Management of Federal Information Resources

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON D.C. 20503

THE DIRECTOR

OFFICE OF MANAGEMENT AND BUDGET

Management of Federal Information Resources

AGENCY: Office of Management and Budget, Executive Office of the President

ACTION: Revision of OMB Circular No. A-130, Transmittal No. 4.

SUMMARY: The Office of Management and Budget issues a revision to Circular No. A-130, "Management of Federal Information Resources," to implement provisions of the Clinger-Cohen Act (also known as AInformation Technology Management Reform Act of 1996" and for other purposes. The revision modifies sections of the Circular concerning information systems and information technology management to follow more closely provisions of the Clinger-Cohen Act and OMB Circular A-11. These sections involve the acquisition, use, and disposal of information technology as a capital asset by the Federal government to improve the productivity, efficiency, and effectiveness of Federal programs.

OMB has issued previous guidance regarding the Clinger-Cohen Act implementation, including 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;" and M-97-16, "Information Technology Architectures." As a convenience to readers, these Memoranda are rescinded and their content incorporated into this Circular.

This revision also incorporates the content of three other OMB Memoranda. The guidance in Memorandum M-98-09, on the handbook requirement of the 1996 Electronic FOIA Amendments, has been incorporated into Appendix IV. The guidance on "Implementing the Government Paperwork Elimination Act" (OMB Memorandum M-00-10) has been inserted in Appendix II, and the principles on "Incorporating and Funding Security in Information Systems Investments" (OMB Memorandum M-00-07) have been incorporated into Section 8b(4). Appendix IV has been expanded to reflect these changes. With its incorporation into the Circular, Memoranda M-98-09 is rescinded.

OMB intends to review this Circular in 2001 for other revisions including Information Policy, Security and Privacy. At that time, we will review the Circular generally and update it to reflect plain language principles.

AVAILABILITY: You can find a full recompiled version of Circular A-130, including the changes made here along with the existing sections that have not changed on the Internet at the OMB web site, http://obamawhitehouse.archives.gov/OMB/circulars/index.html and at the CIO Council home page at http://www.cio.gov. You can also obtain a copy of OMB Circular No. A-11, including the supplement to Part 3, "The Programming Guide," at the OMB web site and the CIO Council web site, or by calling the Budget Review and Concepts Division at OMB at 202-395-3172.

FOR FURTHER INFORMATION CONTACT: Tony Frater, Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236, New Executive Office Building, Washington, D.C. 20503. Telephone: (202) 395-3785.

SUPPLEMENTARY INFORMATION:

Background: The Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E, codified at 40 U.S.C. Chapter 25) grants to the Director of the Office of Management and Budget (OMB) authority to oversee the acquisition, use, and disposal of information technology by the Federal government, so as to improve the productivity, efficiency, and effectiveness of Federal programs. It supplements the information resources management (IRM) policies contained in the Paperwork Reduction Act (PRA) (44 U.S.C. Chapter 35) by establishing a comprehensive approach to improving the acquisition and management of agency information systems through work process redesign, and by linking planning and investment strategies to the budget process.

The Clinger-Cohen Act establishes clear accountability for IRM activities by creating agency Chief Information Officers (CIOs) with the authority and management responsibility necessary to advise agency heads on budget, program, and implementation issues concerning information technology. Among other responsibilities, CIOs oversee the design, development, and implementation of information systems. CIOs also monitor and evaluate system performance and advise agency heads whether to modify or terminate those systems. The Clinger-Cohen Act directs agencies to work together towards the common goal of using information technology to improve the productivity, effectiveness, and efficiency of Federal programs and to promote an interoperable, secure, and shared government-wide information resources infrastructure.

OMB Circular No. A-130, "Management of Federal Information Resources," contains the policy framework for the management of Federal information resources. OMB last revised Circular A-130 on February 20, 1996 (61 FR 6428). To provide agencies with additional guidance on implementing the

Clinger-Cohen Act, and for other purposes, OMB on April 13, 2000 (65 FR 19933) requested public comment on a proposed revision to this Circular. In addition to publishing the proposed revision in the Federal Register, OMB posted it on its public web site and sent copies of the proposal directly to Federal agencies.

Comments on the Proposed Revision to Circular A-130

In response to the request for public comment, OMB received specific comments from thirty four organizations and individuals. Federal agencies submitted the majority of comments, but non-profit organizations and concerned citizens also responded. Most comments proposed changes in clarity and detail. Where these comments added clarity and did not conflict with the substance of the provision in question, OMB incorporated them. Several organizations suggested changes to parts of the Circular that are not within the scope of this update of the Circular. OMB intends to review Circular No. A-130 for other revisions in 2001.

We describe below the principal substantive issues raised in the comments and our responses to them.

1. Comments regarding the IT Capital Plan

A number of agencies wanted greater clarification regarding the distinction between the Information Technology (IT) Capital Plan and the Information Resources Management (IRM) Strategic Plan. We have updated the section outlining the IT Capital Plan and the IRM Strategic Plans. The new section describes in much greater detail, and in so doing clarifies, the different objectives of the two plans: the IT Capital Plan is operational in nature while the IRM Strategic Plan is a long range planning document.

The IRM Strategic Plan is the agency's IT vision or roadmap that will align its information resources with its business strategies and investment decisions. As an example, the IRM Strategic Plan might include the mission of the agency, key business processes, IT challenges, and guiding principles.

Conversely, the IT Capital Plan provides the justification for individual assets. A sample IT Capital Plan would include: the business case, expected benefits and costs, schedule, return on investment analysis, performance measures to evaluate the effectiveness of the investment, an examination of the alternative solutions, an acquisition strategy, and a discussion of how that system comports with IT security and privacy guidance.

The Government Performance and Results Act requires agencies to develop and submit to OMB agency Strategic Plans. Each agency submits this information annually along with its Performance Plans, as part of its budget submission to OMB. IRM Strategic Plans should support the Agency Strategic Plans, describing how information resources will help accomplish agency missions and ensuring that IRM decisions are integrated with organizational planning, budget, financial management, procurement, human resources management, and program decisions. The IT Capital Plan, on the other

hand, supports the goals and missions identified in the IRM Strategic Plan, is an operational document, and is updated twice yearly. The IT Capital Plan is largely comprised of existing documents that accompany the agency budget submission, as updated to reflect the Presidential budget request to Congress. The updated IT Capital Plan becomes the implementation plan for the budget year.

2. Comments on the relationship between the agency Enterprise Architecture and the agency capital planning and investment control process

Several agencies wanted further elaboration on how the Enterprise Architecture (EA) and the capital planning and investment control (CPIC) process should work together. To address these comments, we include information on the EA within the body of Section 8b and elaborate on its relationship with the capital planning and investment control process. In doing so, information contained in the proposed Appendix II regarding the EA (April 13, 2000 (65 FR 19933)) has been incorporated into Section 8b(2). Appendix II is now dedicated to information on implementing the Government Paperwork Elimination Act.

We also add a discussion that describes how the EA documents linkages between mission needs, information sources and content, and information technology capabilities. The EA should inform the CPIC process by defining the technologies and information critical to operating an agency's business, and by creating a roadmap which enables the agency to transition from its current to its targeted state. The EA helps the agency respond to changing business needs, and ensures that potential solutions support the agency's targeted state. A proposed IT solution that does not comply with the EA should not be considered as a possible investment, and should not enter the CPIC process. The CPIC process helps select, control and evaluate investments that conform with the EA.

For example, during the select stage of capital planning an agency identifies and investigates different potential solutions for an investment. An agency then selects the option with the best business case. If any of these alternatives does not conform with the EA, the agency should drop it from consideration.

Another example might include an agency considering a new financial management system. The new system will require users to have a certain computing environment in order to operate the proposed system. During the select stage of capital planning, the agency should review the EA to determine if that proposed system design is appropriate for all of the necessary users in the organization. Users in field offices, for example, may not have the computing resources to use the system. The agency must consider the costs of upgrading these users' computing resources in the evaluation of this alternative. If the system is selected, the agency must incorporate, into the EA, its impact on business processes, data, security, etc.

There were also comments regarding how the Federal Enterprise Architecture (FEA) framework relates to the agency Enterprise Architecture. The Chief Information Officers Council created and currently

maintains the FEA. We discuss the FEA in Appendix IV; agencies should address the Federal framework when developing the agency-specific EA. Collaboration among agencies who share a common business function promotes information sharing and is critical for the creation of a responsive, customer-focused electronic government.

3. Comments on the threshold for a major information system

A few agencies wanted OMB to create a dollar threshold for major information systems. We did not adopt this recommendation.

Since 1985, OMB has included in Circular A-130 a definition for what is a "major information system" (50 FR 52730, 52735; December 24, 1985.) Since its revision in 1994, the Circular has defined "major information system" as follows: "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" (59 FR 37906, 37909; July 25, 1994.) As this definition indicates, whether an information system qualifies as "major" depends on the particular circumstances of that system and its context within the agency's operations. Therefore, an information system that is "major" for one agency may not necessarily be "major" for another agency. This determination is to be made by the respective agency, and this determination necessarily involves an exercise of judgment.

Because there is significant variance among agency information technology budgets, we think it is inadvisable to establish a uniform, one-size-fits-all dollar threshold across all agencies, and therefore we have not done so.

4. Comments on Data Quality concerns

A few organizations inquired about the quality of Federal data. Ensuring the quality of the information that the Federal Government disseminates to the public is very important. Federal agencies must take seriously their responsibility to ensure the quality of their data. OMB works with the agencies to ensure the quality of Federally disseminated information in several ways, including the review of collections of information under the Paperwork Reduction Act (to ensure that collections "maximize usefulness"), statistical coordination and review, and the establishment in this Circular of general policies for information dissemination. The current Analysis of Key Sections in Appendix IV stresses the importance of data quality protections. OMB intends to review data quality policies in 2001 and to issue new guidance as appropriate.

5. Comments on Computer Security

Several agencies inquired about changes regarding computer security and privacy. OMB Memorandum M-00-07 "Incorporating and Funding Security in Information Systems Investments" (February 28, 2000) is incorporated into Section 8b(3).

Of special note, Title X, Subtitle G, "Government Information Security Reform" of the FY 2001 Defense Authorization Act (P.L. 106-398), was enacted during the final stages of revision to this Circular. In order to include these reforms, and other important computer security modifications, we plan more substantive changes when we revise Circular A-130 in 2001. During the upcoming revision process, we will take into consideration the comments that we have received on computer security.

6. Comments on information dissemination and information resources management

One organization suggested we add to Section 9 "Assignment of Responsibilities" a provision to reflect Section 5403 of the Clinger Cohen Act (40 U.S.C. 1503). Section 5403 requires agencies, in the designing of IT systems for disseminating information to the public, to reasonably ensure that an index of information disseminated by the system is included in the directory, created by the Superintendent of Documents pursuant to 44 U.S.C. 4101. OMB has included a new Section 9a(14) to reiterate Section 5403.

One organization expressed concern that language in Appendix IV (Sections 8a(5) and 8a(6)) describing agency requirements for the Government Information Locator Services (GILS) could lead to agency non-compliance with those requirements. OMB expects all agencies to comply with the information dissemination provisions of the PRA and of the E-FOIA Amendments to the Freedom of Information Act. In this regard, in accordance with the PRA (44 U.S.C. 3511) and the FOIA (5 U.S.C. 552(g)), each agency must develop and make available to the public (including through the Government Information Locator Service) an inventory that includes the agency's major information systems.

In addition, with respect to the "information resources management" responsibilities of each agency under the PRA (44 U.S.C. 3506(b)), OMB continues to believe that an agency needs to focus its management attention on its "major" information systems. For this reason, an agency's management of its information resources is best improved by having the agency maintain an inventory of its "information resources" that includes those major information systems (rather than all of the agency's information systems).

In sum, in addition to reflecting the passage of the E-FOIA Amendments, the revisions to Section 9 also clarify the agency obligations under the PRA and FOIA. These revisions reiterate that each agency must maintain and disseminate an inventory of its major information systems (these systems may be electronic or paper -- the Circular's definition of "major information systems" is format neutral). The revisions also clarify that, under the "information resources management" responsibilities in Section

3506(b)(4) of the PRA, each agency needs to maintain an inventory of its other "information resources" (such as personnel and funding) at the level of detail that the agency's managers believe is most appropriate for use in the agency's management of its information resources.

Because this revised Circular A-130 is not being reprinted here in its entirety, changes from the previous version are provided below. A copy of the recompiled Circular (consisting of the February 1996 Circular and the amendments in this notice) is available on OMB's web site (see "Availability" above).

Section 3. **Authorities.** This section is amended to cite and to incorporate changes necessitated by the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), and Executive Order 13011.

Section 5**. Background.** A discussion of the basic principles and goals of the Clinger-Cohen Act is added.

Section 6. **Definitions.** The terms "Chief Information Officers Council" and "Information Technology Resources Board" are introduced to reflect the interagency support structures established by Executive Order 13011. The terms "executive agency" and "national security system" are introduced to reflect the definitions found in the Clinger-Cohen Act. The term "information technology" is amended to reflect definitional changes made by the Clinger-Cohen Act, and is supplemented by the limiting term "national security system" to clearly identify those systems to which the Circular applies. The term "capital planning and investment control process" is introduced to assist agencies in the reporting requirements of the Clinger-Cohen Act.

Section 7. **Basic Considerations and Assumptions**. The existing basic considerations and assumptions are supplemented with a modified subsection (i) and new subsection (r) to reflect the relevant goals and purposes of the Clinger-Cohen Act and Executive Order 13011.

Section 8b. **Policy. Information Systems and Information Technology Management.** This section is substantially revised to implement the policies of the Clinger-Cohen Act and the principles of Executive Order 13011. Previous subsections (8b(1)-8b(5)) have been merged and revised to integrate requirements under Clinger-Cohen Act, the Government Performance and Results Act (Pub. L. 103-62), and revisions to OMB Circular A-11.

Section 9a, **All Federal Agencies,** is changed to reflect the new Chief Information Officer (CIO) position created by the Clinger-Cohen Act, and reflects developments since the Circular was last revised in February 1996

Section 9b, Section 9c, Section 9e, Section 9h, are revised to reflect responsibilities described in the Clinger-Cohen Act and Executive Order 13011.

Accordingly, OMB revises Circular A-130 as set forth below, and rescinds OMB Memoranda M-96-20, M-97-02, M-97-09, M-97-15, M-97-16, and M-98-09.

Jacob J. Lew
Director

---

1. Section 3, "Authorities," is revised to read as follows:

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.

2. Section 5, "Background," is revised to read as follows:

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.

3. Section 6, "Definitions," is revised by adding five new definitions (c,d,f,t, and v, below); revising the definition of "information technology"; and redesignating the remaining definitions accordingly:

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.

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)).

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.

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.

4. Section 7, "Basic Considerations and Assumptions," is amended by revising Section 7i, and by adding Section 7r, as follows:

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.

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.

5. Section 8b is revised to read as follows:

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).

6. Section 9a is revised to read as follows:

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;

1. 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.
2. 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;
3. Develop agency policies and procedures that provide for timely acquisition of required information technology;
4. 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.
5. Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.
6. Identify to the Director of OMB any statutory, regulatory, and other impediments to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;
7. Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

8. Ensure that the agency:

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

   (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.

1. 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;
2. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,
3. 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.)
4. 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;
5. 16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

7. Section 9b is revised to read as follows:

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.

8. Section 9c is revised by revising subparagraph 1, as follows:

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;

9. Section 9e is revised to read as follows:

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;

10. Section 9h is revised by deleting subparagraph (10), renumbering subparagraphs (11) and (12) as (10) and (11), and adding the following new subparagraphs:

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

1. 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;

2. Notify an agency if OMB believes that a major information system project requires outside assistance;
3. 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
4. Designate one or more heads of executive agencies as executive agent for government-wide acquisitions of information technology.

11. Appendix II to Circular A-130, which was formerly reserved, now incorporates OMB's guidance on the Government Paperwork Elimination Act (OMB Memorandum M-00-10; April 25, 2000); published at 65 FR 25508-21 (May 2, 2000).

In addition to referencing 65 FR 25508-21, readers may also find a full text of the GPEA guidance on the Internet at the OMB web site, http://obamawhitehouse.archives.gov/OMB/memoranda/index.html and at the CIO Council home page at **http://cio.gov**.

12. Appendix IV of Circular A-130, is revised by revising section 1 and 2, and by adding supplemental discussions regarding Section 8(a)(5), 8(b), 9(a)(3), and 9(a)(4) of the Circular, as follows:

1. Purpose

The purpose of this Appendix is to provide a general context and explanation for the contents of the key Sections of the Circular.

2. Background

The Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996" (Pub. L. 104-106, Division E, codified at 40 U.S.C. Chapter 25) grants to the Director of the Office of Management and Budget (OMB) various authorities for overseeing the acquisition, use, and disposal of information technology by the Federal government, so as to improve the productivity, efficiency, and effectiveness of Federal programs. It supplements the information resources management (IRM) policies contained in the Paperwork Reduction Act (PRA) (44 U.S.C. Chapter 35).

The Paperwork Reduction Act (PRA) of 1980, Public Law 96-511, as amended by the Paperwork Reduction Act of 1995, Public Law 104-13, codified at Chapter 35 of Title 44 of the United States Code, establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. Section 3504 authorizes the Director of OMB to 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 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.

The Circular implements OMB authority under the PRA with respect to Section 3504(b), general information resources management policy, Section 3504(d), information dissemination, Section 3504(f), records management, Section 3504(g), privacy and security, and Section 3504(h), information technology. The Circular also implements certain provisions of the Privacy Act of 1974 (5 U.S.C. 552a); the Government Paperwork Elimination Act. (Pub. L. 105-277, Title XVII); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949, as amended (40 U.S.C. 759 and 487, respectively); the Computer Security Act (40 U.S.C. 759 note); the Budget and Accounting Act of 1921 (31 U.S.C. 1 et seq.); and Executive Order No. 12046 of March 27, 1978, and Executive Order No. 12472 of April 3, 1984, Assignment of National Security and Emergency Telecommunications Functions. The Circular complements 5 CFR Part 1320, Controlling Paperwork Burden on the Public, which implements other Sections of the PRA dealing with controlling the reporting and recordkeeping burden placed on the public.

3. Analysis

Sections 8a(5) and 8a(6). Information Dissemination Policy.

Section 8a(5). As described in Section 11 of the "Electronic Freedom of Information Act Amendments of 1996" (Pub. L. 104-231), 5 U.S.C. 552(g), an agency must place its index and description of major information and record locator systems in its reference material or guide. We expect that this index and description would include an agency's Government Information Locator Service (GILS) presence as well as any other major information and record locator systems the agency has identified.

In addition, each agency should prepare a handbook that describes in one place the various ways by which a person can obtain public information from the agency, as well as the types and categories of information available. In preparing the handbook, each agency should review the dissemination policies contained in this Circular. The handbook should be in plain English and user-friendly. Where applicable, it should indicate that the public is encouraged to access information electronically via the agency's home page or to search in its reading room, and that the public may also submit a request to the agency under the Freedom of Information Act. "Types and categories" of available information will vary from agency to agency, and agencies should describe their information resources in whatever manner seems most appropriate.

Although the law does not require that the handbook be available on-line, OMB encourages agencies to do so as a matter of policy. The handbook should include the following elements:

1. The location of reading rooms within the agency and within its major field offices, as well as a brief description of the types and categories of information available.
2. The location of the agency's World Wide Web home page.
3. A reference to the agency's FOIA regulations and how to get a copy.
4. A reference to the agency's FOIA annual report and how to get a copy.
5. The location of the agency's GILS page.
6. A brief description of the types and categories of information generally available from the agency.

In addition, if there is an on-line version, it should have electronic links to these elements wherever they exist.

Every agency has a responsibility to inform the public within the context of its mission. This responsibility requires that agencies distribute information at the agency's initiative, rather than merely responding when the public requests information.

Section 8b. Information Systems and Information Technology Management

Section 8b(1). Capital planning and investment control.

What is the capital planning and investment control process?

The capital planning and investment control process is a systematic approach to managing the risks and returns of IT investments. The process has three phases: select, control and evaluate. The process covers all stages of capital programming, including planning, budgeting and procurement. For additional information describing capital planning, please consult Circular A-11.

What will happen if I don't maintain an IT Capital Plan?

The IT Capital Plan is the document that demonstrates to the agency Investment Review Board and to OMB officials, that a project deserves Federal funds. If the agency does not provide this information, merits of the project can not be determined.

As part of the agency IT Capital Plan, do I need to report on both development, modernization and enhancement (DME) as well as Steady State investments?

Yes. Additional information is provided in Part 3 of OMB Circular No. A-11, "Planning, Budgeting, and Acquisition of Capital Assets."

As part of the portfolio view of the agency IT Capital Plan, do I only need to report on major investments?

In accordance with the Clinger-Cohen Act and Circular A-11, agencies are required to manage all investments. They must also provide OMB with individual IT Capital Plans for major projects, as well as significant projects at the request of OMB.

Where can I get more information about return on investment (ROI)?

Agencies that would like to learn more about compiling and demonstrating projected return on investments (ROI) are encouraged to consult the Federal CIO Council document "ROI and the Value Puzzle". This document may be obtained at the CIO Council's web page (www.cio.gov).

Why do agencies need to conduct a Benefit-Cost Analysis?

Benefit-cost analyses provide vital management information on the most efficient allocation of human, financial, and information resources to support agency missions. Agencies should conduct a benefit-cost analysis for each information system to support management decision making to ensure: (a) alignment of the planned information system with the agency's mission needs; (b) acceptability of information system implementation to users inside the Government; (c) accessibility to clientele outside the Government; and (d) realization of projected benefits. When preparing benefit-cost analyses to support investments in information technology, agencies should seek to quantify the improvements in agency performance results through the measurement of program outputs.

The requirement to conduct a benefit-cost analysis need not become a burdensome activity for agencies. The level of detail necessary for such analyses varies greatly and depends on the nature of the proposed investment. Proposed investments in "major information systems" as defined in this Circular require detailed and rigorous analysis. This analysis should not merely serve as budget justification material, but should be part of the ongoing management oversight process to ensure prudent allocation of scarce resources. Proposed investments for information systems that are not considered "major information systems" can be analyzed more informally.

While it is not necessary to create a new benefit-cost analysis at each stage of the information system life cycle, it is useful to refresh these analyses with up-to-date information to ensure the continued viability of an information system prior to and during implementation. Reasons for updating a benefit-cost analysis may include such factors as significant changes in projected costs and benefits, significant changes in information technology capabilities, major changes in requirements (including legislative or regulatory changes), or empirical data based on performance measurement gained through prototype results or pilot experience.

How will portfolio management aid in the selection of investments?

Agencies must also weigh the relative benefits of proposed investments in information technology across the agency. Given the fiscal constraints facing the Federal government, agencies should fund a

portfolio of investments across the agency that maximizes return on investment for the agency as a whole. Agencies should also emphasize those proposed investments that show the greatest probability (i.e., display the lowest financial and operational risk) of achieving anticipated benefits for the organization.

Is there a preferred model for information life cycles?

The policy statements in this Circular describe an information system life cycle. It does not, however, make a definitive statement that there must be, for example, four versus five phases of a life cycle because the life cycle varies by the nature of the information system. Only two phases are common to all information systems - a beginning and an end.

While each phase of an information system life cycle may have unique characteristics, the dividing line between the phases may not always be distinct. For instance, both planning and evaluation must continue throughout the information system life cycle. In fact, during any phase, it may be necessary to revisit the previous stages based on new information or changes in the environment in which the system is being developed.

Why are post-implementation reviews necessary?

Agencies will complete a retrospective evaluation of information systems once operational to validate projected savings, changes in practices, and effectiveness in serving stakeholders. These post-implementation reviews may also serve as the basis for agency-wide learning about effective management practices.

Section 8b(2). Enterprise Architectures.

How will the EA guide the agency?

An EA should guide the agency's management of information resources for agency-wide information and information technology needs consistent with Section 8b(2) of this Circular. The EA will help the agency cope with technology and business change by serving as a reference for updates to existing and new information systems. The EA will also assure interoperability of business processes, data, applications and technology as agencies integrate proposed information systems projects with one another and with existing legacy systems.

Where can I get more information describing the EA?

Agencies that require additional information on developing or maintaining an EA are encouraged to consult the Federal CIO Council document entitled, "The Federal Enterprise Architecture (FEA) Framework," which is available on the CIO Council's web site (http://cio.gov). The Architecture Plus

web site (http://www.itpolicy.gsa.gov/mke/archplus/archhome.htm>) also has a number of useful documents.

What is an open systems environment?

An open system should be based on an architecture with published or documented interface specifications that have been adopted by a standards settings body.

What Enterprise Architecture issues must an agency consider that have government-wide or multiple agency implications?

The CIO Council has begun to address this issue in its "Federal Enterprise Architecture Framework (FEAF), Version 1.0," and subsequent versions. The FEAF was created to promote shared development for common Federal processes, interoperability, and sharing of information among the agencies of the Federal government and other governmental entities, as required by the Clinger-Cohen Act. The FEAF is recommend for use in (1) Federal government-wide efforts, (2) multi-Federal agency (2 or more agencies) efforts and, (3) whenever Federal business-areas and substantial Federal investment are involved with international, state, or local governments. The Federal Enterprise Architecture Framework, Version 1.0, which is a conceptual model, begins the process of defining a better documented and coordinated structure for cross-cutting businesses and technology developments in the government. Collaboration among agencies who share a common business function promotes information sharing and is a prerequisite for the creation of a responsive electronic government.

Where can I get more information on Federal EA efforts?

Some other examples of ongoing Federal government efforts in this arena are Treasury Enterprise Architecture Framework (TEAF) and Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR).

Section 8b(3) Securing Agency Information Systems

How should agencies incorporate security into management of information resources?

Effective security is an essential element of all information systems. A process assuring adequate security must be integrated into the agency's management of information resources. This process should be a component of the both capital planning process and the EA. A system's security requirements must be supported by the agency EA in order for it to be considered during the select phase of the capital planning process. Agencies will use the control and evaluate phases of capital planning to ensure these security requirements are met throughout the system's life cycle. For more information on computer security please read Appendix III of this Circular.

Ultimately, who determines the acceptable level of security for a system?

Each agency program official must understand the risk to systems under their control. They are also responsible for determining the acceptable level of risk, ensuring adequate security is maintained to support and assist the programs under their control, ensuring that security controls comport with program needs and appropriately accommodate operational necessities. In addition, program officials should work in conjunction with Chief Information Officers and other appropriate agency officials so that security measures support agency information architectures.

Section 8b(4) Acquiring Information Technology

What should agencies consider before acquiring a COTS solution?

Commercial-off-the-shelf (COTS) products can provide agencies a cost effective and efficient solution. However, often COTS products require customization for seamless use. Therefore agencies must still thoroughly examine the impact of a COTS product selection. A lessons-learned guide describing the risks of COTS products has been published by the Information Technology Resources Board (ITRB). The guide, entitled "Assessing the Risks of Commercial-Off-The-Shelf (COTS) Applications," is available on the ITRB web site (http://www.itrb.gov).

Section 9a(3). Chief Information Officer (CIO).

To whom does the CIO report?

Each agency must appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who will report directly to the agency's head to carry out the responsibilities of the agency under the PRA.

What is the CIO's role in the capital planning process?

The CIO will ensure that a capital planning process is established and rigorously used to define and validate all information resource investments. Through this process, the CIO will monitor and evaluate the performance of the information technology portfolio of the agency and advise the agency head on key budget, program, and implementation issues concerning information technology.

Additionally, the CIO will help establish a board composed of senior level managers, including the Chief Financial Officer and Chief Procurement Executive, who will have the responsibility of making key business recommendations on information resource investments, and who will be continuously involved. Many agencies will institute a second board, composed of program or project level managers, with more detailed business and information resource knowledge. They will be able to provide technical support to the senior level board in proposing, evaluating, and recommending information resource investments.

What is the CIO's role in the annual budget process?

The CIO will be an active participant during all agency annual budget processes and strategic planning activities, including the development, implementation, and maintenance of agency strategic plans. The CIO's role is to provide leadership and a strategic vision for using information technology to transform the agency. CIO's must also ensure that all information resource investments deliver a substantial mission benefit to the agency and/or a substantial return on investment (ROI) to the taxpayer.

Additionally, the CIO will ensure integration of information resource planning processes and documentation with the agency's strategic, performance and budget process, in coordination with the CFO and Procurement Executive.

Section 9a(4).

Why is the CIO considered an Ombudsman?

The CIO designated by the head of each agency under 44 U.S.C. 3506(a) is charged with carrying out the responsibilities of the agency under the PRA. Agency CIOs are responsible for ensuring that their agency practices are in compliance with OMB policies. It is envisioned that the CIO will work as an ombudsman to investigate alleged instances of agency failures to adhere to the policies set forth in the Circular and to recommend or take corrective action as appropriate. Agency heads should continue to use existing mechanisms to ensure compliance with laws and policies.