CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

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

3. Applicability

The requirements of this Circular apply to the information resources management activities of all agencies[2] of the Executive Branch of the Federal Government. The requirements of this Circular apply to management activities concerning all information resources in any medium (unless otherwise noted), including paper and electronic information. When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements of this Circular is not shifted (to the service provider). Agencies shall describe the responsibilities of service providers in relevant agreements with the service providers. Agencies are not required to apply this Circular to national security systems (defined in 44 U.S.C. § 3552), but are encouraged to do so where appropriate. For national security systems, agencies shall follow applicable statutes, executive orders, directives, and internal agency policies.

4. Basic Considerations

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

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

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

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

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

[2] 'Agency' means any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.

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

a) Inventories

Agencies shall:

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

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

b) Information Management

Agencies shall:

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

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

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

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

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

3) Planning, Programming, and Budgeting

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

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

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

c) The agency head, in consultation with the CFO, CAO, CIO, and program leadership, shall define the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[13] The Federal Acquisition Streamlining Act of 1994 (Pub. L. 103-355) requires agencies to achieve, on average, ninety percent of the cost and schedule goals established for major and non-major acquisition programs of the agency without reducing the performance or capabilities of the items being acquired.

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

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

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

b) Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full life cycle costs of IT products and services, including but not limited to, planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements;[16]

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

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

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

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

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

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

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

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

2) Agency Approval

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

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

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

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

f) Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the Government has been selected.

4) Selection Criteria and Requirements

Agencies shall consider the following factors when analyzing IT investments:

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

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

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

d) Information systems security levels are commensurate with the impact that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information consistent with NIST standards and guidelines.

5) IT Investment Design and Management

Agencies shall implement the following requirements:

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

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

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

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

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

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

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

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

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

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

4) Agencies shall collect or create information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public, where appropriate, by creating or collecting all new information electronically by default, in machine-readable open formats, using relevant data standards, that upon creation includes standard extensible metadata in accordance with OMB guidance.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h. Records Management

Agencies shall:

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

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

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

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

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

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

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

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

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

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

i. Leveraging the Evolving Internet

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

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

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

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

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

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

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

b. Department of Homeland Security

The Secretary of Homeland Security shall:[42]

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

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

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

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

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

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

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

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

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

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

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

[43] FISMA, 44 U.S.C. § 3553(b)(1).

[44] FISMA, 44 U.S.C. § 3553(b)(2).

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

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

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

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

d. Federal Privacy Council

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

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

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

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

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

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

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

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

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

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

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

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

g. Office of Personnel Management

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

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

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

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

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

7. Effectiveness

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

8. Oversight

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

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

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

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

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

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

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

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

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

8) 'Authorization package' means the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

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

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

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

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

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

new technologies in response to changing mission needs; and (b) includes – (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan (44 U.S.C. § 3601).

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

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

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

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

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

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

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

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

28) 'Information' means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

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

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

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

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

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

41) ‘Information security program plan’ means a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

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

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

44) ‘Information system resilience’ means the ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

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

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

47) ‘Information Technology Investment Management’ means a decision-making process that, in support of agency missions and business needs, provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of

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

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

54) 'Ongoing authorization' means the risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency's mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.

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

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

57) 'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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

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