GAO

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

May 23, 2000

Mr. Jacob J. Lew
Director
Office of Management and Budget
New Executive Office Building
725 17th Street, NW
Washington, DC 20503

Subject: Revisions to OMB's Circular A-130

Dear Mr. Lew:

This letter provides our comments on the proposed revision of Office of Management and Budget (OMB) Circular A-130, as published in the *Federal Register* on April 13, 2000.

The proposed revision is an important step toward the incorporation of the language and intention of the Clinger-Cohen Act (Public Law 104-106, Division E, codified at 40 U.S.C. Chapter 25) into OMB guidance regarding the management of information resources in the federal government. We concur with the proposal's emphasis on the institutionalization of strong information technology (IT) management practices and the creation of a strong Chief Information Officer (CIO) as an active participant in all agency strategic management activities. In addition, the emerging focus on the enterprise architecture and its role in guiding the development of new information systems is consistent with GAO's position on the topic. We are specifically encouraged by the revision's requirements that

- Agencies establish and maintain a capital planning and investment control process that links mission needs, information, and technology in an effective and efficient manner;
- Agencies include in their strategic information resources management (IRM) plan a component summarizing the agency's security plan;
- Agencies include, as part of their capital planning process, references to processes used to that assure adherence to fundamental selection, control, and evaluation activities;
- Agencies adopt a portfolio management approach to information systems investment decision-making and provide information about the impact of alternative IT investment strategies and funding levels;
- Agencies create an information technology architecture that documents linkages among mission needs, information content, and information technology capabilities.

Changes to the proposed revisions are needed in four general areas that are critical to ensuring that agencies have the capability to manage their information resources investments effectively and efficiently. In addition, we address the need to ensure coordinated

implementation of the Paperwork Reduction Act (PRA) (44 U.S.C. Chapter 35) with the Clinger-Cohen Act (CCA).

Capital Planning and Investment Management

The increased emphasis on IT capital planning and investment management in agencies addresses the lack of adequate attention to it in the current version of Circular A-130. In general, the proposed changes align with existing guidance offered by OMB and GAO.[1] However, three specific attributes associated with both the OMB guidance and the GAO guidance require further attention in the revised circular. The following changes are needed:

- Circular A-130 should include a requirement that agencies ensure that full funding is requested for useful segments, or for the entire project if it is not divisible into useful segments. A useful segment is either a planning segment or a separate segment of the asset for which benefits exceed costs even if no further funding is appropriated. This requirement is included in Circular A-11, to which Circular A-130 makes reference, but a specific reference in Circular A-130 would reinforce of the importance of this practice to the IT capital planning community.
- Agencies should provide guidance for selecting, controlling, and evaluating all IT projects. This does not mean that all IT investment projects need to be subjected to the same justification processes or management review as one would expect for major investment initiatives. The revised Circular A-130 only specifies that capital planning processes are required for major projects. At many agencies that can exclude as much as, if not more than, 70 percent of the total IT budget.
- The requirement for "periodic" reviews of projects is unclear. We believe that it is important to specify that reviews should occur at regular intervals and when established performance criteria are met (such as milestones) or exceeded (such as spending limits or cost estimates).

Appointment and Responsibilities of the Chief Information Officer (CIO)

References to CIO appointments and responsibilities in the proposed Circular A-130 are, in some cases, incomplete or inconsistent with existing laws and executive orders. The evolution from designated senior official with responsibility for IRM, as specified in the original PRA, to Chief Information Officer in the CCA is a significant acknowledgement of the expanding importance of information in the federal government. The recognition that departments and agencies should appoint a senior executive with primary responsibility for carrying out information management-related duties should be captured in the revised Circular A-130. At the same time, however, not all CIOs are assigned the same responsibilities under the law. It would be helpful if the revised Circular A-130 reference the differences and describe the responsibilities accordingly.

The following changes to the proposed revisions are needed:

[1] Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making (GAO/AIMD-10.1.13, Version 1, February, 1997); and Capital Programming Guide, Version 1.0, Supplement to Office of Management and Budget Circular A-11, Part 3: Planning, Budgeting, and Acquisition of Capital Assets, July 22, 1997.

- The reference only to the list of CIOs in Executive Order 13011 is too limited. The Executive Order list refers to specific CIOs who make up the membership of the federal CIO Council and to certain agencies with specific responsibilities assigned by the President. The CCA created CIOs for all agencies and assigned additional responsibilities beyond those assigned by the PRA to certain agencies. Accordingly, proposed section 9.a.3 should reference responsibilities of agencies provided by the PRA and the CCA, as well as E.O. 13011. (See enclosure, issue 4 for further explanation of this point.)
- CIOs of the 24 major CFO Act agencies should have IRM as their primary duty as specified in the CCA. This CCA requirement was not included in proposed Section 9a. Those agencies should not have "dual" or "multi-hatted" CIOs.
- Responsibilities of CIOs created in agency subcomponents and in non-CFO Act agencies should be consistent with all of the requirements of the CCA. Even though the Act does not apply to these positions, the guidance is valuable and applicable.

Requirements of the Paperwork Reduction Act

It appears that in the attempt to make the requirements of Circular A-130 congruent with the requirements of the CCA some of the specific requirements of the PRA have not been addressed. The CCA built upon the existing statutory and policy framework for the management of information; it did not negate the provisions of the PRA. In particular, while the CCA created a new definition of information technology for its purposes and called for the institutionalization of IT capital planning, these changes do not replace the definitions or planning processes specified in PRA. Likewise, definitions of information resources inventories specified in PRA and elsewhere should be reconciled and explained within the revised Circular A-130. Specifically the following changes to the revised circular are needed:

- The distinction between IT capital planning and IRM planning required under the PRA is not addressed; particularly, the notion of the information lifecycle is not readily apparent. Capital planning under Circular A-11 would not appear to satisfy the PRA requirement for IRM planning. (See enclosure, issues 2 and 3 for further explanation of this point.)
- The current definition of "information technology" in section 6(p) of the circular reflects the PRA's definition of information technology, which exempts national security systems (44 U.S.C. 3502(9)). The proposed revision replaces that exemption with a separate definition that references the CCA's multi-part national security exemption. The proposed revisions to the circular do not, however, provide any guidance on the breadth of the CCA exemption in the context of the complete exemption still in effect under the PRA. (See enclosure, issue 1 for further explanation of this point.)
- The reference to information resources inventory requirements is internally inconsistent in the revised language. OMB calls for agency inventories to include only "major" information systems. This advice is consistent with PRA section 3511 which calls for agencies to make public an inventory of their major systems. However, PRA section 3506(b)(4) calls for each agency to "maintain a current and complete inventory of the agency's information resources," including those needed to satisfy section 3511. In line with that provision, OMB appears to support a complete inventory in proposed section 8b(2), where it states that an agency information technology architecture "should be supported by a complete inventory of the agency information resources." OMB should

resolve this apparent contradiction in the guidance by stating clearly its advice vis-a-vis the information resources inventory. (See enclosure, issue 5 for further explanation of this point.)

Software Change Control

We are aware that Appendix III, *Security of Federal Automated Information Resources*, of Circular A-130 is not proposed for revision at this time. However, recent work we have done has raised concerns about software change control to the point that we believe changes to Circular A-130 are essential.[2]

Currently, Circular A-130, Appendix III requires agencies to ensure that general support systems and major applications incorporate adequate security controls consistent with guidance issued by the National Institute of Standards and Technology (NIST). Adequate security is defined in Circular A-130 as the cost-effective use of management, personnel, operational, and technical controls commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. However, Circular A-130 does not specifically include operational controls in the detailed discussion of requirements for security plans. Guidance issued by NIST[3] describes software change controls (also referred to as configuration management and software maintenance controls) as part of the operational controls that agencies should describe in security plans and implement to ensure that changes to software are authorized, documented, and tested.

The proposed revisions to Circular A-130 do not address strengthening requirements for the security of federal information systems as provided in Appendix III. Our work[4] in the area of software change control has identified that controls over changes to system and application software for federal information systems governmentwide are currently inadequate, and this deficiency has persisted for several years. Key controls include

- Documentation, approval, and testing of changes,
- Maintenance and protection of source code libraries,
- Separation of duties to prevent unauthorized changes,
- Labeling and inventory of software programs,
- Monitoring and addressing unusual change activity,
- Managing changes to both system software and application software.

Controls over access to and modification of software are essential in providing reasonable assurance that system-based security controls are not compromised. Without proper software change controls, there are risks that security features could be inadvertently or deliberately

[2] Information Security: Controls Over Software Changes at Federal Agencies (GAO/AIMD-00-151R, May 4, 2000).
[3] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (dated October 1995), Chapters 8 and 14; and NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (dated December 1998), Sections 5.GSS.5 and 5.MA.5.
[4] Financial Audit: 1999 Financial Report of the United States Government (GAO/AIMD-00-131, March 31, 2000), and Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998).

omitted or rendered inoperable, that processing irregularities could occur, or that malicious code could be introduced.

In light of the deficiencies we have documented, we suggest that OMB strengthen the general support system technical security and major application technical control requirements of Circular A-130, Appendix III, to address control of changes to system and application software. Agencies should be encouraged to adopt industry best practices for software change management, such as those suggested by NIST or the Software Capability Maturity Model developed by the Software Engineering Institute at Carnegie-Mellon University.

Additional technical corrections for your consideration are included in the enclosure, issue 6.

We appreciate the opportunity to comment on the proposed revision of Circular A-130, and we hope that you find our suggestions useful. If you have any questions, please contact me at (202) 512-6257 or Lester Diamond at (202) 512-7957.

Sincerely yours,

David L. McClure
Associate Director
Governmentwide and Defense
Information Systems

This enclosure provides additional discussion and rationale for concerns about specific issues raised in our letter. The page references are to the Federal Register (April 13, 2000), in which the proposed revisions to Circular A-130 were published.

1. Definitions -- §6

The circular's current definition of "information technology" (IT) (§6(p), OMB Circular No. A-130, February 8, 1996) reflects the Paperwork Reduction Act's (PRA) definition of information technology, which exempts national security systems (44 U.S.C. 3502(9)). Note that the effect of this definition was unchanged by the amendment made by §5605(a) of the Clinger-Cohen Act (CCA) (110 Stat. 679, 700)). The proposed revision to the circular (§6(t), at p. 19936, 1st column) eliminates the exemption for national security systems in the IT definition, and adds a separate definition for such systems. This new definition includes a statement that the circular "shall apply to national security systems in a manner consistent with" the multi-part CCA national security exemption (§6(w), referring to §5141 of the CCA (110 Stat. 689)). While this might suffice if only the CCA were in effect, the continued application of the PRA argues for guidance that can explain to agencies how to reconcile the broader PRA exemption with the narrower CCA exemption.

2. Basic Considerations and Assumptions -- §7

The current circular, at §7(i), reflects the PRA's strategic information resources management (IRM) planning requirements. The proposed revisions would replace that language with references to "capital planning and investment control" processes (proposed §7(i), p. 19936, 2nd column). While the CCA created new requirements for IT investment planning and control, it did not replace or otherwise repeal the PRA's broader IRM planning requirements. i) should be modified to preserve the existing language, while perhaps inserting additional sentences with specific regard to IT capital planning and investment and its relationship to the broader IRM plans.

The proposed §7(r) refers to "interagency and interoperable shared information resources" (p. 19936, 2nd column). For improved clarity, and to more accurately reflect the provisions of the CCA, the term "information resources" probably should be changed to "information

3. Policy -- §8

The proposed amendments to §8b, Information Systems and Information Technology Management, should be reconsidered because they confuse IT capital planning with IRM planning, as well as the more general distinction between information resources and information technology.

In its preliminary background discussion, OMB states:

> "Section 8b. 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. Sections 8b(1), 8b(2), 8b(3) have been merged to better integrate requirements under Clinger-Cohen Act, the Government Performance and Results Act (Public Law 103-62), and revisions to OMB Circular A-11.
>
> New section 8b(1) is revised to provide guidance on both strategic and operational IRM planning by integrating the agency's information resources management plans, strategic plans, performance plans, financial plans, and budget processes, as discussed in OMB Circular A-11, Sec. 210.8." (p. 19935, bottom of 1st column).

While this summary correctly describes the major goal of implementing the policies of the CCA and Executive Order No.13011 (July 17, 1996), the proposed revisions confuse provisions that are distinctive to the PRA and CCA. By its heading, §8b of the circular applies to IT management, which is also the stated subject of both the CCA and E.O. 13011. By its text, however, the subsection reaches more broadly into the subject of IRM, which is the subject of the still effective PRA. Specifically, the current §8b contains three subparagraphs that apply to IRM: (1) Evaluation and Performance Measurement, (2) Strategic Information Resources Management (IRM) Planning, and (3) Use of Information Resources. Given that these subparagraphs implement provisions of the PRA that continue to be in effect, it would seem more appropriate for them to be moved under §8a, Information Management Policy, rather than retained under §8b. Care should be taken to review the discussion of §8a and §8b in the circular's Appendix IV to ensure that it accurately reflects the applicable authorities and appropriate subject matter.

The proposed revision also includes these same §8b IRM subparagraphs as part of its discussion of IT capital planning processes. The proposed revision states that capital planning under OMB Circular A-11 constitutes IRM planning required by the PRA:

> "As a product of the capital planning and investment control process, agencies must develop and maintain the agency Information Resource Management Plan (IRM) (also known as the IT Capital Plan), as required by 44 U.S.C. 3506(b)(2)." (proposed §8b(1)(A), p. 19936, 3rd column).

It is not clear that IT capital planning, by itself, constitutes the broader IRM planning required under PRA. According to OMB Circular A-11, capital planning is intended to guide the planning, budgeting, and acquisition of capital assets. (§300.1, Circular No. A-11, Part 3, "Planning, Budgeting, and Acquisition of Capital Assets, July 1999). The Circular defines capital assets as "land, structures, equipment, and intellectual property (e.g., software) that are used by the Federal Government and have an estimated useful life of two years or more." (ibid., §300.4). The Circular also describes IT as a capital asset (ibid.). There is, however, no suggestion in Circular A-11 that the term capital asset includes all other information resources or information functions, such as collection, records management, privacy protection, and security (see 44 U.S.C. 3504 & 3506). Quite the contrary, under current law, IT is a subset of "information resources," which the PRA defines as "information and related resources, such as personnel, equipment, funds, and information technology." 44 U.S.C. 3502(6). Accordingly, OMB is required to develop a government-wide IRM strategic plan

their responsibilities under the PRA. It did, however, add to their responsibilities (see §5125(b)&(c), 110 Stat. 685, 40 U.S.C. 1425(b) & (c)). E.O. 13011 also provides additional duties. Thus, the proposed §9a(3) should reference the continuing responsibilities under the PRA (specifically 44 U.S.C. 3506), and the CCA (specifically, 40 U.S.C. 1425(b) & (c)), as well as E.O.13011.

Second, the reference to E.O. 13011 is confusing. It is not clear if the reference is meant to limit CIO appointments to those identified in the E.O. Under the PRA, all agencies must have a CIO. The CCA describes CIO responsibilities in "executive agencies" (which the circular should align with the PRA's "agency"), and provides additional responsibilities for CIOs of the major, so-called CFO Act, agencies (40 U.S.C. 1425(b) & (c)). For its part, E.O. 13011 defines "executive agency" exactly like the CCA, but it "lists" the 28 agencies to be represented by CIOs on a presidentially established CIO Council. It also mentions four agencies with specific duties, i.e., OMB, GSA, the Department of Commerce, and the Department of State. Given the provisions of the PRA and the CCA, there should be no such limit on the number of CIOs. Accordingly, §9a(3) should be revised.

In addition, the following sections make references to "information resource" duties of the CIO, but it appears that they are more specific to "information technology management:"

- §9a(3)(b) – "investment priorities for agency information resources"
- §9a(3)(c) – "information resource implications"
- §9a(3)(d) – "information resource investments"
- §9a(3)(e) – "information resource decisions"
- §9a(3)(f) – "design, development, and implementation of information resources".

Cross-Agency Cooperation -- §9a(11)

Proposed §9a(11) is described as being "added to ensure cross agency cooperation" (p. 19935, 2nd column – note discussion below concerning apparent misnumbering). First, the basis for this new subsection is unclear. Subsection a(11) is not included in the explanation that subsections a(3), (12), (13), (14), and (15) are being added "to describe the CIO's responsibilities under the Clinger-Cohen Act" (p. 19935, 2nd column). Second, it is not clear what is meant by the mandate in §9a(11)(b) for a "government wide infrastructure that is provided and supported by a diversity of private sector suppliers" (p. 19938, 1st column). The meaning of "infrastructure" and the extent to which "infrastructure products and are meant to be provided exclusively by the private sector are not explained. Section 5113(b) of CCA (110 Stat. 682) requires a determination of whether a function supported by an information system should be privatized, but it does not require it.

Responsibilities of the Department of State -- §9b

The background discussion of revisions to §9b (p. 19935, bottom of 2nd column) states that the responsibilities of the Department of State are "revised to reflect responsibilities described in the Clinger-Cohen Act and Executive Order 13011." There do not appear to be any requirements in the CCA exclusively applicable to the Department of State.

5. EFOIA & PRA Inventory Requirements -- §9a(7)

In the background discussion of EFOIA and PRA inventory requirements (p. 19934, 3rd column), OMB explains that agency inventories should only include "major" information systems. This is consistent with 44 U.S.C. 3511, which requires the creation of a Government Information Locator Service (GILS) that is to "identify major information

systems, holdings, and dissemination products of each agency." It is not, however, consistent with 44 U.S.C. 3506(b), which OMB cites in its discussion in the 3rd column of p. 19934.

The PRA's §3506(b)(4) calls for each agency to "maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511." If nothing else, this suggests that agency GILS listings are to be a subset of the §3506(b) inventory – thus, an inventory of "major" systems and holdings could be a part of a larger "complete" inventory of information resources. OMB's acceptance of the "complete" inventory requirement seems to be reflected in its description of an Information Technology Architecture (ITA) in proposed §8b(2), where it states that an agency ITA "should be supported by a complete inventory of the agency information resources" (p. 19937, bottom of 2nd column).

OMB's discussion on p. 19934, however, suggests that both the §3506 and §3511 inventory requirements would be satisfied by an inventory of only "major" systems – "an inventory that includes those major systems (but not all systems) makes the most sense for improving agency management." OMB says as much in proposed §9a(7), which would require agencies to:

> "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; and 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." (p. 19938, 1st column, emphasis added).

The proposed §9a(7) list of inventory components is certainly redundant, but it neither clearly satisfies, nor explains away the PRA's §3506(b)(4) requirement for a "current and complete" inventory of information resources. If OMB does not believe the §3506(b)(4) requirement is practical, it should say so. It is important, therefore, for OMB to more clearly explain its interpretation of both the §3506 and §3511 inventory requirements.

6. Technical Corrections

a. A correction is needed in §8a of the current A-130 with regard to the numbered paragraphs that follow §8a(1)(k). Because of the repeated use of arabic numbering and an incorrect indentation, §8a(1)(k)(1) is followed by (2), (3), etc. Rather than being (k)(2) and (k)(3), it seems that those paragraphs are meant to be §8a(1), (2) and (3).

b. The amendments to §8b are not clearly identified. First, the amendments to §8b are described as "revising Section 8b(1) (p.19936, 2nd column), whereas, as explained earlier (p. 19935, 1st & 2nd columns), they actually revise §8b(1) – (5). Second, given the explanation that §8b(5) is being revised as 8b(3), it appears that the paragraph numbered (1) in the 3rd

column of p. 19937 should be (3). In general, the numbering of the paragraphs should be reviewed for accuracy.

c. The background discussion of §9a (p. 19935, 2nd column) appears to have misnumbered two subsections in comparison with the actual amendments on p. 19937-8, 3rd & 1st columns. It seems the discussion in the 2nd column of p. 19935 should refer to §9a(11) instead of §9a(10) and §9a(14) instead of §9a(11).

d. The proposed revisions to App. IV (p. 19939) are not clearly identified. It is unclear whether the proposed provisions are meant to be additions or substitutions for existing language. See, for example, "Revise Section 8a(5) **to include**:" (p.19939, bottom of 1st column, emphasis added), "Section 8b(1) (p. 19939, top of 3rd column), and "Section 8b(2)" (p.19940, bottom of 1st column). In light of the comments above with regard to §8 revisions, we would suggest a thorough review of the contents and organization of Appendix IV.

(511995)