The Office of Management and Budget (OMB) is proposing to revise Circular No, A-130, Management of Federal Information Resources, (hereinafter, Circular A-130, or the Circular) in light of changes that have taken place in statute for information policy and information technology (including privacy and security) since the Circular was last revised in November 2000.

It has been the policy of the United States Government to support the development and use of efficient and effective information technology and information policy approaches that, when adopted by Federal agencies, can address important regulatory, procurement, or policy objectives. OMB is revising Circular A-130 to provide guidance that is timely and relevant to agency operations in a current, interconnected, ever-changing information resources environment. This revision is being conducted to incorporate revised and new statutory policy, technological advancements and enhanced technological capabilities, as well as current and evolving technical and personnel security threats. Agencies are asked to incorporate this guidance into their policies, understanding that the subject nature of this document will demand agencies continually reassess, reexamine, and reevaluate their information resources management policies and strategies.

This Circular establishes general policy for the acquisition and management of information technology personnel, equipment, funds, and other resources. It also includes a discussion of agency responsibilities for managing personally identifiable information, provides guidance on use of electronic transactions and related electronic documentation statutes, and discusses policy on protecting Federal information resources as appendices. Although this Circular touches on many specific issues such as privacy, confidentiality, information quality, dissemination, and statistical policy, those topics are covered more fully in other OMB policies, which are available on the OMB website at https://www.whitehouse.gov/omb/.

In this notice, OMB is seeking comment on proposed revisions to this Circular. These revisions reflect the experience gained by OMB and agencies in implementing the Circular since 2000. The revisions were undertaken by examining the Circular in its current form, and attempting to highlight any areas where either the guidance was duplicative, accepted as common practice as to no longer need specific instruction, or failed to address a specific issue area that had developed since previous publication. The Circular was examined concurrent with its appendices to ensure the broader direction of the Circular was complimented by the specificity of the appendices. The document's language is designed for the guidance to maintain a timeless characteristic, not immediately becoming outdated or irrelevant.

In the main body of the Circular, OMB proposes additional language on the purpose of the Circular and amends the authorities section to more fully cover existing statutes and Executive Orders.

In the Applicability section of the main body, OMB has simplified the reference to national security systems by removing "Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No.

12472" and replacing it with "For national security systems, agencies should follow applicable laws, Executive Orders, and directives."

OMB has revised the background section of the main body to better articulate agency responsibilities in this area.

In the Definitions Section, OMB has proposed several changes.

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

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

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

The Circular also proposes to modify the definitions for "agency", "capital planning and investment control process", "information resources", "information resources management", "information system", "information system life cycle", "information technology", "the CIO Council", and "dissemination", to be consistent with current guidance and statute.

Section 6, Basic Considerations and Assumptions and Section 7, Policy have been revised to incorporate both policy and statute changes since the Circular was last revised.

Section 8 of the Circular designates responsibilities first, government-wide and then specifically agency-by-agency. The section incorporates additional statutory requirements enacted since the last revision of the Circular in 2000.

Appendix I, previously titled Federal Agency Responsibilities for Maintaining Records About Individuals, is being revised to provide guidance to Federal agencies on their responsibilities for managing information resources that involve personally identifiable information (PII). The previous version of Appendix I described agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, as amended (5 U.S.C. § 552a). This information is being revised and reconstituted as OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act. The revised Appendix I, titled Responsibilities for Management of Personally Identifiable Information, provides guidance on Federal agencies' responsibilities for protecting PII – including PII collected for statistical purposes under a pledge of confidentiality – and describes a set of fair information practice principles (FIPPs) that Federal agencies should consult when managing

information resources that involve PII. Finally, Appendix I requires Federal agencies to implement the privacy controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Additional guidance on implementing the NIST SP 800-53 privacy controls is provided in Circular No. A-130, Appendix III, Responsibilities for Protecting Federal Information Resources.

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

Appendix III, previously titled Security of Federal Automated Information Resources, is being revised to establish new requirements for information security and privacy management, to incorporate new mandates in the Federal Information Security Modernization Act of 2014, and to ensure consistency with OMB policies and NIST Federal Information Processing Standards and 800-series publications. In short, the revised Appendix III provides guidance on how agencies should take a coordinated approach to information security and privacy when protecting Federal information resources. As a result, the title of the Appendix has been changed to Responsibilities for Protecting Federal Information Resources. The proposed revisions provide guidance on agency information security and privacy management, including the transition from the current static, point-in-time authorization process to a more dynamic continuous monitoring and ongoing authorization process for information systems and common controls. Examples of additional requirements included in the revised Appendix III focus on incident response, encryption, inclusion of security requirements in contracts, oversight of contractors, protecting against insider threats, protecting against supply chain risks, prohibiting unsupported software and system components, and holding personnel accountable.

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

CIRCULAR NO. A-130

Proposed

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Management of Federal Information Resources

1. Purpose

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

2. Authorities

OMB issues this Circular pursuant to the following statutes and Executive Orders:

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

b. Chief Financial Officers Act (31 U.S.C. 3512 et seq.);

c. Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E);

d. Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA);

e. Digital Accountability and Transparency Act of 2014;

f. E-Government Act of 2002 (Pub. L. 107-347);

g. Federal Acquisition Streamlining Act of 1994;

h. Federal Information Security Modernization Act of 2014;

i. Federal Information Technology Acquisition Reform Act (FITARA);

j. Federal Property and Administrative Services Act of 1940, as amended (40 U.S.C. 487);

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

l. Freedom of Information Act;

m. Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII);

n. Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRM) of 2010 (Pub. L. 111-352);

o. Information Quality Act;

p. Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7);

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

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

s. Section 508 of the Rehabilitation Act of 1973 (as amended (Pub. L. 105-220, 29 U.S.C. 794d);

t. Executive Order No. 12046, Relating to the Transfer of Telecommunications Functions, of March 27, 1978;

u. Executive Order No. 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, of April 3, 1984; and

v. Other relevant statutes and Executive Orders.

3. Applicability

a. The requirements of this Circular apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government; and

b. The requirements of this Circular do not apply to national security systems. For national security systems, agencies should follow applicable laws, Executive Orders, and directives.

4. Background

The Paperwork Reduction Act, Government Paperwork Elimination Act, Clinger-Cohen Act, E-Government Act of 2002, and Federal Information Technology Acquisition Reform Act establish a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

a. Establishing a broad mandate for agencies to perform their information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner;

b. Focusing information resources planning to support their strategic missions;

c. Implementing a Capital Planning and Investment Control (CPIC) process that links to and supports budget formulation and execution; and

d. Rethinking and restructuring the way agencies do their work before investing in information systems.

5. Definitions

a. 'Agency' means any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the Executive Branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include: (i) the Government Accountability Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) Government-owned, contractor-operated facilities, including laboratories engaged in national defense research and production activities (44 U.S.C., Sec. 3502).

b. 'Capital Planning and Investment Control Process' (CPIC) means a decision-making process that ensures that IT investments integrate strategic planning, budgeting, procurement, and management of IT in support of agency missions and business needs. The CPIC process has three distinct phases: Select, Control, and Evaluate. See 40 U.S.C 11302 and the Clinger-Cohen Act of 1996 for statutory requirements.

c. ‘Chief Information Officer’ (CIO) means the senior official that, pursuant to the Clinger-Cohen Act, provides advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that achieves the agency’s strategic goals and information resources management goals (40 USC 11315).

d. ‘Chief Information Officers Council’ (CIO Council) means the Council codified in the E-Government Act of 2002 (Pub. L. 107-347).

e. ‘Confidentiality’ means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information (44 U.S.C. § 3542(b)(B)).

f. ‘Digital services’ means the software and related technology the Federal Government provides for the public to access a service of the Federal Government, or software and technology that is custom-built on behalf of the Federal Government to directly support the delivery of a service of the Federal Government to the public.

g. ‘Dissemination’ means the government-initiated distribution of information to a nongovernment entity, including the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees, intra- or interagency use or sharing of government 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). (Note: For purposes of the Privacy Act and other privacy requirements, the term “dissemination” has a different meaning.)

h. ‘Enterprise architecture’ (a) means – (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (b) includes – (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan.

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

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

k. ‘Federal information system’ means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency (40 U.S.C., Sec. 11331).

l. ‘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).

m. ‘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.

n. ‘Information dissemination product’ means any book, paper, map, machine-readable material, electronic file, audiovisual production, or other documentary material, regardless of form or characteristic, disseminated by an agency to the public.

o. ‘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.

p. ‘Information management’ means the planning, budgeting, manipulating, controlling, and processing of information throughout its life cycle.

q. ‘Information resources’ means information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. 3502).

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

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

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

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

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

t. ‘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).

u. ‘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.

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

include any equipment that is acquired by a contractor incidental to a contract which does not require its use (40 U.S.C. 11101).

w. 'Information technology resources' means all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements which include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants which establish or support information technology not operated directly by the Federal Government.

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

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

z. '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: (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (44 U.S.C. 3542).

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

bb. 'Personally identifiable information' (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. To determine whether information is PII, agencies must perform an assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-identifiable information can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

cc. 'Records' means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government 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 Government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included (44 U.S.C. 3301). (Note: For purposes of the Privacy Act, the term 'Record' has a different meaning.)

dd. '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).

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

6. Basic Considerations and Assumptions

a. Government information is both a strategic asset and a valuable national resource. It enables the performance of effective government missions and programs and provides the public with knowledge of the government, society, and economy – past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain and enhance the healthy performance of the economy, and is itself a commodity in the marketplace.

b. Information technology is not an end in itself. Its role is in support of agency missions and programs and cannot be planned or managed independently from agency missions, priorities, and program needs.

c. The Federal Government's success in achieving the overall goals of its missions and programs depends on effective and efficient support by information resources, information technology, digital services, and related resources.

d. Openness in government strengthens our democracy. Government agencies have a responsibility to be open, transparent, and accountable to the public.

e. Managing government information as an asset to promote openness and interoperability, subject to applicable restrictions, increases operational efficiencies, reduces costs, improves services, supports mission needs, safeguards personally identifiable information, and increases public access to valuable government information.

f. Agencies must have information security programs that consider the risks and range of threats to their data and implement controls to mitigate those risks to acceptable levels.

g. The individual's right to privacy must be considered and protected throughout the information life cycle in Federal Government information activities involving personally identifiable information.

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

i. Agencies must make information accessible to employees and members of the public with disabilities in compliance with Section 508 of the Rehabilitation Act of 1973, as amended.

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

k. The Government must balance the utility of information against the burden imposed on the public and the cost of its collection.

l. Information quality is a key parameter of information utility. The rigor of information collection design should be consistent with the likely use of the information. Quality standards provide established means to evaluate rigor.

m. Federal Government collection and dissemination of information must be done pursuant to applicable statutory requirements and conform to information quality standards established by the Federal Government. These standards include, among others, statistical directives, policy guidelines, and best practices. The degree to which the information collection must conform to Federal standards should be consistent with the likely use of the information.

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

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

p. The protection of confidential statistical or trade secret information as required by statute must be upheld in Federal Government information activities throughout the information life cycle.

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

r. Because State, local, tribal, and territorial governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government should cooperate with these governments in the

management of information resources. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

s. Effective information management practices in times of limited budgetary resources depend on the strategic management of personnel, equipment, and information technology.

7. Policy

a. Ensuring Effective Information Resources Planning and Management

1) When planning, budgeting, and executing Government programs and services, agencies shall take explicit account of information resources and information technology (IT) assets, personnel, and policies.

2) Agencies shall manage information throughout its life cycle, including information collection, processing, maintenance, storage, use, sharing, dissemination, and disposition. In doing so, agencies shall:

a) Collect or create and disseminate information in a way that is open and supports downstream interoperability among information systems and dissemination of information to the public, as appropriate, without the need for costly retrofitting, to the extent permitted by law and subject to privacy, confidentiality, security, and other valid restrictions;

b) Protect the individual's right to privacy, ensure confidentiality, and have information security and privacy programs that consider the risks and range of threats to their data;

c) Consider target audiences of Government information when determining format, frequency of update, and other information management decisions;

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

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

f) Seek 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;

g) Provide training to personnel involved in information resources management;

h) Protect Government information commensurate with the risk that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information;

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

j) Collect, record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

k) Consider the effects of their actions on accessibility of technology for Federal employees and members of the public with disabilities and comply with Section 508 of the Rehabilitation Act of 1973, as amended (Pub. L. 105-220, 29 U.S.C. 794d);

l) Make their information publicly accessible to the extent permitted by law and subject to privacy, confidentiality, security, and other valid restrictions, and maintain a public inventory of their information to provide the public an efficient way to discover and access agencies' publicly available information;

m) Collect or create only that information necessary for the proper performance of authorized agency functions and that has practical utility;

n) Comply with the Privacy Act of 1974, the privacy provisions of the E-Government Act of 2002, other applicable laws, and all OMB policies on privacy;

o) Comply with the Confidential Information Protection provisions of Title IV of the E-Government Act of 2002 and OMB guidance on implementing the Confidential Information Protection provisions of the E-Government Act of 2002;

p) Comply with the Information Quality Act and OMB implementing guidance;

q) Comply with OMB Statistical Policy Directives issued under Section 3504 of the PRA; and

r) Executive agencies under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide:

(i) The option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and

(ii) The use and acceptance of electronic signatures, when practicable. Agencies shall follow the provisions in OMB memoranda on implementing requirements of the Government Paperwork Elimination Act.

b. Information Resources Management (IRM) Strategic Plan

In support of agency missions and business needs, as part of the agency's overall strategic and performance planning processes, agencies shall have an IRM Strategic Plan that describes the agency's technology and information resources goals, including but not limited to the processes described in c.-i. below. The IRM Strategic Plan shall show how these goals map to the agency's mission and organizational priorities. These goals should be specific, verifiable, and quantitatively measurable, so that progress against these goals can be tracked. The agency should review its IRM Strategic Plan annually alongside the Annual Performance Plan reviews to determine if there are any performance gaps or changes to mission needs, priorities or goals. The IRM Strategic Plan should be updated each year to incorporate necessary changes, and any annual updates should be publicly posted on the agency's website in conjunction with the Agency Strategic Plan. The associated materials shall be provided to OMB upon request.

c. Implementing Records Management

1) Agencies shall ensure that records management programs provide adequate and proper documentation of agency activities.

2) Agencies shall ensure the ability to access and retrieve records throughout their life cycle regardless of form or medium.

3) Agencies shall, in a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records.

4) Agencies shall provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

d. Providing Information to the Public

1) Agencies shall make information resources accessible, discoverable, and usable by the public to the extent permitted by law and subject to privacy, confidentiality, security and other valid restrictions.

2) Agencies have a responsibility to provide information to the public that is consistent with their missions.

3) Agencies shall address this responsibility by:

a) Managing information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguarding systems and information;

b) Maintaining a public data listing and an enterprise data inventory describing agency information resources in accordance with guidance from OMB;

c) Ensuring that the public has timely and equitable access to the agency's public information;

d) Providing information, as required by law, describing agency organization, activities, programs, meetings, record series and systems, and other information holdings, and how the public may gain access to agency information;

e) Providing access to agency records under provisions of the Freedom of Information Act, the Privacy Act of 1974, the Information Quality Act, the Federal Records Act, the E-Government Act of 2002, the Federal Information Security Modernization Act of 2014, and other relevant statutes subject to the protections and limitations provided for in these Acts;

f) Providing notice of Federal agency privacy practices for the collection, use, maintenance, and dissemination of personally identifiable information;

g) Providing any other information that is necessary or appropriate for the proper performance of agency functions and to ensure the transparency and accountability of government;

h) Providing such information proactively rather than waiting for it to be requested;

i) Providing such information in a format(s) accessible to employees and members of the public with disabilities in compliance with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d);

j) Considering whether information disseminated from other Federal or nonfederal sources is equivalent to agency information and reasonably fulfills the dissemination responsibilities of the agency;

k) Establishing and maintaining inventories of all agency information dissemination products;

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

m) Identifying the source of the information disseminated to the public, if from outside the agency;

n) Ensuring that government publications are made available to depository libraries through the Government Publishing Office, as required by law (44 U.S.C. Part 19);

o) Establishing and maintaining communications with members of the public and with State, local, tribal, and territorial governments so that the agency publishes information that meets their respective needs;

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

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

e. Conforming with Open Data Standards

Agencies shall adopt a presumption in favor of openness to the extent permitted by law and subject to privacy, confidentiality, security, and other valid restrictions. Additionally, agencies shall:

1) Whenever possible, plan for IT solutions or services that incorporate capabilities to release data online in open, machine-readable formats;

2) Disseminate information in a manner that best achieves a balance between the usefulness of the information and the cost to the government and the public;

3) Disseminate information on equitable and timely terms;

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

5) Help the public locate government information maintained by or for the agency and help make information already disseminated easy to find and locate;

6) Comply with all applicable laws governing the disclosure of information, including those related to the quality, privacy, confidentiality, security, and other valid restrictions; and

7) To the extent practicable and subject to valid restrictions, publish information online (in addition to any other planned or mandated publication methods) in an open, machine-readable format that can be retrieved, downloaded, indexed, and searched by commonly

used web search applications and is public, accessible, described, reusable, complete, timely, and managed in manners consistent with OMB guidance regarding open data. This includes providing such information in a format(s) accessible to employees and members of the public with disabilities in compliance with Section 508 of the Rehabilitation Act of 1973, as amended (Pub. L. 105-220, 29 U.S.C. 794d).

f. Avoiding Improperly Restrictive Practices

To avoid improperly restrictive practices, agencies shall:

1) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with allowing the agency to disseminate its information on a timely and equitable basis. Exceptions to this policy are time-limited restrictions or exclusivity in cases where the agency, due to resource constraints, would normally be unable to provide the information to the public on its own;

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

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

a) Where statutory requirements are at variance with the policy;

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

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

d) Where the Director of OMB determines an exception is warranted.

g. Implementing Information Safeguards

To ensure proper safeguards, agencies shall:

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

2) Limit the collection of personally identifiable information to that which is legally authorized and necessary for the proper performance of agency functions;

3) Only maintain personally identifiable information for as long as is necessary to accomplish a legally authorized purpose;

4) Limit the sharing of personally identifiable information or 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; and

5) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records consistent with the provisions of the Privacy Act.

h. IT Resources Portfolio Management

In support of agency missions and business needs and in coordination with program managers, the agency shall define, implement, and maintain processes, standards, and policies applied to all 'information technology resources' at the agency, in accordance with OMB guidance. Specifically, agencies shall ensure that department/headquarters chief information officers lead and oversee, in coordination with program managers, the following agency-wide and investment-level management processes, in accordance with OMB guidance:

1) Define the development processes, milestones, review gates, and the overall policies for all capital planning and project management and reporting for IT resources;

2) Perform planning, programming, budgeting, and execution decisions, related reporting requirements, and reports related to IT resources, and the management, governance, and oversight processes related to IT resources;

3) Establish and maintain a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. Work with program managers to ensure that legacy and ongoing IT investments are appropriately delivering customer value and meeting the business objectives of programs;

4) Establish a portfolio-wide acquisition strategy that avoids duplication by considering existing solutions first and adopt the contracting vehicles necessary to build a robust technology infrastructure in coordination with program managers;

5) Ensure that the workforce related to IT resources has the appropriate knowledge and skill for facilitating the achievement of the performance goals established for the portfolio of IT resources and evaluate the extent to which the executive-level workforce of the agency has appropriate IT-related knowledge and skills;

6) Develop an enterprise architecture that describes the baseline architecture, the target architecture, and a plan to get to the target architecture;

7) Ensure that IT resources across the portfolio use appropriate measurements to evaluate the cost variance, schedule variance, and overall performance of their activities as a part of portfolio-wide processes such as capital planning and investment control, enterprise architecture, and other agency information technology or performance management processes. When an Earned Value Management System (EVMS) is required, the standard definitions of cost variance and schedule variance will be used to measure progress;

8) Establish agency-wide policies and procedures for conducting investment reviews, operational analyses, or other applicable performance reviews to evaluate the following aspects of IT resources, including projects in development and ongoing activities: determine whether there is a continuing need for the activity as planned; for high-risk activities whether the root causes of risk in the investment have been addressed, whether there is sufficient capability to deliver the remaining planned increments within the planned cost and schedule, and what corrective actions, including termination, should be taken;

9) Establish an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:

a) Weighing potential and ongoing investments and their underlying capabilities against other proposed and ongoing investments in the portfolio;

b) Implementing an EVMS and conducting an Integrated Baseline Review (IBR) as required by Federal Acquisition Regulation Subpart 34.2 or, when an EVMS is not required, implementing a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance; and

c) Identifying gaps between planned and actual cost, schedule, and performance goals for information technology investments and identifying strategies and time frames to close such gaps;

10) 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 judgment—including but not limited to the results of the processes described in 1) through 9) above—within the terms of the relevant contracts and applicable regulations; and

11) Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511), Freedom of Information Act (5 U.S.C. 552(g)), and Federal Information Security Modernization Act of 2014: an inventory of the agency's major information systems, holdings, and dissemination products; a description of the agency's major information and record locator systems; an inventory of the agency's other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency's information resources); and an online resource for persons to obtain public information from the agency pursuant to these Acts.

i. IT Investment Management

IT investment decisions must also be consistent with policies and processes defined by the agency as described above. Agency chief information officers shall establish criteria identifying which of the following investment management aspects require the direct involvement of the chief information officer in accordance with the below requirements. Agencies shall ensure that policies and processes approved by the department/headquarters chief information officer are applied to all IT investment decisions and processes below.

1) Acquisition of Information Technology

Agencies shall:

a) Consistent with applicable Federal acquisition requirements, make use of adequate competition, allocate risk between government and contractor, and maximize return on investment (ROI) when acquiring information technology;

b) Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of migration and retraining costs, scaled to the size and complexity of individual requirements (definitive acquisition planning provisions are set forth in Federal Acquisition Regulation [FAR] subparts 7.1, Acquisition Plans, and 10, Market Research);

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

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

e) Not approve an acquisition strategy or acquisition plan (as described in FAR Part 7) or interagency agreement (such as those used to support purchases through another agency) that includes IT without review and approval by the agency CIO. The CIO shall consider the following factors when reviewing acquisition strategies and acquisition plans:

(i) Alignment with mission and program objectives in coordination with program leadership;

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

(iii) Appropriateness of contract type for IT-related resources; and

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

2) IT Capital Planning and Investment Control

IT Capital Planning and Investment Control (CPIC) is the process by which agencies establish the need and goals to plan, acquire or develop, and evaluate the results of investments in information systems, technologies, and capabilities in support of agency missions, organizational and performance requirements, strategies, and goals. Agencies must designate IT investments as major investments or non-major investments according to relevant statute, regulations and guidance in OMB Circular A-11, and perform CPIC processes commensurate with the size, scope, duration, and delivery risk of the investment. The CPIC process consists of all stages of capital programming, including planning, budgeting, procurement, management, and assessment. For further guidance on capital programming, refer to OMB Circular A-11, including the Capital Programming Guide. IT CPIC comprises portfolio-level planning and management, and investment-specific planning and management. Agency CPIC processes must be consistent with OMB guidance defining the steps, standards, reporting artifacts, responsibilities, and other aspects of CPIC. The actions, policies, and artifacts of the CPIC process's evaluation, selection, and control phases shall ensure that the following requirements are appropriately met by all IT resources:

a) All IT resources are included in IT portfolio and capital planning documents or artifacts;

b) In coordination with program managers, significant decisions related to major IT investments are supported by business cases with appropriate evidence;

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

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

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

f) Preference must first be given to using available and suitable Federal information systems, technologies, and shared services or information processing facilities, or to acquiring commercially available off-the-shelf software and technologies over developing or acquiring custom or duplicative solutions. Decisions to acquire custom or duplicative solutions must be justified based on overall life-cycle cost-effectiveness or ability to meet specific and high-priority mission or operational requirements;

g) Information technology needs are met through scalable, provisioned services when it is cost-effective to do so rather than acquiring or developing new information systems or equipment;

h) New acquisitions which include information technology must evaluate open source software and off-the-shelf technology as options;

i) Information systems security levels are commensurate with the risk that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information;

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

k) Information systems and processes must support interoperability and information accessibility, maximize the usefulness of information, minimize the burden on the public, and preserve the appropriate integrity, usability, availability, confidentiality, and disposition of information throughout the life cycle of the information, in accordance with the PRA, FISMA, Privacy Act (as amended) and the Federal Records Act (as amended);

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

m) Agencies must incorporate records management functions and retention requirements into the design, development, and implementation of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service.

8. Assignment of Responsibilities

a. For all Federal agencies, the head of each agency shall:

1) Have primary responsibility for managing agency information resources to support agency missions and business requirements;

2) Ensure that the digital services provided by the agency work well and are continually improved to better meet the needs of the public;

3) Ensure that the agency implements the information policies, principles, directives, standards, guidelines, rules, and regulations promulgated by OMB, as appropriate;

4) Develop agency policies and procedures that provide for timely acquisition of required information technology;

5) Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design, and operation of information systems;

6) Identify to the Director of OMB any statutory, regulatory, and other impediments to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

7) Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

8) Ensure that the agency:

a) Cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs; and

b) Promotes a coordinated, interoperable, secure, and shared governmentwide infrastructure that is provided and supported by a diversity of private sector suppliers;

9) Develop a well-trained corps of information resources management professionals;

10) Develop an effective and experienced corps of digital services experts;

11) Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, Acquisition and Management of Capital Assets," and other relevant OMB guidance for IT CPIC to promote effective and efficient capital planning within the organization;

12) Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11 and related OMB guidance, and ensure, to the extent reasonable, that in the design of information systems with the purpose of disseminating information to the public, an index of information disseminated by the system shall be included in the directory created by the Superintendent of Documents pursuant to 41 U.S.C. 4101. (Nothing in this paragraph authorizes the dissemination of information to the public unless otherwise authorized.);

13) Permit, to the extent practicable, the use of one agency's contract by another agency or the award of multiagency contracts, provided the action is within the scope of the contract and consistent with OMB guidance;

14) As designated by the Director of OMB, act as executive agent for the governmentwide acquisition of information technology;

15) Ensure compliance with Federal information privacy and security requirements, to include statistical confidentiality;

16) Designate a senior agency official for privacy (SAOP) who has overall agency-wide responsibility for information privacy; and

17) Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a).

a) The CIO shall report directly to the agency head as required by the Clinger-Cohen Act (40 U.S.C. 1425(b) & (c)). Agencies that have implemented legislation that requires the CIO and other management officials to report to a Chief Operating Officer (COO), Undersecretary for Management, Assistant Secretary for Administration, or similar management executive shall ensure that the CIO has direct access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the Secretary's behalf) for their information technology responsibilities to remain consistent with the Clinger-Cohen requirement.

b) The CIO shall carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger-Cohen Act (40 U.S.C. 1425(b) & (c)), the E-Government Act of 2002 (Pub. L. 107-347), the Privacy Act of 1974 (as amended (5 U.S.C. 552a)), the Government Performance and Results Modernization Act of 2010 (Pub. L. 111-352), the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), the Federal Records Act of 1950 (as amended, codified (44 U.S.C. Chapter 29, 31, 33)), the Federal Acquisition Streamlining Act V, Section 508 of the Rehabilitation Act of 1973 (as amended (Pub. L. 105-220, 29 U.S.C. 794d)); the Digital Accountability and Transparency Act of 2014; the Federal Information Security Modernization Act of 2014; and other related statutes.

c) The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and shall advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer.

For purposes of this paragraph (17), military departments and the Office of the Secretary of Defense may each appoint one official.

b. The Chief Information Officer, in coordination with other agency senior officials and program managers, must, among other things:

1) Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities (including the management of information technology resources) for conformity with the policies set forth in this Circular;

2) Advise the agency head on information resources implications of strategic planning decisions;

3) Advise the agency head on the design, development, and implementation of information resources;

4) Advise the agency head on budgetary implications of decision affecting information resources and information technology resources;

5) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information technology resources;

6) Review and approve all reprogramming of funds related to information technology resources;

7) Advise and support the teams responsible for creating and maintaining the agency's digital services, including by coordinating with such teams to ensure that digital services activities support the overall program and business objectives of the information technology resources portfolio as well as the agency's missions and programs;

8) Define, maintain, and oversee policies and standards governing all strategic-level and investment-level information technology management processes described in Section 8. Identify incomplete or inconsistent application of these policies and standards within the agency and report these to the agency head and OMB as appropriate. In consultation with OMB, describe the effectiveness of these agency processes as a part of portfolio reviews or other reporting;

9) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans;

10) Designate an official within the office of the CIO to serve as a liaison to help coordinate agency actions and policies with the agency's SAOP, unless the agency's CIO is designated as the SAOP;

11) Collaborate with heads of Federal principal statistical agencies and recognized statistical units to support their conformance with Statistical Policy Directives governing the design, scope, collection, processing, calculation, production, and dissemination of official Federal statistics;

12) Monitor and evaluate the performance of information technology investments through a CPIC process, and advise the agency head on whether to continue, modify, or terminate a program or project;

13) Be responsible for ensuring that the agency workforce has the information resources management skills it needs by playing a material role in the selection of staff with significant information technology resource management responsibilities; continuously assessing and improving the requirements established for agency personnel regarding knowledge and skills; determining the extent to which the positions and personnel at the agency meet those requirements; and developing strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements;

14) Report to the agency head on the effectiveness of the agency information security program;

15) Maintain regular participation with the Chief Information Officers Council which serves as the principal interagency forum for CIOs to share best practices, seek out assistance

from other Federal CIOs and to collaborate on improving the management of Federal IT; and

16) Oversee agency compliance with the prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under the Paperwork Reduction Act, which include reducing the information collection burdens on the public and increasing the utility of information created, collected, maintained, used, shared, and disseminated by the agency. Specific responsibilities include:

a) Establishing an independent (independent of program responsibility) review process for information collections;

b) Seeking and obtaining OMB approval before undertaking a collection of information directed to 10 or more persons;

c) Publishing a 60-day notice in the *Federal Register* requesting public comment on the proposed collection of information;

d) Reviewing and considering public comments received on the proposed collection of information;

e) Publishing a 30-day notice in the *Federal Register* notifying the public of the agency's request for comments and submission to OMB for review of the proposed collection of information; and

f) Fulfilling all other duties and responsibilities assigned to the Chief Information Officer per 5 C.F.R. 1320.

c. Department of State

The Secretary of State shall:

1) Consult with and advise the Director of OMB on the development of United States positions and policies on international information policy and technology issues affecting Federal Government activities and the development of international information technology standards; and

2) Be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including Federal information technology. The Secretary must also ensure, in consultation with the Secretary of Commerce, that the United States is robustly represented in the development of international standards and recommendations affecting information technology. These responsibilities may also require the Secretary to consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

d. Department of Commerce

The Secretary of Commerce shall:

1) Develop and issue Federal Information Processing Standards (FIPS) and guidelines necessary to ensure the efficient and effective acquisition, management, security, and

use of information technology, while taking into consideration the recommendations of the agencies and the CIO Council;

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

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;

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

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; and

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

e. Department of Defense

The Secretary of Defense shall develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

f. Department of Homeland Security

The Department of Homeland Security shall:

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

2) Assist the Office of Management and Budget in carrying out its information security oversight and policy responsibilities;

3) In consultation with OMB, develop and oversee the implementation of binding operational directives to agencies. Such directives shall be consistent with OMB policies and NIST standards and guidelines. The directives may be revised or repealed by OMB if the direction issued on behalf of OMB is not in accordance with policies developed by OMB. The binding operational directives shall focus on:

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

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

   c) Other operational requirements, as deemed necessary by OMB or DHS, in consultation with OMB;

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

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

6) Coordinate governmentwide efforts on information security policies and practices, including consultation with the Chief Information Officers Council and the National Institute of Standards of Technology;

7) Provide and operate Federal information security shared services as directed by OMB;

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

   a) Operating the Federal information security incident center;

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

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

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

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

10) Consult with OMB to determine what other actions may be necessary to support implementation of effective governmentwide information security programs; and

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

g. General Services Administration

The Administrator of General Services shall:

1) Continue to manage a governmentwide network contract program and coordinate the follow-up to that program, on behalf of and with the advice of agencies;

2) Develop, maintain, and disseminate for the use of the Federal community (as requested by OMB or agencies) recommended methods and strategies for the development and acquisition of information technology;

3) Conduct and manage outreach programs in cooperation with agency managers;

4) Serve as a liaison on information resources management (including Federal information technology) with State, local, tribal, and territorial governments. GSA must also be a liaison with nongovernmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5) Provide support and assistance to the CIO Council; and

6) Manage the Acquisition Services Fund in accordance with Public L. 109-313.

h. Office of Personnel Management

The Director, Office of Personnel Management shall:

1) Analyze on an ongoing basis, the personnel needs of the Federal Government related to information technology and information resources management;

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

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

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

i. National Archives and Records Administration

The Archivist of the United States shall:

1) Administer the Federal records management program in accordance with the Federal Records Act and National Archives and Records Administration (NARA) requirements (36 CFR Subchapter B – Records Management);

2) Assist the Director of OMB in developing standards and guidelines relating to the records management program; and

3) Create records management policies, ensure agency compliance with records management requirements and provide training as needed, and coordinate with OMB and other agencies, to provide public access to high-value government records.

9. Effectiveness

This Circular is effective upon issuance. 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.

10. Oversight

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

11. Inquiries

All questions or inquiries regarding information resources management, Government paperwork elimination, privacy, and confidentiality should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785 or Email: infopolicy-oira@omb.eop.gov or privacy-oira@omb.eop.gov. Questions or inquiries regarding information systems and technology or the security of Federal information resources should be addressed to the Office of Electronic Government and

Information Technology, Office of Management and Budget, Washington, D.C. 20503.
Telephone: (202) 395-0379 or Email: egov@omb.eop.gov.

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

1. Purpose

This Appendix outlines some of the general responsibilities for Federal agencies managing information resources that involve personally identifiable information (PII). For more specific requirements, agencies should consult specific OMB guidance documents, which are available on the OMB website.

Previous versions of this Appendix included information about the reporting and publication requirements of the Privacy Act of 1974 (5 U.S.C. § 552a) and additional OMB guidance. This information has been revised and reconstituted as OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, which is also available on the OMB website.

2. Responsibilities for Protecting PII

The Federal Government necessarily collects, uses, disseminates, and maintains PII to carry out the missions mandated by the Constitution and laws of the United States. The term PII, as defined in the main body of this Circular, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. To determine whether information is PII, agencies must perform an assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-identifiable information can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

When Federal agencies manage information resources that involve PII, the individual's privacy must be considered and appropriately protected. Agencies are required to designate a senior agency official for privacy (SAOP) who has overall agency-wide responsibility and accountability for ensuring the agency's implementation of all privacy requirements. The SAOP should have a central policy-making role and should ensure that the agency considers the privacy impact of all agency actions and policies that involve PII. The SAOP's review of privacy implications should begin at the earliest planning and development stages of agency actions and policies that involve PII, and should continue through the life cycle of the information.

The SAOP must ensure that the agency complies with all applicable requirements in law, regulation, and policy. Relevant authorities include, but are not limited to, the Privacy Act of 1974 (5 U.S.C. § 552a), the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35), the E-Government Act of 2002 (44 U.S.C. § 3501 note), *Privacy Act Implementation: Guidelines and Responsibilities* (40 Fed. Reg. 28,948, July 9, 1975), *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988* (54 Fed. Reg. 25,818, June 19, 1989), and *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (OMB Memorandum M-03-22, Sept. 26, 2003).

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

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

Given the importance of robust and objective official Federal statistics, agencies and components charged with the production of these statistics are assigned particular responsibility. Specifically, information acquired by an agency or component under a pledge of confidentiality and for exclusively statistical purposes cannot be used for any regulatory or enforcement purpose. As defined in the Confidential Information Protection and Statistical Efficiency Act (Pub. L. 107–347, title V; 116 Stat. 2962), statistical purpose refers to the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that compose such groups; it includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support such purposes. These agencies and components must protect the integrity and confidentiality of this information against unauthorized access, use, modification, or deletion throughout the life cycle of the information. Further, these agencies and components must adhere to legal requirements and follow best practices for protecting the confidentiality of data, including training their employees and agents, and ensuring the physical and information system security of confidential information.

Relevant authorities include, but are not limited to, Title V of the E-Government Act of 2002, the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) (Pub. L. 107–347, title V; 116 Stat. 2962) and *Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002* (CIPSEA Implementation Guidance) (72 Fed. Reg. 33362, 33368, June 15, 2007); and *Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units* (79 Fed. Reg. 71610, Dec. 2, 2014).

4. Fair Information Practice Principles

In addition to the requirements in law, regulation, and policy, agencies should consult the Fair Information Practice Principles (FIPPs) when managing information resources that involve PII. The FIPPs are a collection of widely accepted principles that agencies should use when evaluating systems, processes, programs, and activities that affect individual privacy. Rooted in a 1973 Federal Government report, the FIPPs are at the core of the Privacy Act of 1974, and are reflected in the laws of many U.S. states and foreign nations, as well as incorporated in the policies of many organizations around the world.

The precise expression of the FIPPs has varied over time and in different contexts. However, the FIPPs retain a consistent set of core principles that are broadly relevant to agencies' information management practices. The FIPPs are as follows:

a. *Individual Participation*. Agencies should involve the individual in the decision-making process regarding the collection, use, dissemination, and maintenance of PII and, to the extent practicable, seek individual consent for these activities.

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

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

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

e. *Minimization*. Agencies should only collect and maintain 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.

f. *Access and Amendment*. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

g. *Redress*. Agencies should provide individuals with appropriate opportunity for redress regarding unauthorized use and dissemination of PII, and should establish procedures to receive and address individuals' privacy-related complaints.

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

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

j. *Training*. Agencies should clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

k. *Integration*. Agencies should begin to consider the effect on individual privacy during the earliest planning and development stages of any actions and policies, and should continue to account for privacy implications during each stage of the life cycle of PII.

l. *Accountability*. Agencies should be accountable for complying with these principles and all applicable privacy requirements, and should appropriately monitor, audit, and document compliance.

5. Privacy Controls for Federal Information Systems and Organizations

Agencies cannot protect privacy without considering information security. Therefore, it is essential for agencies to take a coordinated approach to identifying and addressing privacy and security requirements. A coordinated approach allows agencies to more effectively consider

privacy and security requirements that may overlap in concept and in implementation within Federal information systems, programs, and organizations.

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

The requirement to implement security and privacy controls is described in more detail in Appendix III to this Memorandum, *Responsibilities for Protecting Federal Information Resources.*

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

1. Summary

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

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

E-SIGN promotes the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between:

a. Contracts written on paper and contracts in electronic form;

b. Pen-and-ink signatures and electronic signatures; and

c. Other legally required written documents (termed "records") and the same information in electronic form.

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

In support of GPEA and E-SIGN, the General Services Administration, in coordination with the Federal Chief Information Officers' Council, maintains guidance on use of Electronic Signatures (E-Signatures) in Federal organization transactions which expands upon OMB guidance.

2. Background

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

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

Public confidence in the security of the government's electronic information processes is essential as agencies make this transition. Electronic commerce, electronic mail, and electronic

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

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

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

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

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

3. Guidance

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

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

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

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

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

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

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

Requirements

1. Introduction

Agencies[1] 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 (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. These threats include environmental disruptions, purposeful attacks, structural failures, human errors, and other threats that can compromise the confidentiality, integrity, or availability of information. Leaders at all levels of the Federal Government must understand their responsibilities and be held accountable for managing information security and protecting privacy.

Federal agencies must implement information security programs and privacy programs with the flexibility to meet current and future information management needs and the sufficiency to comply with applicable requirements. Emerging technologies and services will 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 address current threats while protecting their information resources and privacy. The programs must also have the capability to address new and emerging threats. To be effective, information security and privacy must be part of the day-to-day operations of agencies. This is best accomplished by planning for the requisite security and privacy capabilities as an integral part of the agency strategic planning and risk management processes, not as a separate activity. This includes, but is not limited to, the integration of information security and privacy requirements (and associated security and privacy controls) into the enterprise architecture, system development life cycle activities, systems engineering processes, and acquisition processes.

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. OMB requires agencies to take a risk-based approach to information security to ensure that appropriate safeguards and countermeasures are selected and implemented in a prioritized manner for current missions and business operations. Such risk-based approaches involve framing, assessing,

[1] The terms *agency* and *organization* are interspersed throughout the document. However, these terms have similar meaning depending on the original sources of reference. The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as Federal statute or policy. The term *organization* is used in this publication to describe an entity of any size, complexity, or positioning within an organizational structure (e.g., a Federal agency or, as appropriate, any of its operational elements).

responding to, and monitoring security risks on an ongoing basis. Risk-based approaches can also support potential performance improvements and cost savings when agencies make decisions about maintaining, modernizing, or replacing existing information technologies and services or implementing new technologies and services that leverage internal, other government, or private sector innovative and market-driven solutions. These responsibilities extend to the creation, collection, processing, storage, transmission, dissemination, and disposal of Federal information when such information is hosted by nonfederal entities on behalf of the Federal Government. Ultimately, agency heads remain responsible and accountable for ensuring that information management practices comply with all applicable requirements, and that Federal information is adequately protected commensurate with the risk resulting from the unauthorized access, use disclosure, disruption, modification, or destruction of such information.

While it is essential for agencies to take a coordinated approach to identifying and addressing security and privacy requirements, it is also important to recognize that security and privacy are different and may require different approaches. For example, privacy laws and policies often establish clear rules and requirements that agencies must comply with when collecting, using, maintaining, or disseminating personally identifiable information (PII). When agencies are taking steps to meet these specific requirements, a purely risk-based approach is not taken since the requirements must be satisfied in full. However, once the baseline privacy requirements are met, agencies are expected to use privacy impact assessments and other tools to further analyze privacy risks and consider the implementation of additional privacy control enhancements to protect PII. For more information about privacy requirements, consult Appendix I to this Memorandum, *Responsibilities for Management of Personally Identifiable Information*.

2. Purpose

This Appendix establishes minimum requirements for Federal information security programs, assigns Federal agency responsibilities for the security of information and information systems, and links agency information security programs and agency management control systems established in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. This Appendix also establishes requirements for Federal privacy programs, assigns responsibilities for privacy program management, and describes how agencies should take a coordinated approach to implementing information security and privacy controls.[2] This Appendix revises requirements contained in previous versions of Appendix III to OMB Circular No. A-130, and incorporates requirements of the Federal Information Security Modernization Act of 2014 (P.L. 113-283), the E-Government Act of 2002 (P.L. 107-347), and responsibilities assigned in Executive Orders and Presidential Directives.

3. Definitions

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

b. 'Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of

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

information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

c. 'Authorization' means the official management decision given by a senior Federal official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational 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 organizational information systems.

d. 'Authorization boundary' means all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.[3]

e. 'Authorization official' means a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

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

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

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

i. 'Control inheritance' means a situation in which an information system or application receives protection from security and privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal and external to the organization where the system or application resides.

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

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

k. '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)).

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

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

n. '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.

o. 'Information security continuous monitoring' means maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[4]

p. 'Information system resilience' means the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

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

r. 'National security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency: (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (44 U.S.C. § 3552).

s. 'Ongoing authorization' means the risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk

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

tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether or not the mission/business risk of continued system operation is acceptable.

t. 'Overlay' means a specification of security and/or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

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

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

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

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

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

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

aa. '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.

bb. 'Risk management' means the program and supporting processes to manage information security and privacy risk to organizational operations (including mission, functions, image, reputation), organizational 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.

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

dd. ‘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 organizational operations, organizational assets, individuals, other organizations, and the Nation.

ee. ‘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.

ff. ‘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.

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

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

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

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

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

ll. ‘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 organization-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.

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

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

4. General Requirements

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

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

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

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

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

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

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

7) Implement an agency-wide risk management approach that frames, assesses, responds to, and monitors information security risk across three organizational tiers (i.e., organization level, mission/business process level, and information system level);[5]

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

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

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

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

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

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

c. Agencies must implement security and privacy policies, standards, and procedures that are consistent and compliant with statutory and governmentwide requirements as well as applicable security- and privacy-related policies, standards, and procedures issued by the Office of Management and Budget (OMB), the Department of Commerce (DOC), the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes following the standards and guidelines contained in Federal Information Processing Standards (FIPS) and NIST (800-series) Special Publications.

5. Specific Requirements[6]

a. Security Categorization

Agencies must:

1) Identify appropriate authorization boundaries for information systems; and

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

b. Planning and Budgeting, Capital Planning, and Enterprise Architecture

Agencies must:

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

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

3) Ensure that capital 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

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

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

c. Plans, Controls, and Assessments

Agencies must:

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

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

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

4) Develop security and privacy plans for information systems and environments of operation to record security and privacy controls and appropriate implementation details;

5) Designate common controls in order to provide cost-effective security and privacy capabilities that can be inherited by multiple organizational information systems;

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

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

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

9) Conduct and record the results of security control assessments and privacy control assessments in security and privacy assessment reports, respectively;

10) Use agency Plans of Action and Milestones (POA&Ms), and make available or provide access to OMB, DHS, Inspectors General, and the Government Accountability Office, upon request, to record and manage the mitigation and remediation of identified

weaknesses and deficiencies, not associated with accepted risks, in organizational information systems and environments of operation; and

11) 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 organization's operations and assets, individuals, other organizations, and the Nation.

d. Authorization and Continuous Monitoring

Agencies must:

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

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

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

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

5) Develop an ISCM strategy and PCM strategy to address information security and privacy risks and requirements across the organizational risk management tiers (i.e., organization/governance tier, mission/business process tier, and/or information system tier);[7]

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

7) Ensure that all selected and implemented controls are addressed in the ISCM strategy and PCM strategy and are effectively monitored on an ongoing basis, as determined by the agency's ISCM and PCM programs;[8]

8) Establish and maintain an ISCM program that:

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

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

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

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

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

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

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

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

g) Maintains awareness of threats and vulnerabilities;

9) Establish and maintain a PCM program that:

a) Ensures continued compliance with all applicable privacy requirements;

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

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

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

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

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

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

e. Privacy Controls for Federal Information Systems and Organizations

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

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

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

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

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

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

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

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

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

f. Incident Response

Agencies must:

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

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

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

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

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

6) Document lessons learned for incident response and update procedures as necessary; and

7) Provide reports on incidents as required by FISMA, OMB policy, and DHS binding operational directives.

g. Awareness and Training

Agencies must:

1) Develop and maintain agency-wide information security and privacy awareness and training programs;

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

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

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

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

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

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

8) Consider consequences of violating rules of behavior to include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy.

h. Additional Measures to Protect the Confidentiality, Integrity, and Availability of Federal Information and Information Systems

Agencies must:

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

2) Implement a policy of least privilege by minimizing the number of information system privileges that are needed to perform functions;

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

4) Audit the execution of information system functions by privileged users to detect misuse and to help mitigate the risk from insider threats;

5) Prohibit the use of unsupported information system components[9] unless there is an overriding mission necessity validated by the Deputy Secretary or equivalent;

6) Implement and maintain current updates for all software and firmware components of information systems;[10]

7) For systems that promote public access, ensure that identity proofing, registration, and authentication processes provide assurance of identity consistent with security and

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

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

privacy requirements, in accordance with Executive Order 13681,[11] OMB policy, and NIST standards and guidelines;

8) Require use of multifactor authentication for employees and contractors in accordance with governmentwide identification standards;

9) Encrypt all moderate- and high-impact information at rest or in transit, unless the ability to do so is technically infeasible and the risk of not encrypting is accepted by the authorizing official;

10) Implement the current encryption algorithms in accordance with NIST standards and guidelines;

11) Develop and implement policies and procedures to support employees and contractors in uniformly applying digital signatures to secure documents and communications;

12) Implement attribute-based access security controls to control and monitor access to Federal information;

13) Implement digital rights management capabilities to control the distribution and prevent the unauthorized alteration or disclosure of Federal information;

14) Implement measures to protect against supply chain threats to information systems, system components, or information system services by employing agency-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy; and

15) Employ contingency planning and resiliency concepts and methodologies to ensure the confidentiality, integrity, and availability of Federal information and information systems supporting agency missions and business operations.

i. Contracts and Grants

Agencies must ensure that terms and conditions in contracts and grants involving the processing, storage, transmission, and destruction of Federal information are sufficient to enable agencies to meet necessary mitigation, oversight, and law enforcement requirements concerning Federal information, including but not limited to, sufficient provisions for government notification and access, as well as cooperation with agency personnel and Inspectors General, particularly in the event of a data breach or related security or privacy incident. Refer to the Federal Acquisition Regulation, Part 7, Acquisition Planning, Subpart 7.1, Acquisition Plans for additional requirements pertaining to information technology acquisitions.

j. Oversight of Nonfederal Entities Hosting Federal Information

Agencies must:

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

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

a) Documenting policies and procedures for information security and privacy oversight of systems operated on the organization's behalf, or that contain Federal information, by contractors or other entities;

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

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

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

e) Ensuring that the appropriate procedures are in place for incident response for these systems including timelines for breach notification and required data points;

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

g) Implementing policies and procedures to ensure that systems that are owned or operated by contractors or entities that contain Federal information are compliant with FISMA requirements, OMB policies, and applicable NIST standards and guidelines; and

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

k. Mitigation of Deficiencies and Issuance of Status Reports

Agencies must correct deficiencies that are identified through information security assessments, ISCM programs, or internal/external audits and reviews. OMB Circular No. A-123, *Management's Responsibility for Internal Control*, provides guidance to determine whether a deficiency in controls is material when so judged by the agency head against other agency deficiencies. Material deficiencies must be included in the annual Federal Managers Financial Integrity Act (FMFIA) report, and remediation tracked and managed through the agency's Plan of Action and Milestones (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 must provide FISMA and privacy management reports in accordance with processes established by OMB and DHS.

m. Cybersecurity Framework

The Cybersecurity Framework was developed by NIST in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The Framework describes five core cybersecurity functions (i.e., Identify, Protect, Detect, Respond, and Recover) that may be helpful in raising awareness and facilitating communication among agency stakeholders,

including executive leadership. The Cybersecurity Framework may also be helpful in improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. The Framework is not intended to duplicate the current information security and risk management practices in place within the Federal Government. However, in the course of managing information security risk using the established NIST Risk Management Framework and associated security standards and guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to complement their current information security programs. NIST will provide additional guidance on how agencies can use the Cybersecurity Framework and in particular, how the two frameworks can work together synergistically to help agencies develop, implement, and continuously improve their information security programs.

n. Independent Evaluations

Agencies must:

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

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

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

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

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

6. Assignment of Responsibilities

a. Department of Commerce

The Secretary of Commerce must:

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

2) Review and update guidelines for information security awareness, training, and education and accepted information security practices, with assistance from OPM;

3) Provide agencies guidance for security planning to assist in their development of security plans;

4) Provide guidance and assistance, as appropriate, to agencies concerning cost-effective security controls;

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

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

b. Department of Homeland Security

The Secretary of Homeland Security must:

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

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

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

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

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

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

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

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

6) Revise or repeal binding operational directives when OMB determines that the directives are not in accordance with OMB policies, principles, standards, or guidelines;

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

8) Coordinate governmentwide efforts on information security policies and practices, including consultation with the Chief Information Officers Council and NIST;

9) Manage governmentwide information security programs and provide and operate Federal information security shared services, as directed by OMB;

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

   a) Operating the Federal information security incident center;

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

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

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

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

12) Consult with OMB to determine what other actions may be necessary to support implementation of effective governmentwide information security programs; and

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

c. Department of Defense

The Secretary of Defense must:

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

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

d. Department of Justice

The Attorney General must:

1) Provide appropriate guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents; and

2) Pursue appropriate legal actions when security incidents occur.

e. General Services Administration

The Administrator of General Services must:

1) Provide guidance to agencies on addressing security considerations when acquiring information technology resources;

2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services;

3) Provide appropriate security-related services to meet the needs of agencies to the extent that such services are cost-effective;

4) Maintain a public key infrastructure framework to allow efficient interoperability among executive agencies when using digital certificates; and

5) Ensure effective security controls are in place to protect the confidentiality, integrity, availability of the Federal public key infrastructure.

f. Office of Personnel Management

The Director of the Office of Personnel Management must:

1) Ensure that its regulations concerning information security training for Federal civilian employees are effective;

2) Assist the Department of Commerce in updating and maintaining guidelines for security training and education; and

3) Determine minimum investigative requirements for Federal employees and contractors requiring access to Federal facilities, information, and/or information systems.

Discussion of the Major Provisions in the Appendix

1. NIST Standards and Guidelines

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

For non-national security programs and information systems, agencies must follow NIST guidelines unless otherwise stated by OMB. Federal Information Processing Standards (FIPS) are mandatory. There is flexibility within NIST's guidelines (specifically in the 800-series) in how agencies apply those guidelines. Unless specified by additional implementing policy by OMB, the concepts and principles described in NIST guidelines must be followed. However, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant with the guidelines.

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

2. 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 no less than annually. This requirement 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 organization in accordance with the ISCM and PCM strategies. These strategies will define the specific security and privacy controls selected for assessment during any one-year period (i.e., the annual assessment window) with the understanding that all controls may not be formally assessed every

year. Rotational assessment of security and privacy controls is consistent with the transition to ongoing authorization and assumes the information system has completed an initial authorization where all controls were formally assessed for effectiveness.

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

3. Responding to Information Security Risk

Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Identifying and analyzing alternative courses of action typically occurs at Tier 1 (organizational governance level) or Tier 2 (mission/business process level). Alternative courses of action (i.e., potential risk responses) are evaluated in terms of anticipated organization-wide impacts and the ability of organizations to continue to successfully carry out missions and business functions. Decisions to employ risk response measures organization-wide are typically made at Tier 1, although the decisions are informed by risk-related information from the lower tiers. At Tier 2, alternative courses of action are evaluated in terms of anticipated impacts on missions/business functions, the associated mission/business processes, and resource requirements. At Tier 3 (information system level), alternative courses of action tend to be evaluated in terms of the system development life cycle or the maximum amount of time available for implementing the selected course(s) of action. The breadth of potential risk responses is a major factor for whether the activity is carried out at Tier 1, Tier 2, or Tier 3. Risk decisions are influenced by organizational risk tolerance developed as part of risk framing activities at Tier 1. Organizations can implement risk decisions at any of the risk management tiers with different objectives and utility of information produced.

4. Authorization to Operate

The authorization to operate an information system and the authorization of organization-designated common controls granted by senior Federal officials provide an important quality control for agencies. By authorizing an information system, a Federal official accepts the risk associated with operating that system to include the risk associated with the inherited common controls, which may have been separately authorized by another Federal official. Authorization is an inherently Federal responsibility and must be conducted by a Federal official. The decision to authorize a system to operate should be based on a review of the authorization package and includes an assessment of compliance with applicable requirements and risk to organizational

operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

The decision to authorize a system, or organization-defined common controls, should be made by the appropriate authorizing official – an agency official responsible for the associated missions, business functions, and/or supporting infrastructure. Since the security plan and privacy plan establish the security and privacy controls selected for implementation, those plans are a critical part of the authorization package and should form the basis for the authorization, supplemented by more specific information as needed. The authorizing official should consult with the SAOP prior to making risk determination and risk acceptance decisions. The SAOP should review authorization packages and determine that all applicable privacy requirements are met and the risk to PII is sufficiently addressed before authorizing officials make risk determination and risk acceptance decisions. In situations where the authorizing official and SAOP cannot reach a final resolution regarding the appropriate protection for the organizational information and information system, the head of the agency must review the associated risks and requirements and makes a final determination regarding the issuance of the authorization to operate.

5. Ongoing Authorization

Ongoing authorization[12] 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 organization's risk tolerance and mission/business requirements. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the near real-time state of the information system and inherited common controls to determine whether or not all applicable security and privacy requirements have been satisfied and the mission/business risk is acceptable. Effective ongoing authorization requires robust ISCM and PCM strategies and effective operational ISCM and PCM programs. Agencies can move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process for information systems and common controls after having satisfied two conditions: the system and/or common controls have been granted an initial authorization to operate by the designated authorizing official; and ISCM and PCM programs are in place to monitor all implemented security and privacy controls with the appropriate degree of rigor and at the appropriate frequencies in accordance with applicable ISCM and PCM strategies and OMB and NIST guidance.

Agencies must define and implement a process to specifically designate information systems and/or common controls that have satisfied the following two conditions and have been transitioned to ongoing authorization. The authorizing official formally acknowledges that the information system and/or common controls are being managed under an ongoing authorization process and accepts the responsibility for ensuring all necessary activities associated with the ongoing authorization process are performed. Until a formal approval is obtained from the authorizing official to transition to ongoing authorization, information systems (and common

[12] 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.*

controls) remain under a static authorization process with specific authorization termination dates enforced by the agency.

6. Reauthorization

Reauthorization consists of a review of the information system similar to the review carried out during the initial authorization but conducted during the operations/maintenance phase of the system development life cycle rather than prior to that phase. In general, reauthorization actions may be time-driven or event-driven. However, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that drives information security above the previously agreed-upon organizational risk tolerance. Changes in statutory requirements and OMB or NIST guidance may also trigger a reauthorization.

The reauthorization process differs from the initial authorization inasmuch as the authorizing official can initiate: a complete zero-base review of the information system or common controls; or a targeted review based on the type of event that triggered the reauthorization, the assessment of risk related to the event, the risk response of the organization, and the organizational risk tolerance. Reauthorization is a separate activity from the ongoing authorization process, though security- and privacy-related information from the organization'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.

7. Joint and Leveraged Authorizations

Agencies are encouraged to use joint and leveraged authorizations whenever practicable.[13] Joint authorizations can be used when multiple organizational officials either from the same organization or different organizations, have a shared interest in authorizing an information system or common controls. The participating officials are collectively responsible and accountable for the system and the common controls and jointly accept the information security risks that may adversely impact organizational operations and assets, individuals, other organizations, and the Nation. Organizations choosing a joint authorization approach should work together on the planning and the execution of the Risk Management Framework tasks described in NIST Special Publication 800-37 and document their agreement and progress in implementing the tasks. The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization including, for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only as long as there is mutual agreement among authorizing officials and the authorization meets the requirements established by Federal and/or organizational policies.

Leveraged authorizations can be used when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency based on the need to use the same information resources (e.g., information system and/or services provided by the system). The leveraging organization reviews the owning organization's authorization package as the basis for determining risk to the leveraging organization. The leveraging organization

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

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 organization. The leveraging organization may determine that additional security measures are needed and negotiate with the owning organization to provide such measures. To the extent that a leveraged authorization includes an information system that collects, processes, stores, maintains, transmits, or disseminates PII, leveraging organizations must consult their SAOP. The SAOP may determine that additional measures are required to protect PII prior to leveraging the authorization.

8. Continuous Monitoring

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

9. Critical Infrastructure

Agencies that operate information systems that are part of the critical infrastructure must employ organizational assessment and management of risk 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, organizations must ensure that the privacy controls assigned to critical infrastructure meet all applicable requirements and adequately protect individual privacy. This includes the ongoing monitoring of deployed security and privacy controls in critical infrastructure systems to determine the ongoing effectiveness of those controls against current threats; improving the effectiveness of those controls, when necessary; managing associated changes to the systems and environments of operation; and satisfying specific protection and compliance requirements in statutes, Executive Orders, directives, and policies required for critical infrastructure protection.

10. Encryption

Where technically feasible, agencies must encrypt Federal information at rest and in transit unless otherwise protected by alternative physical safeguards. Encrypting information at rest and in transit helps protect the confidentiality, integrity, and availability of such information by making it less susceptible to unauthorized disclosure or modification. Encryption requirements apply to Federal information categorized as either moderate or high impact in accordance with FIPS Publication 199. Only FIPS-validated and NSA-approved cryptography are approved for use in Federal information systems.

11. Digital Signatures

Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use. Additionally, digital signatures can help agencies streamline mission/business processes and transition manual processes to more automated processes to include, for example, online transactions. Because of the advantages provided by this technology, OMB expects agencies to implement digital signature capabilities in accordance with Federal Public Key Infrastructure (PKI) policy, and NIST standards and guidelines. For employees and contractors, agencies should require use the digital signature capability of the Personal Identity Verification (PIV) credentials.[14] For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures.

12. Identity Assurance

To streamline the process of citizens, businesses, and other partners[15] securely accessing government services online requires a risk-appropriate demand of identity assurance. Identity assurance, in an online context, is the ability of an agency to determine that a claim to a particular identity made by an individual can be trusted to actually be the individual's "true" identity. Citizens, businesses, and other partners that interact with the Federal Government need to have and be able to present electronic identity credentials to identify and authenticate themselves remotely and securely when accessing Federal information resources. An agency needs to be able to know, to a degree of certainty commensurate with the risk determination, that the presented electronic identity credential truly represents the individual presenting the credential before a transaction is authorized.[16]

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. In doing so, agencies are expected to leverage Federal shared services intended to allow a user to authenticate with multiple information systems across agencies by selecting from a set of interoperable credentials that are appropriate for the level of identity assurance required.

13. Unsupported Information System Components

Unsupported information system components (e.g., when vendors are no longer providing critical software patches) provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. For such systems, organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual

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

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

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

relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

14. FISMA Applicability to Nonfederal Entities

The Federal Information Security Modernization Act 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 which are either fully or partially provided, including agency hosted, outsourced, and cloud-based solutions.

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

15. Other Requirements

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

References[17]

1. Privacy Act of 1974 (P.L. 93-579), December 1974.
2. E-Government Act of 2002 (P.L. 107-347), December 2002.
3. Federal Information Security Modernization Act of 2014 (P.L. 113-283, Title II), December 2014.
4. Executive Order 13556, *Controlled Unclassified Information*, November 2010.
5. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.
6. Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.
7. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), *Standards for Security Categorization of Federal Information and Information Systems*.

[17] 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 200 (as amended), *Minimum Security Requirements for Federal Information and Information Systems*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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