CIRCULAR NO. A-130

Revised, (Transmittal Memorandum No. 4)

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Management of Federal Information Resources

1. Purpose: This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2. Rescissions: This Circular rescinds OMB Memoranda M-96-20, “Implementation of the Information Technology Management Reform Act of 1996;” M-97-02, “Funding Information Systems Investments;” M-97-09, “Interagency Support for Information Technology;” M-97-15, “Local Telecommunications Services Policy;” M-97-16, "Information Technology Architectures”.

3. Authorities: OMB issues this Circular pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as “Information Technology Management Reform Act of 1996”) (Pub. L.

104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); the Computer Security Act of 1987 (Pub. L. 100-235); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); the Government Performance and Results Act of 1993(GPRA); the Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), Executive Order No. 12046 of March 27, 1978; Executive Order No. 12472 of April 3, 1984; and Executive Order No. 13011 of July 17, 1996.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

b. 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.

5. Background: The Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

1. focusing information resource planning to support their strategic missions;
2. implementing a capital planning and investment control process that links to budget formulation and execution; and
3. rethinking and restructuring the way they do their work before investing in information systems.

The PRA establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the PRA requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.

c. The term "capital planning and investment control process " means a management process for ongoing identification, selection, control, and evaluation of investments in information

resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

d. The term "Chief Information Officers Council" (CIO Council) means the Council established in Section 3 of Executive Order 13011.

e. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency 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 Privacy Act.

f. The term "executive agency" has the meaning defined in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

g. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.

h. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

i. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

j. The term "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, or audiovisual forms.

k. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

l. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

m. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

n. The term "information resources" includes both government information and information technology.

o. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

p. The term "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.

q. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

r. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

s. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

t. The term "Information Technology Resources Board" (Resources Board) means the board established by Section 5 of Executive Order 13011.

u. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

v. The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget document preparation requirements set forth in OMB Circular A-11. The resultant budget document may be classified in accordance with the provisions of Executive Order 12958.

w. The term "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)

x. The term "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))

y. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It 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 the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations..

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Strategic planning improves the operation of government programs. The agency strategic plan will shape the redesign of work processes and guide the development and maintenance of an Enterprise Architecture and a capital planning and investment control process. This management approach promotes the appropriate application of Federal information resources

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

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

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

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

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

r. The Chief Information Officers Council and the Information Technology Resources Board will help in the development and operation of interagency and interoperable shared information resources to support the performance of government missions.

8. Policy:

a. Information Management Policy

1. How will agencies conduct Information Management Planning?

Agencies must plan in an integrated manner for managing information throughout its life cycle. Agencies will:

(a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;

(b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;

(c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;

(d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;

(f) Train personnel in skills appropriate to management of information;

(g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;

(h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;

(i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

(j) 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) Incorporate records management and archival functions into the design, development, and implementation of information systems;

1. Provide for public access to records where required or appropriate.

2. What are the guidelines for Information Collection?

Agencies must collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

3. What are the guidelines for Electronic Information Collection?

Executive agencies under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide, by October 21, 2003, the (1) option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. Agencies will follow the provisions in OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act."

4. How must agencies implement Records Management?

Agencies will:

(a) Ensure that records management programs provide adequate and proper documentation of agency activities;

(b) Ensure the ability to access records regardless of form or medium;

(c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records; and

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

5. How must an agency provide information to the public?

Agencies have a responsibility to provide information to the public consistent with their missions. Agencies will discharge this responsibility by:

(a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts;

(c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and

(d) In determining whether and how to disseminate information to the public, agencies will:

(i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;

(ii) Disseminate information dissemination products on equitable and timely terms;

(iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

6. What is an Information Dissemination Management System?

Agencies will maintain and implement a management system for all information dissemination products which must, at a minimum:

(a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);

(b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;

(c) Establish and maintain inventories of all agency information dissemination products;

(d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;

(e) Identify in information dissemination products the source of the information, if from another agency;

(f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;

(g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);

(h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;

(i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination products that meet their respective needs;

(j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(k) Ensure 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.

7. How must agencies avoid improperly restrictive practices?

Agencies will:

(a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis;

(b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on

the reuse, resale, or redissemination of Federal information dissemination products by the public; and,

(c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They must exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:

(i) Where statutory requirements are at variance with the policy;

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

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

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

8. How will agencies carry out electronic information dissemination?

Agencies will use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

(a) The agency develops and maintains the information electronically;

(b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;

(c) The agency disseminates the product frequently;

(d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;

(e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

9. What safeguards must agencies follow?

Agencies will:

(a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains 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;

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

b. How Will Agencies Manage Information Systems and Information Technology?

(1) How will agencies use capital planning and investment control process?

Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide both strategic and operational IRM, IT planning, and the Enterprise Architecture by integrating the agency's IRM plans, strategic and performance plans prepared pursuant to the Government Performance and Results Act of 1993, financial management plans prepared pursuant to the Chief Financial Officer Act of 1990 (31 U.S.C. 902a5), acquisition under the Federal Acquisition Streamlining Act of 1994, and the agency's budget formulation and execution processes. The capital planning and investment control process includes all stages of capital programming, including planning, budgeting, procurement, management, and assessment.

As outlined below, the capital planning and investment control process has three components: selection, control, and evaluation. The process must be iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results (for further guidance on Capital Planning refer to OMB Circular A-11). The agency's capital planning and investment control process must build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture. The Capital Planning and Investment Control processes must be documented, and provided to OMB consistent with the budget process. The Enterprise Architecture must be documented and provided to OMB as significant changes are incorporated.

(a) What plans are associated with the capital planning and investment control process?

In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

The IT Capital Plan is operational in nature, supports the goals and missions identified in the IRM Strategic Plan, is a living document, and must be updated twice yearly. This IT Capital Plan is the implementation plan for the budget year. The IT Capital Plan should also reflect the goals of the agency's Annual Performance Plan, the agency's Government Paperwork

Elimination Act (GPEA) Plan, the agency's EA, and agency's business planning processes. The IT Capital Plan must be submitted annually to OMB with the agency budget submission. annually. The IT Capital Plan must include the following components:

(i) A component, derived from the agency's capital planning and investment control process under OMB Circular A-11, Section 300 and the OMB Capital Programming Guide, that specifically includes all IT Capital Asset Plans for major information systems or projects. This component must also demonstrate how the agency manages its other IT investments, as required by the Clinger-Cohen Act.

(ii) A component that addresses two other sections of OMB Circular A-11: a section for Information on Financial Management, including the Report on Financial Management Activities and the Agency's Financial Management Plan, and a section entitled Information Technology, including the Agency IT Investment Portfolio.

(iii) A component, derived from the agency's capital planning and investment control process, that demonstrates the criteria it will use to select the investments into the portfolio, how it will control and manage the investments, and how it will evaluate the investments based on planned performance versus actual accomplishments.

(iv) A component that includes a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance.

(b) What must an agency do as part of the selection component of the capital planning process?

It must:

(i) Evaluate each investment in information resources to determine whether the investment will support core mission functions that must be performed by the Federal government;

(ii) Ensure that decisions to improve existing information systems or develop new information systems are initiated only when no alternative private sector or governmental source can efficiently meet the need;

(iii) Support work processes that it has simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology;

(iv) Reduce risk by avoiding or isolating custom designed components, using components that can be fully tested or prototyped prior to production, and ensuring involvement and support of users;

(v) Demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. The return may include improved mission performance in accordance with GPRA measures, reduced cost, increased quality, speed, or flexibility; as well as increased customer and employee satisfaction. The return should reflect such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes;

(vi) Prepare and update a benefit-cost analysis (BCA) for each information system throughout its life cycle. A BCA will provide a level of detail proportionate to the size of the investment, rely on systematic measures of mission performance, and be consistent with the methodology described in OMB Circular No. A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs";

(vii) Prepare and maintain a portfolio of major information systems that monitors investments and prevents redundancy of existing or shared IT capabilities. The portfolio will provide information demonstrating the impact of alternative IT investment strategies and funding levels, identify opportunities for sharing resources, and consider the agency's inventory of information resources;

(viii) Ensure consistency with Federal, agency, and bureau Enterprise architectures, demonstrating such consistency through compliance with agency business requirements and standards, as well as identification of milestones, as defined in the EA;

(ix) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector;

(x) Ensure that the selected system or process maximizes the usefulness of information, minimizes the burden on the public, and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information, as determined in accordance with the PRA and the Federal Records Act. This portion must specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(xi) Establish oversight mechanisms, consistent with Appendix III of this Circular, to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data;

(xii) Ensure that Federal information system requirements do not unnecessarily restrict the prerogatives of state, local and tribal governments;

(xiii) Ensure that the selected system or process facilitates accessibility under the Rehabilitation Act of 1973, as amended.

(c) What must an agency do as part of the control component of the capital planning process?

It must:

(i) Institute performance measures and management processes that monitor actual performance compared to expected results. Agencies must use a performance based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality;

(ii) Establish oversight mechanisms that require periodic review of information systems to determine how mission requirements might have changed, and whether the information system continues to fulfill ongoing and anticipated mission requirements. These mechanisms must also require information regarding the future levels of performance, interoperability, and maintenance necessary to ensure the information system meets mission requirements

cost effectively;

(iii) Ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle. Information systems must also continue to deliver intended benefits to the agency and customers, meet user requirements, and identify and offer security protections;

(iv) Prepare and update a strategy that identifies and mitigates risks associated with each information system;

(iv) Ensure that financial management systems conform to the requirements of OMB Circular No. A-127, "Financial Management Systems;"

(v) Provide for the appropriate management and disposition of records in accordance with the Federal Records Act.

(vi) Ensure that agency EA procedures are being followed. This includes ensuring that EA milestones are reached and documentation is updated as needed.

(d) What must an agency do as part of the evaluation component of the capital planning process?

It must:

(i) Conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use;

(ii) Evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements.

(iii) Document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge.

(iv) Re-assess an investment's business case, technical compliance, and compliance against the EA.

(v) Update the EA and IT capital planning processes as needed.

(2) The Enterprise Architecture

Agencies must document and submit their initial EA to OMB. Agencies must submit updates when significant changes to the Enterprise Architecture occur.

(a) What is the Enterprise Architecture?

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle

methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with GPEA, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. Agencies must implement the EA consistent with following principles:

(i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;

(ii) Meet information technology needs through cost effective intra-agency and interagency sharing, before acquiring new information technology resources; and

(iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

(b) How do agencies create and maintain the EA?

As part of the EA effort, agencies must use or create an Enterprise Architecture Framework. The Framework must document linkages between mission needs, information content, and information technology capabilities. The Framework must also guide both strategic and operational IRM planning.

Once a framework is established, an agency must create the EA. In the creation of an EA, agencies must identify and document:

(i) Business Processes - Agencies must identify the work performed to support its mission, vision and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive changes in the EA.

(ii) Information Flow and Relationships - Agencies must analyze the information utilized by the agency in its business processes, identifying the information used and the movement of the information. These information flows indicate where the information is needed and how the information is shared to support mission functions.

(iii) Applications - Agencies must identify, define, and organize the activities that capture, manipulate, and manage the business information to support business processes. The EA also describes the logical dependencies and relationships among business activities.

(iv) Data Descriptions and Relationships - Agencies must identify how data is created, maintained, accessed, and used. At a high level, agencies must define the data and describe the relationships among data elements used in the agency's information systems.

(v) Technology Infrastructure - Agencies must describe and identify the functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.

(c) What are the Technical Reference Model and Standards Profile?

The EA must also include a Technical Reference Model (TRM) and Standards Profile.

(i) The TRM identifies and describes the information services (such as database,

communications, intranet, etc.) used throughout the agency.

(ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.

(iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

(3) How Will Agencies Ensure Security in Information Systems?

Agencies must incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems.

(a) To support more effective agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:

(i) Prioritize key systems (including those that are most critical to agency operations);

(ii) Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

(b) Agencies must make security's role explicit in information technology investments and capital programming. Investments in the development of new or the continued operation of existing information systems, both general support systems and major applications must:

(i) Demonstrate that the security controls for components, applications, and systems are consistent with, and an integral part of, the EA of the agency;

(ii) Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;

(iii) Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;

(iv) Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;

(v) Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;

(vi) Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

(vii) Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access;

(viii) Ensure that the handling of personal information is consistent with relevant government-wide and agency policies;

(ix) Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications;

(c) OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

(4) How Will Agencies Acquire Information Technology?

Agencies must:

(a) Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information technology;

(b) Structure major information systems 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;

(c) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes; and

(d) Ensure accessibility of acquired information technology pursuant to the Rehabilitation Act of 1973, as amended (Pub. Law 105-220, 29 U.S.C.794d).

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency must:

1. Have primary responsibility for managing agency information resources;

2. Ensure that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB;

3. Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to 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)), as well as Executive Order 13011. The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and will advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things:

(a) Be an active participant during all agency strategic management activities, including the

development, implementation, and maintenance of agency strategic and operational plans;

(b) Advise the agency head on information resource implications of strategic planning decisions;

(c) Advise the agency head on the design, development, and implementation of information resources.

(i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project;

(ii) Advise the agency head on budgetary implications of information resource decisions; and

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

4. Direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with this Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1st of each year.

5. Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

6. Develop agency policies and procedures that provide for timely acquisition of required information technology;

7. Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511) and the Freedom of Information Act (5 U.S.C. 552(g)): an inventory of the agency's major information systems, holdings, and dissemination products; an agency information locator service; 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 a handbook for persons to obtain public information from the agency pursuant to these Acts.

8. 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.

9. 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;

10. 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;

11. 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;

(b) promotes a coordinated, interoperable, secure, and shared government wide infrastructure that is provided and supported by a diversity of private sector suppliers; and

(c) develops a well-trained corps of information resource professionals.

12. Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization;

13. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,

14. 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 will 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.)

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

16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

b. Department of State. The Secretary of State must:

1. 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 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.

c. Department of Commerce. The Secretary of Commerce must:

1. Develop and issue Federal Information Processing Standards 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. Advise the Director of OMB on the development of policies relating to the procurement and management of Federal telecommunications resources;

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

4. Conduct studies and evaluations concerning telecommunications technology, and concerning 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;

5. 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;

6. 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;

7. 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.

d. Department of Defense. The Secretary of Defense will 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.

e. General Services Administration. The Administrator of General Services must:

1. Continue to manage the FTS2001 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 the 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. Be a liaison on information resources management (including Federal information technology) with State and local governments. GSA must also be a liaison with non-governmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5. Support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations on information resource management matters;

6. Provide support and assistance to the CIO Council and the Information Technology Resources Board.

7. Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act, as amended;

f. Office of Personnel Management. The Director, Office of Personnel Management, will:

1. Develop and conduct training programs for Federal personnel on information resources management, including end-user computing;

2. Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

3. Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States will:

1. Administer the Federal records management program in accordance with the National Archives and Records Act;

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

h. Office of Management and Budget. The Director of the Office of Management and Budget will:

1. Provide overall leadership and coordination of Federal information resources management within the executive branch;

2. Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

3. Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

4. Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

5. Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3;

6. Develop and maintain a Governmentwide strategic plan for information resources management.

7. Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

8. Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;

9. Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes;

10. Review proposed U.S. Government Position and Policy statements on international issues affecting Federal Government information activities, and advise the Secretary of State as to their consistency with Federal information resources management policy.

11. Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy, and policies regarding management of financial management systems with the Office of Federal Financial Management.

12. Evaluate agency information resources management practices and programs and, as part of the budget process, oversee agency capital planning and investment control processes to analyze, track, and evaluate the risks and results of major capital investments in information systems;

13. Notify an agency if OMB believes that a major information system project requires outside assistance;

14. Provide guidance on the implementation of the Clinger-Cohen Act and on the management of information resources to the executive agencies, to the CIO Council, and to the Information Technology Resources Board; and

15. Designate one or more heads of executive agencies as executive agent for government-wide acquisitions of information technology.

10. Oversight:

a. The Director of OMB will 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.

b. 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.

11. Effectiveness: This Circular is effective upon issuance. Nothing in this Circular will be construed to confer a private right of action on any person.

12. Inquiries: All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.

13. Sunset Review Date: OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.