuously monitored and assessed; put procedures in place so 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;

7) Employ systems security engineering principles, concepts, and techniques during the life cycle of information systems to facilitate the development, deployment, operation, and sustainment of trustworthy and adequately secure systems;

8) 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 life cycle;

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

10) Ensure that, in a timely manner, agency CIOs and SAOPs 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;[77] and

11) Ensure ongoing collaboration between the senior agency information security officer and the SAOP to ensure coordination of security and privacy activities.

c. Agencies that share PII shall require, as appropriate, other agencies and entities with which they share PII to maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by the agency sharing the PII.

d. Agencies that share PII with other agencies or entities shall impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance,

[77] Until such information systems or components are appropriately dispositioned, agencies are expected to immediately implement interim remediation measures such as limiting access or connectivity.

dissemination, disclosure, and disposal of the PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.

e. Agencies shall protect Controlled Unclassified Information (CUI) and shall apply NIST FIPS and NIST (800-series) SPs, as appropriate. This includes limiting 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.

f. Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and develop and maintain effective information security and privacy programs. This includes using privacy impact assessments and other tools to manage privacy risks.

g. Agencies shall implement policies issued by OMB, as well as requirements issued by the Department of Commerce, DHS, GSA, and OPM. This includes applying the standards and guidelines contained in NIST FIPS, NIST (800-series) SPs, and, where appropriate and directed by OMB, NISTIRs.

4. Specific Requirements[78]

a. Security Categorization

Agencies shall:

1) Identify authorization boundaries for information systems in accordance with NIST SPs 800-18 and 800-37; and

2) Categorize information and information systems, in accordance with FIPS Publication 199 and NIST SP 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 identified and included in IT investment capital plans and budgetary requests;

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;

[78] 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 NIST standards and guidelines.

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 that risk is addressed and information systems achieve the necessary levels of trustworthiness, protection, and resilience.

c. Plans, Controls, and Assessments

Agencies shall:

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

2) Develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program;

3) Employ a system life cycle process that incorporates the principles, concepts, methods, and techniques of systems security engineering to ensure the development of trustworthy and resilient information systems;

4) Develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems;

5) Employ a process to select and implement security controls for information systems and the environments in which those systems operate[79] that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST SP 800-53, tailored as appropriate;[80]

6) Employ a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*;

7) Implement information system security using sound systems security engineering principles, concepts, methods, practices, and techniques;

8) Develop and maintain security plans for information systems to document which security controls have been selected and how those controls have been implemented;

[79] The environment of operation includes the physical surroundings in which an information system processes, stores, and transmits information. Agencies should take the environment into account when selecting, implementing, documenting, and assessing security controls.

[80] Agencies must conduct tailoring activities in accordance with OMB policy.

9) Develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls;

10) 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 Government-wide and accepted across all Executive Branch agencies;

11) Adhere to Government-wide requirements in the deployment and use of identity credentials used by employees and contractors accessing Federal facilities;[81]

12) Designate common controls in order to provide cost-effective security and privacy capabilities that can be inherited by multiple agency information systems or programs;[82]

13) Conduct and document assessments of all selected and implemented security and privacy controls to determine whether security and privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable requirements and to manage security and privacy risks;

14) Conduct and document security and privacy control assessments prior to the operation of an information system, 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;

15) Use agency plans of action and milestones (POA&Ms), and make available or provide access to OMB, DHS, inspectors general, and the U.S. 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

16) 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.

---

[81] NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, provides additional information on the use of PIV Credentials, the Government-wide standard identity credential, in physical access control systems. Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.

[82] When common controls protect multiple agency information systems of differing impact levels, the controls shall be implemented at 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 or business processes, or separating the higher impact system into its own domain where it can be afforded appropriate levels of protection).

d. Authorization to Operate 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;[83]

2) Complete an initial authorization to operate for each information system and all agency-designated common controls based on a determination of, and explicit acceptance of, the risk to agency operations and assets, individuals, other organizations, and the Nation, and prior to operational status;

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;

5) Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers;[84]

6) Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls; significant changes to information systems; 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 are effectively monitored on an ongoing basis, as determined by the agency's ISCM program;[85]

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 and trend analysis at all 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 organizational missions or business functions, Federal statutes, directives, instructions, regulations, policies, standards and guidelines;

[83] Common controls are authorized for operation in the same manner as system-specific controls.

[84] NIST SP 800-39, *Managing Information Security Risk*, defines three risk management tiers for managing information security risk within organizations. These include an organization or governance tier, mission or business process tier, and information system tier.

[85] For greater efficiency, the ISCM and PCM strategies may be consolidated into a single unified continuous monitoring strategy. Similarly, the ISCM and PCM programs may also be consolidated into a single unified continuous monitoring program.

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

f) Ensures knowledge and control of changes to information systems that have potential to affect security;

g) Maintains awareness of threats and vulnerabilities that have the potential to affect security, including the mitigation of those threats and vulnerabilities;

9) Develop and maintain a PCM strategy, a formal document that:

a) Catalogs the available privacy controls implemented at the agency across the agency risk management tiers; and

b) Ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks;

10) Establish and maintain an agency-wide PCM program that implements the agency's PCM strategy and:

a) Conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;

b) Identifies assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;

c) Maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; and

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

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

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

e. Privacy Controls for Federal Information Systems and Programs

The SAOP has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to manage privacy risks, develop and evaluate privacy policy, and ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. The SAOP shall:

1) Develop and maintain a privacy program plan that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the

program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks;

2) Develop and maintain a PCM strategy and PCM program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;

3) Conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;

4) Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;

5) Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency;

6) 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, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

7) Review and approve, in accordance with NIST FIPS Publication 199 and NIST SP 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;[86]

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

9) Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions; and

10) Coordinate with the CIO, the senior agency information security officer, and other agency officials in implementation of these requirements.

f. Incident Detection, Response, and Recovery

It is essential that agencies react appropriately to incidents after employing a risk-based approach to selecting and implementing their security and privacy controls for their information and information systems.

[86] The categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII will depend on the sensitivity level of the PII, the privacy risks, and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. Agencies should generally categorize information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII at the moderate or high confidentiality impact level. See Appendix II for additional information regarding the sensitivity level of PII.

Agencies shall:[87]

1) Develop and implement incident management policies and procedures, in accordance with OMB policies and NIST guidelines that address incident detection, response, and recovery. This includes developing and implementing appropriate activities to identify the occurrence of an incident; developing and implementing appropriate activities to take action regarding a detected 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 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 or as required by OMB or DHS;
6) Ensure that processes are in place to verify corrective actions;
7) Maintain formal incident response capabilities and mechanisms to include notification to affected individuals and adequate training and awareness for employees and contractors on how to report and respond to incidents;
8) Implement formal incident management 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;
9) Report incidents to OMB, DHS, the CIO, the SAOP, their respective inspectors general and general counsel, law enforcement, and Congress in accordance with procedures issued by OMB; and
10) Provide reports on incidents as required by FISMA, OMB policy, DHS binding operational directives, Federal information security incident center guidelines, NIST guidelines, and agency procedures.

[87] Pursuant to FISMA (44 U.S.C. Chapter 35).

g. Contingency Planning[88]

Agencies shall:

1) Develop and test contingency plans[89] for information systems that:
   a) Identify essential missions and business functions and associated contingency requirements;
   b) Provide recovery objectives, restoration priorities, and metrics;
   c) Address contingency roles and responsibilities; and
   d) Address maintaining essential missions, functions, and services despite a disruption, compromise, or failure of information systems.
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 policies, standards, and guidelines issued by OMB, NIST, and OPM;
3) Apprise agency employees about available security and privacy resources, such as products, techniques, or expertise;
4) Provide foundational as well as more advanced levels of security and privacy 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 employees and contractors with assigned security and privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties;

[88] 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. 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.

[89] Testing of contingency plans must be consistent with the assessment procedures in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. In addition, Homeland Security Presidential Directive 20, *National Continuity Directive*, requires the establishment and maintenance of an effective national continuity capability. Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, provides direction for the further development of continuity plans and programs.

6) Establish rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and

7) Ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.

i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems[90]

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, 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 a 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;

4) Isolate sensitive 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 or 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 or background investigation is conducted prior to granting access;

6) Protect administrator, user, and system documentation related to the design, development, testing, 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 (that ordinary users are not authorized to perform) 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;[91]

---

[90] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides information on additional security safeguarding measures.

[91] 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 SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

9) Implement and maintain current updates and patches for all software and firmware components of information systems;[92]

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,[93] 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;[94]

12) Develop and implement processes to support use of digital signatures for employees and contractors;

13) Ensure that all public key infrastructure (PKI) certificates used by an agency and issued in accordance with Federal PKI policy validate to the Federal PKI trust anchor when being used for user signing, encrypting purposes, authentication and authorization;[95]

14) 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, in consultation with the SAOP (as appropriate);[96]

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

16) Ensure that only individuals or processes acting on behalf of individuals with legitimate need for access have the ability to decrypt sensitive information;

17) Implement data-level protection and access controls to ensure the security of and access to Federal information; and

---

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

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

[94] Pursuant to Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, NIST FIPS 201 describes the initial Government-wide identity management standard for employees and contractors as a smartcard form factor (the PIV card). With the emergence of a newer generation of computing devices and in particular with mobile devices, the use of PIV cards has evolved technically to include other form factors that can be deployed directly with mobile devices as specified in NIST SP 800-157. The PIV credential associated with this alternative is called a Derived PIV Credential. Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63. Issuing a Derived PIV credential to PIV card holders does not require repeating identity proofing and vetting processes. The user simply proves possession and control of a valid PIV Card to receive a Derived PIV Credential.

[95] The trust anchor refers to the Federal PKI root certificate operated by the Federal PKI Management Authority. This root certificate is the trusted source of all Federal PKI certificates. For additional information, refer to https://www.idmanagement.gov and Federal PKI policy.

[96] The encryption of organizational information when in transit over a network and when at rest in storage devices ensures that such information is persistently protected and promotes a defense-in-depth security strategy.

18) 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.[97]

j. Non-Federal Entities

Agencies shall:

1) Ensure that terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, incorporate security and privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information;[98]

2) 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 information 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) Ensuring that these information systems are included in the agency's inventory of information systems;

   d) Ensuring that the interface characteristics, security requirements, and the nature of the information communicated is documented for each interface between these systems and agency-owned or operated information systems;

   e) Ensuring that procedures are in place for incident response for these information systems including timelines for notification of affected individuals and reporting to OMB, DHS, and other entities as required in OMB guidance;

   f) Requiring agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between these information systems and agency-owned or operated information systems; and

3) Consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function;

4) 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,

[97] 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.

[98] For additional information and associated requirements pertaining to IT acquisitions, refer to the FAR.

local, tribal, and territorial governments, are consistent to the greatest extent possible; and

5) Ensure that terms and conditions of contracts and other agreements include sufficient provisions for Federal Government notification and access, as well as cooperation with agency personnel and Inspectors General.

k. Mitigation of Deficiencies and Issuance of Status Reports

Agencies shall correct deficiencies that are identified through information security and privacy assessments, ISCM and PCM programs, or internal or external audits and reviews, to include OMB reviews. OMB Circular A-123, *Management's Responsibility for Internal Controls*, 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.

l. Reporting

Agencies shall provide performance metrics information and FISMA reports in accordance with processes established by OMB and DHS pursuant to FISMA.

m. Independent Evaluations

Pursuant to FISMA, agencies shall:[99]

1) Perform an independent evaluation of the information security programs and practices to determine the effectiveness of such programs and practices, as further described in statute.[100] The evaluation may include an evaluation of their privacy program and practices, as appropriate. Each evaluation shall include:

a) Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's Federal information systems;[101]

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.

[99] FISMA (44 U.S.C. § 3555).

[100] FISMA (44 U.S.C. § 3555).

[101] Agencies have flexibility in implementing the baseline controls in SP 800-53; however, agencies are required to justify, in their security plans or overlays, any tailoring actions.

5. Discussion of the Major Provisions in the Appendix

This section provides additional information regarding the requirements in this appendix.

a. 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[102] to ensure that the set of security controls in the information system 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 or business protection needs of the agency.

For non-national security programs and information systems, agencies must apply NIST guidelines unless otherwise stated by OMB. FIPS are mandatory.[103] 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 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.

b. Risk Management Strategy

Managing risk is a complex, multifaceted activity that requires the involvement of the entire agency—from senior leaders and executives providing the strategic vision and top-level goals and objectives for the agency; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the agency's missions or business functions. Risk management is a comprehensive process that requires agencies to establish the context in which risk-based decisions are made; assess risk; respond to risk once determined; and monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of agencies. Risk management is conducted as an agency-wide activity to ensure that risk-based decision-making is integrated into every aspect of the agency's planning and operations.

[102] Agencies must conduct tailoring activities in accordance with OMB policy.

[103] Pursuant to FISMA (44 U.S.C. Chapter 35).

A key aspect of the risk management process is the development of the risk management strategy. The risk management strategy describes how an agency intends to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that agencies routinely use in making both investment and operational decisions. Establishing a realistic and credible risk management strategy requires that agencies identify their risk assumptions, risk constraints, risk tolerance, and priorities and trade-offs. The risk management strategy also includes any strategic-level decisions by senior leaders and executives regarding the management of risk to agency operations and assets, individuals, other organizations, and the Nation. The risk management strategy guides and informs the use and application of the Risk Management Framework.

c. Risk Management Framework

The Risk Management Framework, as described in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The Risk Management Framework requires agencies to categorize each information system and the information processed, stored, and transmitted by each system based on a mission or 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, as described in NIST SP 800-53. After implementing the security controls, agencies assess the controls using appropriate assessment methods as described in NIST SP 800-53A to determine whether 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, as described in NIST SP 800-137. 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 Risk Management Framework ensures that managing information system-related risks is consistent with the agency's mission or business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function[104] as discussed in NIST SP 800-39. It also ensures that the requisite security and privacy requirements and controls are integrated into

[104] The *risk executive function* is an individual or group within an agency that helps to ensure that: (i) risk-related considerations for individual information systems, to include the authorization to operate 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 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.

the agency's enterprise architecture and system development life cycle processes. Finally, the Risk Management Framework supports consistent, well-informed, and ongoing authorization decisions, transparency of risk management information, reciprocity, and information sharing.

d. 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 satisfies the minimum security requirements set forth in FIPS Publication 200. The security controls must include one of the three security control baselines from NIST SP 800-53 that are associated with the designated categorization (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 include a justification, in their information system security plans or overlays, 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 for specific types of information or communities of interest (e.g., all web-based applications, all health care-related systems) as part of the security control selection process. Overlays provide a specification of security 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 information systems.

All selected security controls must be documented in an information system security plan and implemented. Agencies can use the priority code designations associated with each security control in NIST SP 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, shall focus on the effectiveness of the security controls selected and implemented (as documented in agency information system 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.

e. 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. However, 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. As the transition to ongoing authorization progresses and agency ISCM programs mature, agencies must ensure that assessment frequencies are determined in accordance with NIST SP 800-137.

Security and privacy control assessments shall ensure that security and privacy controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying security and privacy requirements. The risk may change over time based on changes in the threat, agency missions or 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 incident is paramount. The type, rigor, and frequency of control assessments, which is established by the agency's risk tolerance and risk management strategy, shall be commensurate with the level of awareness necessary for effectively determining information security and privacy risk. 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.

f. 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 be responsible for the mission or business operations supported by the system. Through the authorization process, authorizing officials are responsible and accountable for the risks associated with information system operations. Because information security is closely related to the privacy protections required for PII, authorizing officials are also responsible and accountable for the privacy 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 privacy, agencies must consider input and recommendations submitted by the SAOP in the authorization decision. Additionally, the SAOP has responsibility for reviewing the authorization package for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, to ensure that privacy risks are managed 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.[105]

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 6j, *Joint and Leveraged Authorizations*). Agencies can, at their discretion, include the CIO or the SAOP as a co-authorizing official with a senior agency official who has budgetary oversight for an information system or is responsible for the mission or line of business supported by the system being authorized for operation. Regardless of the approach used, only Federal Government personnel may serve as an authorizing official.

g. 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 an information system to operate shall 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, shall be made by the appropriate authorizing official. Since the information system 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 shall form the basis for the authorization, supplemented by more specific information as needed.

In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the continuous monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls and explicitly accepting the risk. If the new authorizing official is not willing to accept the previous authorization results (including the identified risk), a reauthorization action may need to be initiated or the new authorizing

[105] 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.

official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date.

h. Ongoing Authorization

Ongoing authorization[106] 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 or business requirements. In order to implement an ongoing authorization process, and move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process for information systems and controls, two conditions must be met by agencies. First, the information system or common controls must have been granted an initial authorization to operate by the designated authorizing official. Second, ISCM and PCM programs must be in place to monitor all implemented security and privacy controls with the appropriate degree of rigor[107] and at the appropriate frequencies in accordance with applicable ISCM and PCM strategies, OMB guidance, and NIST guidelines. Ongoing authorization can either be a time-driven or event-driven 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 all applicable security and privacy requirements have been satisfied and the mission or business risk is acceptable. Effective ongoing authorization requires robust ISCM and PCM strategies and effective operational ISCM and PCM programs.

Agencies must define and implement a process to designate information systems or common controls that have satisfied the two conditions noted in the previous paragraph and are to be transitioned to ongoing authorization. The process includes the means for the authorizing official to formally acknowledge that the information system or common controls are being managed under an ongoing authorization process and accept the responsibility for ensuring that 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.

i. 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 or 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 or significant

[106] 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*, http://csrc.nist.gov/publications.

[107] The term rigor is used in conjunction with security control assessments and monitoring. It is typically associated with the application of assessment methods described in NIST SP 800-53A, and in particular, the attribute of depth which addresses the formality and comprehensiveness of the assessment or monitoring activity.

change that increases information security or privacy risk above the previously agreed-upon agency risk tolerance. A significant change is defined as a change that is likely to affect the security or privacy 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 or significant change 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.

j. Joint and Leveraged Authorizations

Agencies are encouraged to use joint and leveraged authorizations whenever practicable.[108] 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 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 SP 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 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 or services provided by the system).[109] 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 creates, collects, uses, processes, stores,

[108] NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, provides guidance on joint and leveraged security authorizations.

[109] Agencies using leveraged authorization information from other (owning) agencies shall ensure that such information is included as part of their own Risk Management Framework to provide the appropriate context for managing risk within the leveraging organizations.

maintains, disseminates, discloses, or disposes of PII, leveraging agencies must consult their SAOP. The SAOP may determine that additional measures are required to manage privacy risks prior to leveraging the authorization.

k. Continuous Monitoring

Agencies must develop ISCM and PCM strategies 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 addresses all information systems, or continuous monitoring strategies that address each agency information system individually. The ISCM and PCM strategies must document all available 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 appropriate agency authorizing official and SAOP, respectively, must also include all common controls inherited by agency information systems.

l. Critical Infrastructure

Agencies that operate information systems that are part of the critical infrastructure must conduct a 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 applicable privacy requirements and manage privacy risks. This includes the continuous monitoring of deployed security and privacy controls in information systems designated as critical infrastructure 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.

m. 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 and integrity 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, in consultation with the SAOP (as appropriate). Only FIPS-validated cryptography is approved for use in Federal information systems covered by this policy.

n. 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 or 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 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. For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures.

o. Identity Assurance

Identity assurance is an essential element of an effective information security program. To streamline the process of citizens, businesses, and other partners[110] 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.[111] 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.[112] 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.[113]

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

[111] Pursuant to Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, agencies making personal data accessible to citizens through digital applications shall require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.

[112] NIST SP 800-63, *Electronic Authentication Guidance*, provides additional guidance on identity assurance.

[113] The requirements in this paragraph focus on citizens, businesses, and other partners that interact with the Federal Government. For Federal employees and contractors, with long-term access to Federal facilities and information systems, agencies are required to follow Personal Identity Verification requirements in accordance with OMB policy and NIST standards and guidelines.

p. Unsupported Information System Components

Unsupported information system components (e.g., when developers or 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 or 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.

q. 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 is responsible for providing 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.

r. 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 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 IT that the Clinger-Cohen Act of 1996 (40 U.S.C. § 11101(6)) 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.

s. Controlled Unclassified Information

The Controlled Unclassified Information program, established by Executive Order 13556, is a system that standardizes and simplifies the way the agencies handle unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. The program emphasizes the openness and uniformity of Government-wide practices. Its purpose is to address inefficient and confusing processes that have historically led to inconsistent marking and safeguarding as well as restrictive dissemination policies.

6. Other Requirements

Agencies must adhere to all other applicable information requirements such as privacy requirements in accordance with the Privacy Act of 1974, and its implementing OMB guidance; confidentiality protection requirements in accordance with the Confidentiality Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) and its implementing OMB guidance; applicable requirements of statutes, and regulations pertaining to management of Federal records; and other relevant statutes, executive orders, Presidential directives, and policies.

7. References[114]

a. The following references are used within this policy:

1) Executive Order 13556, *Controlled Unclassified Information*, November 2010.

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

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

4) Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.

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

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

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

[114] Statutes, executive orders, and Presidential directives relevant to this appendix are listed in the Authorities section of the main body. Additionally, OMB policy documents can be located at https://www.whitehouse.gov/omb/circulars_default and https://www.whitehouse.gov/omb/memoranda_default.

8) National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

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

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

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

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

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

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

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

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

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

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

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

20) National Institute of Standards and Technology Special Publication 800-63, *Electronic Authentication Guideline*.

21) National Institute of Standards and Technology Special Publication 800-73, *Interfaces for Personal Identity Verification.*

22) National Institute of Standards and Technology Special Publication 800-76, *Biometric Specifications for Personal Identity Verification.*

23) National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

24) National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).*

25) National Institute of Standards and Technology Special Publication 800-116, *Guidelines for the Use of PIV Credentials in Physical Access Control Systems (PACS).*

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

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

28) National Institute of Standards and Technology Special Publication 800-157, *Guidelines for Derived Personal Identity Verification Credentials*.

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

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

31) National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.*

32) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*.

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

b. References in this section without specific publication dates or revision numbers refer to the most recent updates to those publications.

Appendix II to OMB Circular A-130
Responsibilities for Managing 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) and summarizes the key privacy requirements included in other sections of this Circular. The requirements included in this Appendix apply to PII in any form or medium, including paper and electronic media. Although all of the requirements referenced in this Appendix concern the management of PII, some of the requirements are not solely the responsibility of agencies' privacy programs. The inclusion of shared requirements in this Appendix is not intended to suggest that agencies' privacy programs are solely or primarily responsible for meeting such requirements; however, agencies' privacy programs shall play a key role in meeting requirements that involve PII. This Appendix does not provide a comprehensive account of all the statutory and policy requirements associated with managing PII and protecting privacy. Agencies shall consult law, regulation, and policy, including OMB guidance, to understand all applicable requirements.

The main body of this Circular establishes general policies for Federal agencies managing information resources. Appendix I to this Circular establishes requirements for information security and privacy programs and provides guidance on how agencies should take a coordinated approach when managing Federal information resources. This Appendix and Appendix I are companion documents; it is important to review the appendices together in order to understand the coordination between privacy and security. As noted in the citations, all of the requirements summarized in the tables in this Appendix come from the main body or Appendix I to this Circular.

Previous versions of Circular A-130 included information about the reporting and publication requirements of the Privacy Act of 1974 ("Privacy Act") and additional OMB guidance. This information is being revised and will be reissued in OMB Circular A-108.[115] This Appendix does not extend or interpret the Privacy Act, including agency requirements under the Privacy Act.

2. Introduction

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of PII to carry out missions mandated by Federal statute. The term PII, as defined in 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, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize

[115] Agencies shall continue to apply the requirements in Appendix I of the 2000 version of Circular A-130 regarding review, reporting, and publication pertaining to the Privacy Act until OMB issues a revised version of those requirements in OMB Circular A-108.

that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

Once the agency determines that an information system contains PII, the agency shall then consider the privacy risks and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. When considering privacy risks, the agency shall consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. In particular, the agency shall 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 will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information. In addition, when determining the privacy and associated risks, the agency shall also consider the volume of PII. A higher volume of PII about a single individual or multiple individuals may pose increased privacy or associated risks.

3. Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that agencies should use when evaluating information 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 have informed Federal statute and the laws of many U.S. states and foreign nations, and have been 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.[116]

b. *Accountability*. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to

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

PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

c. *Authority*. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.[117]

d. *Minimization*. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose 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.[118]

e. *Quality and Integrity*. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose 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 process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

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

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, dissemination, or disclosure.

i. *Transparency*. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.[119]

4. Senior Agency Official for Privacy

Agencies are required to designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks. The SAOP shall have a central policy-making role and shall ensure that the agency considers the privacy impact of all agency actions and policies that involve PII. The SAOP's review of privacy risks should begin at the earliest planning and

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

[118] In some versions of the FIPPs, the "minimization" principle is referred to under a different name, such as "collection limitation."

[119] In some versions of the FIPPs, the "transparency" principle is referred to under a different name, such as "openness."

development stages of agency actions and policies that involve PII, and should continue throughout the life cycle of the information.

The SAOP shall ensure that the agency complies with applicable privacy requirements in statute, regulation, and policy.

5. Agency Privacy Program

In order to manage Federal information resources that involve PII, agencies shall develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. Among other things, where PII is involved, agencies' privacy programs shall play a key role in information security, records management, strategic planning, budget and acquisition, contractors and third parties, workforce, training, incident response, and implementing the Risk Management Framework. This Appendix does not provide a comprehensive account of all the statutory and policy requirements associated with managing PII and protecting privacy. Agencies shall consult law, regulation, and policy, including OMB guidance, to understand all applicable requirements.

Agencies' privacy programs are led by the SAOP and are responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks. At the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform particular privacy functions that are assigned to the SAOP. Many of the requirements summarized in this Appendix are shared requirements and are not solely the responsibility of agencies' privacy programs. The inclusion of shared requirements in this Appendix is intended to convey that agencies' privacy programs shall be responsible to the extent that the requirements pertain to the management of PII.

a. General Requirements

Agencies shall have comprehensive privacy programs that ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks. The following table summarizes many of the general privacy requirements that are set forth in this Circular. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Establish and maintain a comprehensive privacy program.	Agencies shall establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks.	Main Body § 5(f)(1)(a); Appendix I §§ 3(b), 3(f), 4(e).
Ensure compliance with privacy requirements and manage privacy risks.	Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and use privacy impact assessments and other tools to manage privacy risks. Agencies shall cost-effectively manage privacy risks and reduce such risks to an acceptable level.	Main Body §§ 4(g), 5(e)(1)(d), 5(f)(1)(a); Appendix I § 3(a), 3(b)(4), 3(f), 3(g).

Responsibility	Description	Citation
Monitor Federal law, regulation, and policy for changes.	Agencies shall monitor Federal law, regulation, and policy for changes that affect privacy.	Main Body § 5(f)(1)(c).
Develop and maintain a privacy program plan.	Agencies shall develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program.	Appendix I § 4(c)(2), 4(e)(1).
Designate a Senior Agency Official for Privacy.	The head of each agency shall designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statues, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency.	Main Body § 5(f)(1)(b); Appendix I § 4(e).
Ensure coordination between privacy and other programs.	Agencies shall ensure that the SAOP and the agency's privacy personnel closely coordinate with the agency CIO, senior agency information security officer, and other agency offices and officials, as appropriate.	Main Body §§ 4(h), 5(f)(1)(k); Appendix I §§ 3(b)(11), 4(e)(10).
Ensure that privacy is addressed throughout the life cycle of each information system.	Agencies shall ensure that privacy is addressed throughout the life cycle of each agency information system.	Main Body §§ 4(g), 5(a)(1)(c)(i), 5(b)(4); Appendix I § 4(b)(2).
Incorporate privacy requirements into enterprise architecture.	Agencies shall incorporate Federal privacy requirements into the agency's enterprise architecture to ensure that risk is addressed and information systems achieve the necessary levels of trustworthiness, protection, and resilience.	Appendix I § 4(b)(5).
Comply with the Privacy Act.	Agencies shall comply with the requirements of the Privacy Act and ensure that Privacy Act system of records notices are published, revised, and rescinded, as required.	Main Body § 5(f)(1)(g).
Conduct privacy impact assessments.	Agencies shall conduct privacy impact assessments in accordance with the E-Government Act and make the privacy impact assessments available to the public in accordance with OMB policy.	Main Body § 5(f)(1)(i).

Responsibility	Description	Citation
Balance the need for information collection with the privacy risks.	Agencies shall ensure that the design of information collections is consistent with the intended use of the information, and the need for new information is balanced against any privacy risks.	Main Body § 4(i).
Comply with requirements for disclosure and dissemination.	Agencies shall comply with all applicable privacy statutes and policies governing the disclosure or dissemination of information and comply with any other valid access, use, and dissemination restrictions.	Main Body § 5(e)(1)(b)-(d), 5(e)(7)(h).
Maintain and post privacy policies on websites, mobile applications, and other digital services.	Agencies shall maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy.	Main Body § 5(f)(1)(j).
Provide performance metrics and reports.	Agencies shall provide performance metrics information and reports in accordance with processes established by OMB and DHS pursuant to FISMA.	Appendix I § 4(1).

b. Considerations for Managing PII

Agencies' privacy programs shall maintain an inventory of PII, regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. In addition, agencies' privacy programs shall impose, where appropriate, conditions on other agencies and entities to which PII is being disclosed that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII. The following table summarizes the privacy requirements in this Circular that pertain to the general management of PII. While some requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Maintain an inventory of agency information systems that involve PII and regularly review and reduce PII to the minimum necessary.	Agencies shall maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.	Main Body § 5(a)(1)(a)(ii), 5(f)(1)(e).
Eliminate unnecessary collection, maintenance, and use of Social Security numbers.	Agencies shall take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.	Main Body § 5(f)(1)(f).

Responsibility	Description	Citation
Follow approved records retention schedules for records with PII.	Agencies shall ensure that all records with PII are maintained in accordance with applicable records retention or disposition schedules approved by NARA.	Main Body § 5(f)(1)(h).
Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.	Agencies shall limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions.	Main Body § 5(f)(1)(d).
Require entities with which PII is shared to maintain the PII in an information system with a particular categorization level.	Agencies that share PII shall require, as appropriate, other agencies and entities with which they share PII to maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by the agency sharing the PII.	Appendix I § 3(c).
Impose conditions on the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of shared PII through agreements.	Agencies that share PII with other agencies or entities shall impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.	Appendix I § 3(d).

c. Budget and Acquisition

Agencies' privacy programs shall have the resources needed to manage Federal information resources that involve PII. This will require privacy programs to play a key role in the development of the agencies' budget requests, as well as any decisions to acquire or develop information system technologies and services. The following table summarizes the privacy requirements in this Circular that pertain to budget and acquisition activities. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Identify and plan for resources needed for privacy program.	Agencies shall identify and plan for the resources needed to implement privacy programs.	Appendix I § 4(b)(1).
Include privacy requirements in IT solicitations.	Agencies shall include privacy requirements in solicitations for IT and services.	Main body § 5(d)(1)(j).

Responsibility	Description	Citation
Establish a process to evaluate privacy risks for IT investments.	Agencies shall consider privacy when analyzing IT investments, and establish a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including privacy risks, associated with the IT investments.	Main Body § 5(d)(3), 5(d)(4)(b).
Ensure that privacy risks are addressed and costs are included in 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, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Agencies shall ensure that agency budget justification materials, in their initial budget submission to OMB, include a statement affirming that the SAOP has conducted the necessary review.	Main Body § 5(a)(3)(e)(ii), 5(d)(3)(e); Appendix I § 4(b)(2), 4(e)(6).
Ensure that investment plans meet the privacy requirements appropriate for the life cycle stage of the investment.	Agencies shall ensure that investment plans submitted to OMB as part of the budget process meet the privacy requirements appropriate for the life cycle stage of the investment.	Appendix I § 4(b)(4).
Upgrade, replace, or retire unprotected information systems.	Agencies shall plan and budget to upgrade, replace, or retire any information systems for which protections commensurate with risk cannot be effectively implemented.	Appendix I § 4(b)(3).
Ensure that SAOPs are made aware of information systems and components that cannot be protected.	Agencies shall ensure that, in a timely manner, SAOPs 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.	Main Body § 5(a)(1)(c)(ii); Appendix I § 3(b)(10).

d. Contractors and Third Parties

Agencies' privacy programs shall ensure that entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of a Federal agency or that operate or use information systems on behalf of a Federal agency, comply with the privacy requirements in law and OMB policies. The following table summarizes the privacy requirements in this Circular that pertain to contractors and third parties. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Ensure that contracts and other agreements incorporate privacy requirements.	Agencies shall ensure that terms and conditions in contracts, and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information.	Main Body § 5(a)(1)(b)(ii); Appendix I § 4(j)(1).
Maintain agency-wide privacy training for all employees and contractors.	Agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors.	Appendix I § 4(h)(1)-(2), (4)-(7).
Ensure that the Privacy Act applies to contractors where required.	Agencies shall, consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function.	Appendix I § 4(j)(3).
Oversee information systems operated by contractors.	Agencies shall 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.	Appendix I § 4(j)(2).
Implement policies on privacy oversight of contractors.	Agencies shall document and implement policies and procedures for privacy oversight of contractors and other entities, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information.	Appendix I § 4(j)(2)(a).
Ensure implementation of privacy controls for contractor information systems.	Agencies shall ensure that privacy controls of information systems and services used or operated by contractors or other entities on behalf of the agency are effectively implemented and comply with NIST standards and guidelines and agency requirements.	Appendix I § 4(j)(2)(b).
Maintain an inventory of contractor information systems.	Agencies shall ensure that information systems used or operated by contractors or other entities on behalf of the agency are included in the agency's inventory of information systems.	Appendix I § 4(j)(2)(c).
Ensure that incident response procedures are in place for contractor information systems.	Agencies shall ensure that procedures are in place for incident response for information systems used or operated by contractors or other entities on behalf of the agency, including timelines for notification of affected individuals and reporting to OMB, DHS, and other entities as required in OMB guidance.	Appendix I § 4(j)(2)(e).

e. Privacy Impact Assessments

As a general matter, an agency shall 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 create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[120] A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

A PIA is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks. Agencies shall 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 shall work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials.

Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

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 shall be drafted in plain language and shall be posted on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information. Although PIAs are generally required by law, such as by the E-Government Act of 2002, agencies may also develop policies to require PIAs in circumstances where a PIA would not be required by law.

f. Workforce Management

Agencies' privacy programs shall play a key role in workforce management activities. The SAOP shall be involved in assessing the hiring and professional development needs at the agency with respect to privacy. The following table summarizes the privacy requirements in this Circular that pertain to workforce management activities. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of agencies' privacy programs.

[120] *See* 44 U.S.C. § 3501 note; Pub. L. 107–347, § 208(b). Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under this section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

Responsibility	Description	Citation
Ensure that the SAOP is involved in assessing and addressing privacy hiring, training, and professional development needs.	Agencies shall ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.	Main Body § 5(c)(6).
Maintain a workforce planning process.	Agencies shall ensure that the CHCO, CIO, CAO, and SAOP develop and maintain a current workforce planning process to ensure that the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.	Main Body § 5(c)(1).
Develop a set of privacy competency requirements.	Agencies shall ensure that the CHCO, CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers and information security, privacy, and IT leadership positions.	Main Body § 5(c)(1).
Ensure that the workforce has the appropriate knowledge and skill.	Agencies shall ensure that the workforce, which supports the acquisition, management, maintenance, and use of information resources, has the appropriate knowledge and skill.	Main Body § 5(c)(2).
Take advantage of flexible hiring authorities for specialized positions.	Agencies shall ensure that the CIO, CHCO, SAOP, and other hiring managers take advantage of flexible hiring authorities for specialized positions, as established by OPM.	Main Body § 5(c)(7).

g. Training and Accountability

Agencies' privacy programs shall develop, maintain, and provide agency-wide privacy awareness and training programs for all employees and contractors. In addition, the privacy program shall establish rules of behavior for employees and contractors with access to PII and hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks. The following table summarizes the privacy requirements in this Circular that pertain to training and accountability activities. Some of the requirements summarized in the table are not solely privacy requirements but may require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Maintain agency-wide privacy training for all employees and contractors.	Agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors.	Appendix I § 4(h)(1).
Ensure that privacy training is consistent with applicable policies.	Agencies shall ensure that the privacy awareness and training programs are consistent with applicable policies, standards, and guidelines issued by OMB, NIST, and OPM.	Appendix I § 4(h)(2).

Responsibility	Description	Citation
Apprise agency employees about available privacy resources.	Agencies shall apprise agency employees about available privacy resources, such as products, techniques, or expertise.	Appendix I § 4(h)(3).
Provide foundational and advanced privacy training.	Agencies shall provide foundational as well as more advanced levels of privacy 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.	Appendix I § 4(h)(4).
Provide role-based privacy training to appropriate employees and contractors.	Agencies shall provide role-based privacy training to employees and contractors with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties.	Appendix I § 4(h)(5).
Hold personnel accountable for complying with privacy requirements and policies.	Agencies shall implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide privacy requirements and policies.	Appendix I § 3(b)(9).
Establish rules of behavior for employees and contractors with access to PII and consequences for violating the rules.	Agencies shall establish rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.	Appendix I § 4(h)(6).
Ensure that employees and contractors read and agree to rules of behavior.	Agencies shall ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.	Appendix I § 4(h)(7).

h. Incident Response

Agencies' privacy programs shall develop and implement incident management and response capabilities. The following table summarizes the privacy requirements in this Circular that pertain to incident response. While some of the requirements summarized in the table are not solely privacy requirements, they may still require the involvement of agencies' privacy programs.

Responsibility	Description	Citation
Maintain formal incident management and response policies and capabilities.	Agencies shall maintain formal incident response capabilities and mechanisms, implement formal incident management policies, and provide adequate training and awareness for employees and contractors on how to report and respond to incidents.	Appendix I § 4(f)(1), (7)-(8).

Responsibility	Description	Citation
Establish roles and responsibilities to ensure oversight and coordination of incident response.	Agencies shall establish clear roles and responsibilities to ensure the oversight and coordination of incident response activities and that incidents are documented, reported, investigated, and handled.	Appendix I § 4(f)(3).
Periodically test incident response procedures.	Agencies shall periodically test incident response procedures to ensure effectiveness of such procedures.	Appendix I § 4(f)(4).
Document incident response lessons learned and update procedures.	Agencies shall document lessons learned for incident response and update procedures annually or as required by OMB or DHS.	Appendix I § 4(f)(5).
Ensure that processes are in place to verify corrective actions.	Agencies shall ensure that processes are in place to verify corrective actions.	Appendix I § 4(f)(6).
Report incidents in accordance with OMB guidance.	Agencies shall report incidents to OMB, DHS, the CIO, the SAOP, their respective inspectors general and general counsel, law enforcement, and Congress in accordance with procedures issued by OMB.	Appendix I § 4(f)(9).
Provide reports on incidents as required.	Agencies shall provide reports on incidents as required by FISMA, OMB policy, DHS binding operational directives, Federal information security incident center guidelines, NIST guidelines, and agency procedures.	Appendix I § 4(f)(10).

i. Risk Management Framework[121]

Agencies' privacy programs have responsibilities under the Risk Management Framework, which is also covered in Appendix I to this Circular. The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle. This Circular requires agencies to use the Risk Management Framework to manage privacy risks beyond those that are typically included under the "confidentiality" objective of the term "information security."[122] While many privacy risks relate to the unauthorized access or disclosure of PII,

[121] Traditionally, the Risk Management Framework was a framework to help agencies address information security and related risks in the authorization process for Federal information systems. As explained in this Appendix, this Circular integrates agencies' privacy programs into the Risk Management Framework process. NIST has published a suite of standards and guidelines that describe how to implement an agency-wide risk management framework. As of the date of this publication, many of the existing NIST standards and guidelines that detail how to implement an agency-wide risk management framework do not fully address the role of privacy and agencies' privacy programs. In the future, NIST may revise or develop standards and guidelines to further clarify how privacy and agencies' privacy programs are integrated into the Risk Management Framework.

[122] The term "information security," as defined in law and in this Circular, includes three objectives: integrity, availability, and confidentiality. The term "confidentiality" means "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information." *See* 44 U.S.C. § 3552.

privacy risks may also result from other activities, including the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation.[123]

The Risk Management Framework has the following steps:

1) *Categorize*. Agencies shall categorize each information system and the information processed, stored, and transmitted by that 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.[124] Each information system is categorized at low, moderate, or high impact according to the criteria in NIST standards and guidelines. The SAOP is responsible for reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

   The categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII will depend on the sensitivity of the PII, the privacy risks, and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. Agencies should generally categorize information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII at the moderate or high confidentiality impact level.

2) *Select*. Agencies shall select security and privacy controls for each information system. A security control is a safeguard or countermeasure prescribed for an information system or an agency to protect the confidentiality, integrity, and availability of the system and its information. Security controls primarily pertain to security but they can also enhance privacy. Agencies shall 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 assessment of security risk and local conditions.[125]

   A privacy control is an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.[126] In order to help agencies satisfy privacy requirements and manage privacy risks, NIST has developed a set of privacy controls, based on the FIPPs, in Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information*

---

[123] Refer to the Fair Information Practice Principles in section 3 of this Appendix.

[124] *See* National Institute of Standards and Technology FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), *available at* http://csrc.nist.gov/publications.

[125] The use of a privacy overlay may assist agencies in effectively selecting and tailoring security controls for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

[126] Privacy risks can include risks beyond those that are typically included under the "confidentiality" prong of the term "information security." Agencies shall use privacy controls to manage all privacy risks associated with PII or an information system, regardless of whether those risks would be considered information security risks.

Systems and Organizations.[127] Agencies are required to use the NIST privacy controls and shall implement a privacy control selection process for information systems. Agencies shall use NIST privacy controls in a manner that is consistent with the agency's authorities, missions, and operational needs.

For privacy controls, the SAOP is responsible for designating which controls the agency will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and essential for managing the agency's privacy program. Program management controls are distinct from common, information system-specific, and hybrid controls because program management controls are independent of any particular information system. Agencies shall document program management controls in their privacy program plan.

The other types of controls – common, information system-specific, and hybrid controls – are necessarily implemented, at least in part, at the information system level. Common controls are controls that are inherited by multiple information systems. When a control is inherited by an information system, the control is selected for the information system but the control is developed, implemented, assessed, authorized, and monitored by programs or officials other than those responsible for the information system. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control.

The determination as to whether a privacy control is a common, hybrid, or information system-specific control is based on context. By assigning privacy controls to an information system as information system-specific, hybrid, or common controls, the agency assigns responsibility and accountability to specific agency programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls. Privacy controls designated by the agency as common controls are, in most cases, managed by an agency program or official other than the information system owner. Moreover, privacy controls designated as information system-specific controls may be the primary responsibility of information system owners and their respective authorizing officials. In all cases, the management of privacy controls shall be subject to the coordination and oversight of the SAOP.

3) *Implement*. Agencies shall implement the security and privacy controls selected for an information system and document how the controls are deployed. Agencies shall develop and maintain security plans and privacy plans for an information system that provide an overview of the security and privacy requirements for the information system and describe the security and privacy controls in place or planned for meeting those requirements. All privacy controls that are selected for an information system shall be

[127] National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013), *available at* http://csrc.nist.gov/publications.

documented in the privacy plan for the information system. The security plan and the privacy plan may be separate or integrated into one consolidated document.

4) *Assess*. Agencies shall assess the security and privacy controls using appropriate methods 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 and privacy requirements for the system and managing risks. The SAOP shall conduct an initial assessment of the privacy controls selected for an information system prior to operation, and shall assess the privacy controls periodically thereafter at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. If a PIA is conducted for the information system, the agency may incorporate the initial assessment of the privacy controls into the PIA process.

5) *Authorize*. Agencies shall authorize an information system prior to operation and periodically thereafter. Authorization of an information system is an explicit acceptance of the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of the security and privacy controls. The determination to authorize an information system shall be made by an agency's authorizing official or officials (which may include the SAOP) and shall be based on a review of the information system authorization package, which includes the security plan, the privacy plan, documented assessments of the security and privacy controls, and any relevant plans of action and milestones.

   Authorizing officials are responsible and accountable for the risks associated with an information system. However, since the SAOP is the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, agencies shall consider recommendations submitted by the SAOP in the decision to authorize an information system. In addition, the SAOP is responsible for reviewing the authorization package for an information system that creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII, to ensure compliance with applicable privacy requirements and manage privacy risks prior to system authorization.

6) *Monitor*. Agencies shall monitor and assess security and privacy controls selected for an information system and shall continue to monitor and assess those controls on an ongoing basis. This includes assessing the effectiveness of the security and privacy controls, documenting changes to the information system, analyzing the security and privacy impact associated with the changes, and reporting the state of the system to appropriate agency officials. The type, rigor, and frequency of control assessments shall be sufficient to account for risks that change over time based on changes in the threat environment, agency missions and business functions, personnel, technology, or environments of operation.

   The ongoing assessment of privacy risks and privacy controls is referred to as privacy continuous monitoring (PCM). The SAOP shall develop and maintain a written PCM strategy that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the controls are effectively monitored

on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

In addition, the SAOP shall establish and maintain a PCM program to implement the PCM strategy. The PCM program is an agency-wide program that is responsible for: maintaining ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitoring changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducting privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and management of privacy risks.

Although the term "privacy continuous monitoring" is new to this Circular, the concept of conducting an ongoing assessment of privacy risks is not new. For many IT systems, agencies are already required to conduct PIAs that involve an analysis of privacy risks throughout the life cycle of the information system and the PII, and the drafting of a living document that is updated whenever changes to the IT or the agency's practices alter the privacy risks associated with the use of the IT.[128] In fact, for IT systems for which a PIA is conducted, agencies may use the PIA as the principal tool to satisfy the requirement to assess the privacy controls for an information system.

The requirement for agencies to implement the Risk Management Framework is described in more detail in Appendix I to this Circular. The following table summarizes the privacy requirements in this Circular that pertain to the Risk Management Framework. While some of the requirements summarized in the table are not exclusively privacy requirements, they may still require the involvement of the agencies' privacy programs.

Responsibility	Description	Citation
Implement a risk management framework.	Agencies shall implement a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.	Appendix I § 3(a), 3(b)(5).
Review and approve the categorization of information systems that involve PII.	The SAOP shall review and approve, in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.	Appendix I § 4(a)(2), 4(e)(7).

[128] Refer to section 5.e of this Appendix for additional information about PIAs.

Responsibility	Description	Citation
Designate program management, common, information system-specific, and hybrid privacy controls.	The SAOP shall designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency. Agencies shall designate common controls in order to provide cost-effective privacy capabilities that can be inherited by multiple agency information systems or programs.	Appendix I § 4(c)(12), 4(e)(5).
Implement a privacy control selection process.	Agencies shall employ a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.	Appendix I § 4(c)(6).
Develop, approve, and maintain privacy plans for information systems.	The SAOP shall review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization. Agencies shall develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.	Appendix I § 4(c)(9), 4(e)(8).
Identify privacy control assessment methodologies and metrics.	The SAOP shall identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks.	Appendix I § 4(e)(4).
Conduct assessments of privacy controls.	The SAOP shall conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. Agencies shall conduct and document privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency privacy continuous monitoring strategy and the agency risk tolerance.	Appendix I §§ 3(b)(6), 4(c)(13)-(14), 4(e)(3).
Correct deficiencies that are identified in information systems.	Agencies shall correct deficiencies that are identified through privacy assessments, the privacy continuous monitoring program, or internal or external audits and reviews, to include OMB reviews. Agencies shall use agency plans of action and milestones to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in agency information systems.	Appendix I § 4(c)(15), 4(k).

Responsibility	Description	Citation
Develop and maintain a privacy continuous monitoring strategy.	The SAOP shall develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.	Appendix I § 4(d)(9), 4(e)(2).
Establish and maintain a privacy continuous monitoring program.	The SAOP shall establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. Agencies shall ensure that a robust privacy continuous monitoring program is in place before agency information systems are eligible for ongoing authorization.	Appendix I §§ 3(b)(6), 4(d)(10)-(11), 4(e)(2).
Review authorization packages for information systems that involve PII.	The SAOP shall review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions.	Appendix I § 4(e)(9).
Encrypt moderate-impact and high-impact information.	Agencies shall encrypt all NIST FIPS Publication 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, in consultation with the SAOP (as appropriate).	Appendix I § 4(i)(14).

6. Managing 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[129] and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes.[130] As defined in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), statistical purpose refers to the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; it includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support such purposes.[131] These agencies and components shall protect the integrity and confidentiality of this information against unauthorized access, use, disclosure, modification, or destruction throughout the life cycle of the information. Further, these agencies and components shall 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.

[129] 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. § 3552. However, for the purposes of section 6 of Appendix II 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; Pub. L. 107–347, § 512(b)(1).

[130] 44 U.S.C. § 3501 note; Pub. L. 107-347, § 512(a). There are some narrowly-delineated, authorized, nonstatistical uses of information collected for statistical purposes that are noted in Section 504 of CIPSEA, including providing information to a law enforcement agency for the prosecution of submissions to the collecting agency of false statistical information under statutes that authorize criminal or civil penalties for the provision of false statistical information, unless such disclosure or use would otherwise be prohibited under Federal law.

[131] 44 U.S.C. § 3501 note; Pub. L. 107-347, § 502(9)(A)).