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. 3, Appendix III, ''Security of Federal Automated Information Resources.''

SUMMARY: The Office of Management and Budget (OMB) is revising Appendix III, ''Security of Federal Information Systems,'' of Circular No. A–130, ''Management of Federal Automated Information Resources.'' This is the third stage of planned revisions to Circular A–130. Enactment of the Information Technology Management Reform Act of 1996 (Division E of the National Defense Authorization Act for Fiscal Year 1996) will require OMB to issue additional guidance on capital planning, investment control, and the management of information technology. A plan for those revisions will be announced in the Spring.

Transmittal 1 to Circular A–130, effective June 25, 1993, and published on July 2, 1993 (58 FR 36068) addressed the Information Management Policy section of the Circular (Section 8a), as well as Appendix I, ''Federal Agency Responsibilities for Maintaining Records About Individuals.'' That issuance dealt primarily with how the Federal government manages its information holdings, particularly information exchange with the public.

Transmittal 2 to Circular A–130, effective July 15, 1994, and published on July 25, 1994 (59 FR 37906) addressed agency management practices for information systems and information technology (Section 8b). That issuance was intended to (1) promote agency investments in information technology that improve service delivery to the public, reduce burden on the public, and lower the cost of Federal programs administration, and (2) encourage agencies to use information technology as a strategic resource to improve Federal work processes and organization.

This Transmittal 3 is intended to guide agencies in securing government information resources as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls, such as individual responsibility, awareness and training, and accountability, and explains how they can be supported by technical controls. Among other things, it requires agencies to assure that risk-based rules of behavior are established, that employees are trained in them, and that the rules are enforced. The revision also integrates security into program and mission goals, reduces the centralized reporting of security plans, emphasizes the management of risk rather than its measurement, and revises government-wide security responsibilities to be consistent with the Computer Security Act and the Paperwork Reduction Act of 1995.

This transmittal also makes minor technical revisions to Section 9 (''Assignment of Responsibilities'') and Section 10 (''Oversight'') to reflect the Paperwork Reduction Act of 1995 (Pub. L. 104–13). One substantive change has been made to Appendix I in Section 3.a. changing the annual requirement to review recordkeeping practices, training, violations, and notices to a biennial review, in accordance with other regular agency reviews not required by statute. Several minor changes have been made, none of which are intended to be substantive. In Section 2.c., a portion of the definition of ''nonfederal agency'' which has been inadvertently omitted has been added to reflect the current practice in state-federal matching programs. In Section 3.a., extraneous and confusing language referring to source or matching agencies was removed because the provision applies to any agency that participates in a matching program. The example's in 4.c.(1) were updated for clarity. Other editorial and organizational changes were made throughout the appendix.

Appendix IV has been changed to include material from OMB Memorandum M–95–22, ''Implementing the Information Dissemination Provisions of the Paperwork Reduction Act of 1995'' (September 29, 1995), and to delete some outdated or otherwise already implemented guidance from the discussion of Sections 9 and 10.

ELECTRONIC AVAILABILITY: This document is available on the OMB Home page of Welcome to the White House World Wide Web site (http://www.whitehouse.gov) as http://www1.whitehouse.gov/White-House/EOP/OMB/html/omb-a130.html. This document is also available on the Internet via anonymous File Transfer Protocol (FTP) from the National Institute of Standards and Technology (NIST) Computer Security Resource Clearinghouse at csrc.ncsl.nist.gov as /pub/secplcy/a130.txt (do not use any capital letters in the file name) or via the World Wide Web from http://csrc.ncsl.nist.gov/secplcy as a130.txt. Appendix III, ''Security of Federal Automated Information Resources'' can be separately obtained as a130app3.txt. The clearinghouse can also be reached using dial-in access at 301–948–5717. For those who do not have file transfer capability, the document can be retrieved via mail query by sending an electronic mail message to docserver@csrc.ncsl.nist.gov with no subject and with send a130.txt (or a130app3.txt for only the security appendix) as the first line of the body of the message. Paper copies may also be obtained by writing to the Publications Office, Office of Management and Budget, Room 2200 NEOB, Washington, D.C. 20503 or by telephone at (202) 395–7332.

FOR FURTHER INFORMATION CONTACT: 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:

Since December 30, 1985, Appendix III of Office of Management and Budget (OMB) Circular No. A–130, ''Security of Federal Automated Information Systems,'' has defined a minimum set of controls for the security of Federal automated information systems (50 FR 52730). That Appendix, and its predecessor, Transmittal Memorandum No. 1 to OMB Circular No. A–71, (July 27, 1978), defined controls that were considered effective in a centralized processing environment which ran primarily custom-developed application software.

Today's computing environment is significantly different. It is characterized by open, widely distributed processing systems which frequently operate with commercial off-the-shelf software. While effective use of information technology often reduces risks to the Federal program being administered (e.g., risks from fraud or errors), the risk to and vulnerability of Federal information resources has increased. Greater risks result from increasing quantities of valuable information being committed to Federal systems, and from agencies being critically dependent on those systems to perform their missions. Greater vulnerabilities exist because virtually every Federal employee has access to Federal systems, and because these systems now interconnect with outside systems.

In part because of these trends, Congress enacted the Computer Security Act of 1987 (Pub. L. 100–235). That Act requires agencies to improve the

security of Federal computer systems, plan for the security of sensitive systems, and provide mandatory awareness and training in security for all individuals with access to computer systems.

To assist agencies in implementing the Computer Security Act, OMB issued Bulletin No. 88–16, ''Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information'' (July 6, 1988), and OMB Bulletin No. 90–08, ''Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information'' (July 9, 1990). This revision of Appendix III to OMB Circular A–130 incorporates and updates the policies set out in those Bulletins and supersedes them.

The report of the National Performance Review, ''Creating a Government that Works Better & Costs Less: Reengineering through Information Technology'' (September 1993), recommended that Circular A–130 be revised to: (1) Require an information security plan to be part of each agency's strategic information technology (IT) plan; (2) require that if computer security does not meet established thresholds, it be identified as a material weakness in the Federal Managers' Financial Integrity Act report; (3) require awareness and training of employees and contractors; (4) require that agencies improve planning for contingencies; and (5) establish and employ formal emergency response capabilities. Those recommendations are incorporated in this revision.

Since its establishment by the Computer Security Act, the Computer System Security and Privacy Advisory Board has recommended changes in Circular A–130 to: (1) Require that agencies establish computer emergency response teams; and (2) link oversight of Federal computer security activities more closely to the oversight established pursuant to the Federal Manager's Financial Integrity Act (FMFIA), Public Law 97–255. This revision incorporates both of those recommendations.

Subsequent to issuance of Bulletin 90–08, OMB, the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA) met with 28 Federal departments and agencies to review their computer security programs. In February 1993, OMB, NIST and NSA issued a report (''Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90–08'') which summarized those meetings and proposed several changes in OMB Circular A–130 as next steps to improving the Federal computer security program. Those proposed changes are incorporated in this revision.

The revised Appendix clarifies the relationship between requirements to protect information classified pursuant to an Executive Order and the requirements in this Appendix. Where an agency processes information which is controlled for national security reasons pursuant to an Executive Order or statute, security measures required by appropriate directives should be included in agency systems. Those policies, procedures, and practices will be coordinated with the U.S. Security Policy Board as directed by the President.

On May 22, 1995, the President signed into law the Paperwork Reduction Act of 1995, Public Law 104–13. That Act, in 44 U.S.C. 3505 and 3506, requires agencies to establish computer security programs, and it tasks OMB to develop and oversee the implementation of policies, principles, standards and guidelines on security. It also requires Federal agencies to identify and provide security protection consistent with the Computer Security Act of 1987 (40 U.S.C. 759 note). This revision is intended to implement those OMB responsibilities.

Comments on the Proposed Appendix

On April 3, 1995, the revised Appendix was proposed for public comment (60 FR 16970). It was also sent directly to Federal agencies for comment and made available for comment via the Internet. Thirty-two comments were received. The comments supported the approach proposed in the revised Appendix. They also made a number of suggestions to improve it. The principal issues raised in comments and our response to them are set forth below.

1. Most of the comments stated that the preamble accompanying the proposed Appendix was useful in their understanding of the Appendix itself. They suggested that the information in the preamble be incorporated in the final Appendix for improved future understanding.

We agree with this suggestion, and have incorporated the preamble, as revised to accommodate changes made to the proposed Appendix, as part B of the final Appendix.

2. Many comments suggested that the terminology of the Appendix should be more directive.

We generally agree with this comment, and have changed part A of the Appendix to be directive, while leaving the descriptive material in part B as explanatory.

3. A number of comments noted that there is a difference between making individuals aware of security needs and training them. They suggested that the Appendix should clarify this distinction and the requirements associated with each.

We agree, and have made changes in the Appendix and the descriptive information in part B to clarify that the requirements for training are consistent with the Computer Security Act (i.e., for increasing computer security awareness and training in accepted security practice).

We have also added a clarification that training for members of the public who are given access to general support systems should normally be accomplished in the context of the application to which they are given access. As was pointed out in comments, members of the public should not be given direct access to general support systems, except through authorized use of an application. We have also added descriptive language in part B to address the need to train members of the public with access to major applications.

4. Several comments raised a concern about the proposed requirement to limit access to systems until a new employee has been trained in security responsibilities. They suggested that training be required to be completed within a certain amount of time after access is granted (e.g., 60 days).

We disagree. Understanding the security requirements that are integral to a system is a fundamental responsibility of each individual who accesses the system. It should not be delayed for administrative convenience. Furthermore, security training should be included as part of general training in use of the system for an employee. Initial awareness and training need not be accomplished through formal classroom training; in some cases it may be through interactive sessions of reading well-written and understandable rules. The critical factor is for the initial and subsequent awareness and training to be commensurate with the risk and magnitude of harm that could occur. Therefore, new employees can and should be trained in their security responsibilities before access is granted. The final Appendix includes this requirement.

5. Several comments expressed concern about the proposed removal of the requirement for agencies to prepare formal risk analyses. They point out that such analyses assist in identifying

threats, vulnerabilities, and risks to a system. They expressed a concern that without such analyses it would be difficult to convince senior management of the need for security. Other comments said that without risk analysis as the basis of decisions, security measures will not be effective. On the other hand, several comments supported the removal of this requirement, which they found not cost-effective.

We agree that security measures must be risk-based. The Computer Security Act requires that security controls be commensurate with the risk and magnitude of harm that could occur. Implicit in that approach is a need to assess the risk to each system. However, given the complexity and detail such formal analyses often entail, a formal risk analysis is not appropriate for every system. Therefore, the Appendix does not require that a formal risk analysis be performed.

At the same time, risk assessment is an essential element in ensuring adequate security. NIST recently issued a handbook, ''An Introduction to Computer Security: The NIST Handbook'' (March 16, 1995), which contains guidance on computer security risk management and provides a flexible framework for performing meaningful risk assessments. Part B references the NIST handbook.

6. Several comments asked about the relation between the rules of behavior required in the Appendix and operating policies prescribed in the NIST Handbook. Other comments made suggestions about the kind and scope of rules that should be included in the security plan.

We have added language to part B to describe the kinds of rules we believe are appropriate and to clarify that rules of behavior in the Appendix should be consistent with the system-specific policies described in the NIST handbook.

7. Several comments raised a concern about the effectiveness of reviews of security controls unless they are performed by independent reviewers.

An independent review can improve the objectivity of the review, as well as its value to top management in assessing the need for corrective action. Therefore, we have added language to the discussion in part B of the Appendix that clarifies that reviews of major applications, because of their higher risk, should be independent. We have not, however, required that reviews of all general support systems be independent. Nevertheless, given the value of an independent review, agencies may elect to use this approach, particularly where a system supports a high-risk agency function.

In addition, we understand that the U.S. General Accounting Office is developing guidance which provides a structured approach for performing reviews. We have also revised the Appendix to be consistent with OMB Circular No. A–123, ''Management Accountability and Control'' (June 21, 1995).

8. Several comments requested additional guidance on enforcement of the rules of behavior, either from the Department of Justice or the Office of Personnel Management (OPM).

The presumption in requiring rules of behavior is that they would be enforced as are other behavioral rules within an agency. Therefore, we are not proposing to have central guidance developed by either Justice or OPM. However, we expect that agencies will share their various approaches through inter-agency forums, such as the Computer Security Program Managers' Forum. We have added a brief discussion of this point to part B.

9. Several comments concerned the protection of shared information and requested that additional guidance be provided. We have clarified our intent in the discussion in part B.

10. One comment raised a concern about the Appendix's apparent subordination of technical controls to management controls. While we are stressing the importance of management controls, we have added preamble language to clarify that both types of controls must be in place to be effective.

11. A number of comments raised a concern about whether adequate funding would be forthcoming to implement the requirements of the Appendix.

Implicit in issuing the Appendix is our presumption that a system is created and maintained with adequate security or it should not be created or maintained. Security costs should therefore be factored into the normal capital planning and investment controls process for information technology, consistent with the information systems and information technology management requirements in Section 8b of this circular.

12. A number of comments concerned the government-wide role of the Security Policy Board. Several favored expanding that role, others proposed that it be more limited. Still others said the Appendix should be silent on national security directives.

We have revised the language in the Appendix to clarify the role of the Security Policy Board regrading security of information technology used to process classified information. We have also added language to the preamble which clarifies that Circular No. A–130 and the Appendix exclude certain mission critical systems, the so-called ''Warner systems'' from coverage, and to describe the Department of Defense's responsibilities pursuant to existing Presidential directives. The Appendix does not attempt to interpret the language of the directives. Rather, it clarifies that requirements issued pursuant to those directives should be used in place of the requirements of the Appendix with respect to the protection of classified information. The discussion of national security directives is included to assist in the coordination of security activities among various security communities.

Accordingly, Circular A–130 is revised as set forth below.

Sally Katzen,

Administrator, Office of Information and Regulatory Affairs.

Executive Office of the President

Office of Management and Budget

February 8, 1996.

Circular No. A–130, Revised (Transmittal Memorandum No. 3)

Memorandum for Heads of Executive Departments and Establishments

Subject: Management of Federal Information Resources.

Circular No. A–130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35. This Transmittal Memorandum contains updated guidance on the ''Security of Federal Automated Information Systems,'' Appendix III and makes minor technical revisions to the Circular to reflect the Paperwork Reduction Act of 1995 (Pub. L. 104–13). The Circular is reprinted in its entirety for convenience.

Alice M. Rivlin,

Director.

Attachment

Circular No. A–130 Revised (Transmittal Memorandum No. 3)

Memorandum for Heads of Executive Departments and Establishments

Subject: Management of Federal Information Resources.

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

2. Rescissions: This Circular rescinds OMB Circulars No. A–3, A–71, A–90, A–108, A–114, and A–121, and all Transmittal Memoranda to those circulars.

3. Authorities: This Circular is issued 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 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. 759 and 487); the Computer Security Act (40 U.S.C. 759 note); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); Executive Order No. 12046 of March 27, 1978; and Executive Order No. 12472 of April 3, 1984.

4. Applicability and Scope:

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

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Paperwork Reduction Act 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 Act requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

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

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

c. The term ''dissemination'' means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

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

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

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

g. The term ''information'' means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

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

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

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

k. The term ''information resources'' includes both government information and information technology.

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

m. The term ''information resources management'' means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

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

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

p. The term ''information technology'' means the hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

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

r. The term ''records'' means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

s. The term ''records management'' means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

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

7. Basic Considerations and Assumptions:

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

b. Government information is a valuable national resource. It provides the public with knowledge of the government, society, and economy—past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

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

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

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

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

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

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

i. Agency strategic planning can improve the operation of government programs. The application of information resources should support an agency's strategic plan to fulfill its mission. The integration of IRM planning with agency strategic planning promotes the appropriate application of Federal information resources.

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

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

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

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

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

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

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

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

8. Policy

a. Information Management Policy:

(1) Information Management Planning. Agencies shall plan in an integrated manner for managing information throughout its life cycle. Agencies shall:

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

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

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

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

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

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

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

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

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

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

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

(l) Provide for public access to records where required or appropriate.

(2) Information Collection. Agencies shall collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

(3) Electronic Information Collection. Agencies shall use electronic collection techniques where such techniques reduce burden on the public, increase efficiency of government programs, reduce costs to the government and the public, and/or provide better service to the public. Conditions favorable to electronic collection include:

(a) The information collection seeks a large volume of data and/or reaches a large proportion of the public;

(b) The information collection recurs frequently;

(c) The structure, format, and/or definition of the information sought by the information collection does not change significantly over several years;

(d) The agency routinely converts the information collected to electronic format;

(e) A substantial number of the affected public are known to have ready access to the necessary information technology and to maintain the information in electronic form;

(f) Conversion to electronic reporting, if mandatory, will not impose substantial costs or other adverse effects on the public, especially State and local governments and small business entities.

(4) Records Management. Agencies shall:

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

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

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

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

(5) Providing Information to the Public. Agencies have a responsibility to provide information to the public consistent with their missions. Agencies shall discharge this responsibility by:

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

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

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

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

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

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

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

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

(6) Information Dissemination Management System. Agencies shall maintain and

implement a management system for all information dissemination products which shall, at a minimum:

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

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

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

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

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

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

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

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

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

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

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

(7) Avoiding Improperly Restrictive Practices. Agencies shall:

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

(b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on the reuse, resale, or redissemination of Federal information dissemination products by the public; and,

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

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

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

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

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

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

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

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

(c) The agency disseminates the product frequently;

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

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

(9) Safeguards. Agencies shall:

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

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

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

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

b. Information Systems and Information Technology Management

(1) Evaluation and Performance Measurement. Agencies shall promote the appropriate application of Federal information resources as follows:

(a) Seek opportunities to improve the effectiveness and efficiency of government programs through work process redesign and the judicious application of information technology;

(b) Prepare, and update as necessary throughout the information system life cycle, a benefit-cost analysis for each information system:

(i) At a level of detail appropriate to the size of the investment;

(ii) Consistent with the methodology described in OMB Circular No. A–94, ''Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs;'' and

(iii) that relies on systematic measures of mission performance, including the:

(a) Effectiveness of program delivery;

(b) Efficiency of program administration; and

(c) Reduction in burden, including information collection burden, imposed on the public;

(c) Conduct benefit-cost analyses to support ongoing management oversight processes that maximize return on investment and minimize financial and operational risk for investments in major information systems on an agency-wide basis; and

(d) Conduct post-implementation reviews of information systems to validate estimated benefits and document effective management practices for broader use.

(2) Strategic Information Resources Management (IRM) Planning. Agencies shall establish and maintain strategic information resources management planning processes which include the following components:

(a) Strategic IRM planning that addresses how the management of information resources promotes the fulfillment of an agency's mission. This planning process should support the development and maintenance of a strategic IRM plan that reflects and anticipates changes in the agency's mission, policy direction, technological capabilities, or resource levels;

(b) Information planning that promotes the use of information throughout its life cycle to maximize the usefulness of information, minimize the burden on the public, and preserve the appropriate integrity, availability, and confidentiality of information. It shall specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(c) Operational information technology planning that links information technology to anticipated program and mission needs, reflects budget constraints, and forms the basis for budget requests. This planning should result in the preparation and maintenance of an up-to-date five-year plan, as required by 44 U.S.C. 3506, which includes:

(i) A listing of existing and planned major information systems;

(ii) A listing of planned information technology acquisitions;

(iii) An explanation of how the listed major information systems and planned information technology acquisitions relate to each other and support the achievement of the agency's mission; and

(iv) A summary of computer security planning, as required by Section 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note); and

(d) Coordination with other agency planning processes including strategic, human resources, and financial resources.

(3) Information Systems Management Oversight. Agencies shall establish information system management oversight mechanisms that:

(a) Ensure that each information system meets agency mission requirements;

(b) Provide for periodic review of information systems to determine:

(i) How mission requirements might have changed;

(ii) Whether the information system continues to fulfill ongoing and anticipated mission requirements; and

(iii) What level of maintenance is needed to ensure the information system meets mission requirements cost effectively;

(c) Ensure that the official who administers a program supported by an information system is responsible and accountable for the management of that information system throughout its life cycle;

(d) Provide for the appropriate training for users of Federal information resources;

(e) Prescribe Federal information system requirements that do not unduly restrict the prerogatives of State, local, and tribal governments;

(f) Ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources; and

(g) Ensure that financial management systems conform to the requirements of OMB Circular No. A–127, ''Financial Management Systems.''

(4) **USE OF INFORMATION RESOURCES.** Agencies shall create and maintain management and technical frameworks for using information resources that document linkages between mission needs, information content, and information technology capabilities. These frameworks should guide both strategic and operational IRM planning. They should also address steps necessary to create an open systems environment. Agencies shall implement the following principles:

(a) Develop information systems in a manner that facilitates necessary interoperability, application portability, and scalability of computerized applications across networks of heterogeneous hardware, software, and communications platforms;

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

(c) Share available information systems with other agencies to the extent practicable and legally permissible;

(d) Meet information technology needs through intra-agency and inter-agency sharing, when it is cost effective, before acquiring new information technology resources;

(e) For Information Processing Service Organizations (IPSOs) that have costs in excess of $5 million per year, agencies shall:

(i) Account for the full costs of operating all IPSOs; (ii) Recover the costs incurred for providing IPSO services to all service recipients on an equitable basis commensurate with the costs required to provide those services; and

(iii) Document sharing agreements between service recipients and IPSOs; and

(f) Establish a level of security for all information systems that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in these information systems.

(5) **ACQUISITION OF INFORMATION TECHNOLOGY.** Agencies shall:

(a) Acquire information technology in a manner that makes use of full and open competition and that maximizes return on investment;

(b) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software to meet mission needs is clear and has been documented;

(c) Acquire information technology in accordance with OMB Circular No. A–109, ''Acquisition of Major Systems,'' where appropriate; and

(d) Acquire information technology in a manner that considers the need for accommodations of accessibility for individuals with disabilities to the extent that needs for such access exist.

9. **ASSIGNMENT OF RESPONSIBILITIES**

a. **ALL FEDERAL AGENCIES.** The head of each agency shall:

(1) Have primary responsibility for managing agency information resources;

(2) Ensure that the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB are implemented appropriately within the agency;

(3) 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;

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

(5) Maintain an inventory of the agencies' major information systems, holdings and information dissemination products, as required by 44 U.S.C. 3511.

(6) 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.

(7) Identify to the Director, OMB, 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;

(8) 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;

(9) Appoint a senior official, as required by 44 U.S.C. 3506(a), who shall report directly to the agency head to carry out the responsibilities of the agency under the PRA. The head of the agency shall keep the Director, OMB, advised as to the name, title, authority, responsibilities, and organizational resources of the senior official. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official.

(10) Direct the senior official appointed pursuant to 44 U.S.C. 3506(a) to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the senior official shall consider alleged instances of agency failure to comply with this Circular and recommend or take corrective action as appropriate. The senior official shall report annually, not later than February 1st of each year, to the Director those instances of alleged failure to comply with this Circular and their resolution.

b. **DEPARTMENT OF STATE.** The Secretary of State shall:

(1) Advise the Director, OMB, on the development of United States positions and policies on international information policy issues affecting Federal Government information activities and ensure that such positions and policies are consistent with Federal information resources management policy;

(2) Ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international information technology standards, and advise the Director, OMB, of such activities.

c. **DEPARTMENT OF COMMERCE.** The Secretary of Commerce shall:

(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;

(2) Advise the Director, OMB, on the development of policies relating to the procurement and management of Federal telecommunications resources;

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

(4) Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;

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

(6) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

(7) Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of

State, international information technology standards, and advise the Director, OMB, of such activities.

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

e. **GENERAL SERVICES ADMINISTRATION.** The Administrator of General Services shall:

(1) Advise the Director, OMB, and agency heads on matters affecting the procurement of information technology;

(2) Coordinate and, when required, provide for the purchase, lease, and maintenance of information technology required by Federal agencies;

(3) Develop criteria for timely procurement of information technology and delegate procurement authority to agencies that comply with the criteria;

(4) Provide guidelines and regulations for Federal agencies, as authorized by law, on the acquisition, maintenance, and disposition of information technology, and for implementation of Federal Information Processing Standards;

(5) Develop policies and guidelines that facilitate the sharing of information technology among agencies as required by this Circular;

(6) Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act as amended;

f. **OFFICE OF PERSONNEL MANAGEMENT.** The Director, Office of Personnel Management, shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(10) Resolve information technology procurement disputes between agencies and the General Services Administration pursuant to Section 111 of the Federal Property and Administrative Services Act;

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

(12) Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy.

10. Oversight:

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

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

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

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

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

Appendix I to OMB Circular No. A–130—Federal Agency Responsibilities for Maintaining Records About Individuals

1. Purpose and Scope

This Appendix describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, 5 U.S.C. 552a, as amended (hereinafter ''the Act''). It applies to all agencies subject to the Act. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 FR 28949–28978, July 9, 1975), or Final Guidance for Conducting Matching Programs (54 FR at 25819, June 19, 1989).

2. Definitions

a. The terms ''agency,'' ''individual,'' ''maintain,'' ''matching program,'' ''record,'' ''system of records,'' and ''routine use,'' as used in this Appendix, are defined in the Act (5 U.S.C. 552a(a)).

b. Matching Agency. Generally, the Recipient Federal agency (or the Federal source agency in a match conducted by a nonfederal agency) is the matching agency and is responsible for meeting the reporting and publication requirements associated with the matching program. However, in large, multi-agency matching programs, where the recipient agency is merely performing the matches and the benefit accrues to the source agencies, the partners should assign responsibility for compliance with the administrative requirements in a fair and reasonable way. This may mean having the matching agency carry out these requirements for all parties, having one participant designated to do so, or having each source agency do so for its own matching program(s).

c. Nonfederal Agency. Nonfederal agencies are State or local governmental agencies receiving or providing records in a matching program with a Federal agency.

d. Recipient Agency. Recipient agencies are Federal agencies or their contractors receiving automated records from the Privacy Act systems of records of other Federal agencies, or from State or local governments, to be used in a matching program as defined in the Act.

e. Source Agency. A source agency is a Federal agency that discloses automated records from a system of records to another Federal agency or to a State or local agency to be used in a matching program. It is also a State or local agency that discloses records to a Federal agency for use in a matching program.

3. Assignment of Responsibilities

a. All Federal Agencies. In addition to meeting the agency requirements contained in the Act and the specific reporting and publication requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered. The head of each agency shall:

(1) Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees. (See 5 U.S.C. 552a(m)(1)).

(2) Recordkeeping Practices. Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.

(3) Routine Use Disclosures. Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.

(4) Exemption of Systems of Records. Review every four years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.

(5) Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.

(6) Privacy Act Training. Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.

(7) Violations. Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.

(8) Systems of Records Notices. Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register (See paragraph 4c of this Appendix).

b. Department of Commerce. The Secretary of Commerce shall, consistent with guidelines issued by the Director, OMB, develop and issue standards and guidelines for ensuring the security of information protected by the Act in automated information systems.

c. The Department of Defense, General Services Administration, and National Aeronautics and Space Administration. These agencies shall, consistent with guidelines issued by the Director, OMB, ensure that instructions are issued on what agencies must do in order to comply with the requirements of Section (m) of the Act when contracting for the operation of a system of records to accomplish an agency purpose.

d. Office of Personnel Management. The Director of the Office of Personnel Management shall, consistent with guidelines issued by the Director, OMB:

(1) Develop and maintain government-wide standards and procedures for civilian personnel information processing and recordkeeping directives to assure conformance with the Act.

(2) Develop and conduct Privacy Act training programs for agency personnel, including both the conduct of courses in various substantive areas (e.g., administrative, information technology) and the development of materials that agencies can use in their own courses. The assignment of this responsibility to OPM does not affect the responsibility of individual agency heads for developing and conducting training programs tailored to the specific needs of their own personnel.

e. National Archives and Records Administration. The Archivist of the United States through the Office of the Federal Register, shall, consistent with guidelines issued by the Director, OMB:

(1) Issue instructions on the format of the agency notices and rules required to be published under the Act.

(2) Compile and publish every two years, the rules promulgated under 5 U.S.C. 552a(f) and agency notices published under 5 U.S.C. 552a(e)(4) in a form available to the public at low cost.

(3) Issue procedures governing the transfer of records to Federal Records Centers for storage, processing, and servicing pursuant to 44 U.S.C. 3103. For purposes of the Act, such records are considered to be maintained by the agency that deposited them. The Archivist may disclose deposited records only according to the access rules established by the agency that deposited them.

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

(1) Issue guidelines and directives to the agencies to implement the Act.

(2) Assist the agencies, at their request, in implementing their Privacy Act programs.

(3) Review new and altered system of records and matching program reports submitted pursuant to Section (o) of the Act.

(4) Compile the biennial report of the President to Congress in accordance with Section (s) of the Act.

(5) Compile and issue a biennial report on the agencies' implementation of the computer matching provisions of the Privacy Act, pursuant to Section (u)(6) of the Act.

4. Reporting Requirements. The Privacy Act requires agencies to make the following kinds of reports:

Report	When Due	Recipient**
Biennial Privacy Act Report	June 30, 1996, 1998, 2000, 2002	Administrator, OIRA.
Biennial Matching Activity Report	June 30, 1996, 1998, 2000, 2002	Administrator, OIRA.
New System of Records Report .	When establishing a system of records—at least 40 days before operating the system*.	Administrator, OIRA, Congress.
Altered System of Records Report.	When adding a new routine use, exemption, or otherwise significantly altering an existing system of records—at least 40 days before change to system takes place.	*Administrator, OIRA, Congress.
New Matching Program Report ..	When establishing a new matching program—at least 40 days before operating the program*.	Administrator, OIRA, Congress.
Renewal of Existing Matching Program.	At least 40 days prior to expiration of any one year extension of the original program—treat as a new program.	Administrator, OIRA, Congress.
Altered Matching Program	When making a significant change to an existing matching program—at least 40 days before operating an altered program*.	Administrator, OIRA, Congress.
Matching Agreements	At least 40 days prior to the start of a matching program*	Congress.

*Review Period: Note that the statutory reporting requirement is 30 days prior; the additional ten days will ensure that OMB and Congress have sufficient time to review the proposal. Agencies should therefore ensure that reports are mailed expeditiously after being signed.

**Recipient Addresses: At bottom of envelope print ''Privacy Act Report''.

House of Representatives: The Chair of the House Committee on Government Reform and Oversight, 2157 RHOB, Washington, D.C. 20515–6143.

Senate: The Chair of the Senate Committee on Governmental Affairs, 340 SDOB, Washington, D.C. 20510–6250.

Office of Management and Budget: The Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, ATTN: Docket Library, NEOB Room 10012, Washington, D.C. 20503.

a. Biennial Privacy Act Report. To provide the necessary information for the biennial report of the President, agencies shall submit a biennial report to OMB, covering their Privacy Act activities for the calendar years covered by the reporting period. The exact format of the report will be established by OMB. At a minimum, however, agencies should collect and be prepared to report the following data on a calendar year basis:

(1) A listing of publication activity during the year showing the following:

*Total Number of Systems of Records (Exempt/NonExempt)
*Number of New Systems of Records Added (Exempt/NonExempt)
*Number Routine Uses Added
*Number Exemptions Added to Existing Systems
*Number Exemptions Deleted from Existing Systems
*Total Number of Automated Systems of Records (Exempt/NonExempt)

The agency should provide a brief narrative describing those activities in detail, e.g., ''the Department added a (k)(1) exemption to an existing system of records entitled ''Investigative Records of the Office of Investigations;'' or ''the agency added a new routine use to a system of records entitled 'Employee Health Records' that would permit disclosure of health data to researchers under contract to the agency to perform workplace risk analysis.''

(2) A brief description of any public comments received on agency publication and implementation activities, and agency response.

(3) Number of access and amendment requests from record subjects citing the Privacy Act that were received during the calendar year of the report. Also the disposition of requests from any year that were completed during the calendar year of the report:

*Total Number of Access Requests
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
Number For Which No Record Found
*Total Amendment Requests
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
*Number of Appeals of Denials of Access
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
Number For Which No Record Found
*Number of Appeals of Denials of Amendment
Number Granted in Whole
Number Granted in Part
Number Wholly Denied

(4) Number of instances in which individuals brought suit under section (g) of the Privacy Act against the agency and the results of any such litigation that resulted in a change to agency practices or affected guidance issued by OMB.

(5) Results of the reviews undertaken in response to paragraph 3a of this Appendix.

(6) Description of agency Privacy Act training activities conducted in accordance with paragraph 3a(6) of this Appendix.

b. Biennial Matching Activity Report (See 5 U.S.C. 552a(u)(3)(D)). At the end of each calendar year, the Data Integrity Board of each agency that has participated in a matching program will collect data summarizing that year's matching activity. The Act requires that such activity be reported every two years. OMB will establish the exact format of the report, but agencies' Data Integrity Boards should be prepared to report the data identified below both to the agency head and to OMB:

(1) A listing of the names and positions of the members of the Data Integrity Board and showing separately the name of the Board Secretary, his or her agency mailing address, and telephone number. Also show and explain any changes in membership or structure occurring during the reporting year.

(2) A listing of each matching program, by title and purpose, in which the agency participated during the reporting year. This listing should show names of participant agencies, give a brief description of the program, and give a page citation and the date of the Federal Register notice describing the program.

(3) For each matching program, an indication of whether the cost/benefit analysis performed resulted in a favorable ratio. The Data Integrity Board should explain why the agency proceeded with any matching program for which an unfavorable ratio was reached.

(4) For each program for which the Board waived a cost/benefit analysis, the reasons for the waiver and the results of the match, if tabulated.

(5) A description of any matching agreement the Board rejected and an explanation of the rejection.

(6) A listing of any violations of matching agreements that have been alleged or identified, and a discussion of any action taken.

(7) A discussion of any litigation involving the agency's participation in any matching program.

(8) For any litigation based on allegations of inaccurate records, an explanation of the steps the agency used to ensure the integrity of its data as well as the verification process it used in the matching program, including an assessment of the adequacy of each.

c. New and Altered System of Records Report. The Act requires agencies to publish notices in the Federal Register describing new or altered systems of records, and to submit reports to OMB, and to the Chair of the Committee on Government Reform and Oversight of the House of Representatives, and the Chair of the Committee on Governmental Affairs of the Senate. The reports must be transmitted at least 40 days prior to the operation of the new system of records or the date on which the alteration to an existing system takes place.

(1) Which Alterations Require a Report. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis or deleting a routine use when there is no longer a need for the disclosure. The following changes are those for which a report is required:

(a) A significant increase in the number, type, or category of individuals about whom records are maintained. For example, a system covering physicians that has been expanded to include other types of health care providers, e.g., nurses, technicians, etc., would require a report. Increases attributable to normal growth should not be reported.

(b) A change that expands the types or categories of information maintained. For example, a benefit system which originally included only earned income information that has been expanded to include unearned income information.

(c) A change that alters the purpose for which the information is used.

(d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system of records. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report.

(e) The addition of an exemption pursuant to Section (j) or (k) of the Act. Note that, in examining a rulemaking for a Privacy Act exemption as part of a report of a new or altered system of records, OMB will also review the rule under applicable regulatory review procedures and agencies need not make a separate submission for that purpose.

(f) The addition of a routine use pursuant to 5 U.S.C. 552a(b)(3).

(2) Reporting Changes to Multiple Systems of Records. When an agency makes a change to an information technology installation or a telecommunication network, or makes any other general changes in information collection, processing, dissemination, or storage that affect multiple systems of records, it may submit a single, consolidated report, with changes to existing notices and supporting documentation included in the submission.

(3) Contents of the New or Altered System Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the system of records. The letter should contain the agency's assurance that the proposed system does not duplicate any existing agency or government-wide systems of records. The letter sent to OMB may also include a request for waiver of the time

period for the review. The agency should indicate why it cannot meet the established review period and the consequences of not obtaining the waiver. (See paragraph 4e below.) There is no prescribed format for the letter.

(b) Narrative Statement. There is also no prescribed format for the narrative statement, but it should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1. Describe the purpose for which the agency is establishing the system of records.

2. Identify the authority under which the system of records is maintained. The agency should avoid citing housekeeping statutes, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, the agency may, however, cite a general housekeeping statute that authorizes the agency head to keep such records as necessary.

3. Provide the agency's evaluation of the probable or potential effect of the proposal on the privacy of individuals.

4. Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be made available to OMB upon request.

5. Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine use.

6. Provide OMB Control Numbers, expiration dates, and titles of any information collection requests (e.g., forms, surveys, etc.) contained in the system of records and approved by OMB under the Paperwork Reduction Act. If the request for OMB clearance of an information collection is pending, the agency may simply state the title of the collection and the date it was submitted for OMB clearance.

(c) Supporting Documentation. Attach the following to all new or altered system of records reports:

1. A copy of the new or altered system of records notice consistent with the provisions of 5 U.S.C. 552a(e)(4). The notice must appear in the format prescribed by the Office of the Federal Register's *Document Drafting Handbook*. For proposed altered systems the agency should supply a copy of the original system of records notice to ensure that reviewers can understand the changes proposed. If the sole change to an existing system of records is to add a routine use, the agency should either republish the entire system of records notice, a condensed description of the system of records, or a citation to the last full text Federal Register publication.

2. A copy in Federal Register format of any new exemption rules or changes to published rules (consistent with the provisions of 5 U.S.C. 552a(f),(j), or (k)) that the agency proposes to issue for the new or altered system.

(4) OMB Review. OMB will review reports under 5 U.S.C. 552a(r) and provide comments if appropriate. Agencies may assume that OMB concurs in the Privacy Act aspects of their proposal if OMB has not commented within 40 days from the date the transmittal letter was signed. Agencies should ensure that letters are transmitted expeditiously after they are signed.

(5) Timing of Systems of Records Reports. Agencies may publish system of records and routine use notices as well as proposed exemption rules in the Federal Register at the same time that they send the new or altered system report to OMB and Congress. The period for OMB and congressional review and the notice and comment period for routine uses and exemptions will then run concurrently. Note that exemptions must be published as final rules before they are effective.

d. New or Altered Matching Program Report. The Act requires agencies to publish notices in the Federal Register describing new or altered matching programs, and to submit reports to OMB, and to Congress. The report must be received at least 40 days prior to the initiation of any matching activity carried out under a new or substantially altered matching program. For renewals of continuing programs, the report must be dated at least 40 days prior to the expiration of any existing matching agreement.

(1) When to Report Altered Matching Programs. Agencies need not report minor changes to matching programs. The term ''minor change to a matching program'' means a change that does not significantly alter the terms of the agreement under which the program is being carried out. Examples of significant changes include:

(a) Changing the purpose for which the program was established.

(b) Changing the matching population, either by including new categories of record subjects or by greatly increasing the numbers of records matched.

(c) Changing the legal authority covering the matching program.

(d) Changing the source or recipient agencies involved in the matching program.

(2) Contents of New or Altered Matching Program Report. The report for a new or altered matching program has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed Federal Register notice.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Privacy Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the matching program. The letter should state that a copy of the matching agreement has been distributed to Congress as the Act requires. The letter to OMB may also include a request for waiver of the review time period. (See 4e below.)

(b) Narrative Statement. There is no prescribed format for the narrative statement, but it should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should provide:

1. A description of the purpose of the matching program and the authority under which it is being carried out.

2. A description of the security safeguards used to protect against any unauthorized access or disclosure of records used in the match.

3. If the cost/benefit analysis required by Section (u)(4)(A) indicated an unfavorable ratio or was waived pursuant to OMB guidance, an explanation of the basis on which the agency justifies conducting the match.

(c) Supporting Documentation. Attach the following:

1. A copy of the Federal Register notice describing the matching program. The notice must appear in the format prescribed by the Office of the Federal Register's *Document Drafting Handbook*. (See 5b (3).)

2. For the Congressional report only, a copy of the matching agreement.

(3) OMB Review. OMB will review reports under 5 U.S.C. 552a(r) and provide comments if appropriate. Agencies may assume that OMB concurs in the Privacy Act aspects of their proposal if OMB has not commented within 40 days from the date the transmittal letter was signed.

(4) Timing of Matching Program Reports. Agencies should ensure that letters are transmitted expeditiously after they are signed. Agencies may publish matching program notices in the Federal Register at the same time that they send the matching program report to OMB and Congress. The period for OMB and congressional review and the notice and comment period will then run concurrently.

e. Expedited Review. The Director, OMB, may grant a waiver of the 40-day review period for either systems of records or matching program reviews. The agency must ask for the waiver in the transmittal letter and demonstrate compelling reasons. When a waiver is granted, the agency is not thereby relieved of any other requirement of the Act. If no waiver is granted, agencies may presume concurrence at the expiration of the 40 day review period if OMB has not commented by that time. Note that OMB cannot waive time periods specifically established by the Act such as the 30 days notice and comment period required for the adoption of a routine use proposal pursuant to Section (b)(3) of the Act.

5. Publication Requirements. The Privacy Act requires agencies to publish notices or rules in the Federal Register in the following circumstances: when adopting a new or altered system of records, when adopting a routine use, when adopting an exemption for a system of records, or when proposing to carry out a new or altered matching program. (See paragraph 4c(1) and 4d(1) above on what constitutes an alteration requiring a report to OMB and the Congress.)

a. Publishing New or Altered Systems of Records Notices and Exemption Rules.

(1) Who Publishes. The agency responsible for operating the system of records makes the necessary publication. Publication should be carried out at the departmental or agency level. Even where a system of records is to

be operated exclusively by a component, the department rather than the component should publish the notice. Thus, for example, the Department of the Treasury would publish a system of records notice covering a system operated exclusively by the Internal Revenue Service. Note that if the agency is proposing to exempt the system under Section (j) or (k) of the Act, it must publish a rule in addition to the system of records notice.

(a) Government-wide Systems of Records. Certain agencies publish systems of records containing records for which they have government-wide responsibilities. The records may be located in other agencies, but they are being used under the authority of and in conformance with the rules mandated by the publishing agency. The Office of Personnel Management, for example, has published a number of government-wide systems of records relating to the operation of the government's personnel program. Agencies should not publish systems of records that wholly or partly duplicate existing government-wide systems of records.

(b) Section (m) Contract Provisions. When an agency provides by contract for the operation of a system of records, it should ensure that a system of records notice describing the system has been published. It should also review the notice to ensure that it contains a routine use under Section (e)(4)(D) of the Act permitting disclosure to the contractor and his or her personnel.

(2) When to Publish.

(a) System Notice. The system of records notice must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information.

(b) Routine Use. A routine use must be published in the Federal Register 30 days before the agency discloses records pursuant to its terms. (Note that the addition of a routine use to an existing system of records requires a report to OMB and Congress, and that the review period for this report is 40 days.)

(c) Exemption Rule. A rule exempting a system of records under (j) or (k) or the Act must be established through informal rulemaking pursuant to the Administrative Procedure Act. This process generally requires publication of a proposed rule, a period during which the public may comment, publication of a final rule, and the adoption of the final rule. Agencies may not withhold records under an exemption until these requirements have been met.

(3) Format. Agencies should follow the publication format contained in the Office of the Federal Register's *Document Drafting Handbook* which may be obtained from the Government Printing Office.

b. Publishing Matching Notices.

(1) Who Publishes. Generally, the recipient Federal agency (or the Federal source agency in a match conducted by a nonfederal agency) is responsible for publishing in the Federal Register a notice describing the new or altered matching program. However, in large, multi-agency matching programs, where the recipient agency is merely performing the matches, and the benefit accrues to the source agencies, the partners should assign responsibility for compliance with the administrative requirements in a fair and reasonable way. This may mean having the matching agency carry out these requirements for all parties, having one participant designated to do so, or having each source agency do so for its own matching program(s).

(2) Timing. Publication must occur at least 30 days prior to the initiation of any matching activity carried out under a new or substantially altered matching program. For renewals of programs agencies wish to continue past the 30 month period of initial eligibility (i.e., the initial 18 months plus a one year extension), publication must occur at least 30 days prior to the expiration of the existing matching agreement. (But note that a report to OMB and the Congress is also required with a 40 day review period).

(3) Format. The matching notice shall be in the format prescribed by the Office of the Federal Register's Document Drafting Handbook and contain the following information:

(a) The name of the Recipient Agency.

(b) The Name(s) of the Source Agencies.

(c) The beginning and ending dates of the match.

(d) A brief description of the matching program, including its purpose; the legal authorities authorizing its operation; categories of individuals involved; and identification of records used, including name(s) of Privacy Act Systems of records.

(e) The identification, address, and telephone number of a Recipient Agency official who will answer public inquiries about the program.

Appendix II to OMB Circular No. A–130—Cost Accounting, Cost Recovery, and Interagency Sharing of Information Technology Facilities

[The guidance formerly found in Appendix II has been revised and placed in Section 8b. See, Transmittal No. 2, 59 FR 37906. Appendix II has been deleted and is reserved for future topics.]

Appendix III to OMB Circular No. A–130—Security of Federal Automated Information Resources

A. Requirements

1. *Purpose*

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A–123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A–130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100–235) and responsibilities assigned in applicable national security directives.

2. *Definitions*

The term:

a. ''Adequate security'' means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

b. ''Application'' means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. ''General support system'' or ''system'' means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

d. ''Major application'' means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. *Automated Information Security Programs.* Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

a. Controls for general support systems.

(1) *Assign Responsibility for Security.* Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

(2) *System Security Plan.* Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent

with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans shall include:

(a) *Rules of the System.* Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

(b) *Training.* Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.

(c) *Personnel Controls.* Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

(d) *Incident Response Capability.* Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

(e) *Continuity of Support.* Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

(f) *Technical Security.* Ensure that cost-effective security products and techniques are appropriately used within the system.

(g) *System Interconnection.* Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

(3) *Review of Security Controls.* Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A–123, ''Management Accountability and Control'' and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

(4) *Authorize Processing.* Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

b. Controls for Major Applications.

(1) *Assign Responsibility for Security.* Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

(2) *Application Security Plan.* Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include:

(a) *Application Rules.* Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

(b) *Specialized Training.* Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

(c) *Personnel Security.* Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the application and periodically thereafter.

(d) *Contingency Planning.* Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

(e) *Technical Controls.* Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

(f) *Information Sharing.* Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.

(g) *Public Access Controls.* Where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.

(3) *Review of Application Controls.* Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A–123, ''Management Accountability and Control'' and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

(4) *Authorize Processing.* Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

4. *Assignment of Responsibilities*

a. *Department of Commerce.* The Secretary of Commerce shall:

(1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

(2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

(3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

(4) Provide guidance and assistance, as appropriate, to agencies concerning cost-effective controls when interconnecting with other systems.

(5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

(6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

b. *Department of Defense.* The Secretary of Defense shall:

(1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

(2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

c. *Department of Justice.* The Attorney General shall:

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

(2) Pursue appropriate legal actions when security incidents occur.

d. *General Services Administration.* The Administrator of General Services shall:

(1) Provide guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended).

(2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services).

(3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

e. *Office of Personnel Management.* The Director of the Office of Personnel Management shall:

(1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

(2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

f. *Security Policy Board.* The Security Policy Board shall coordinate the activities of the Federal government regarding the security of information technology that processes classified information in accordance with applicable national security directives;

5. *Correction of Deficiencies and Reports*

a. *Correction of Deficiencies.* Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. *Reports on Deficiencies.* In accordance with OMB Circular No. A–123, ''Management Accountability and Control'', if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the appropriate agency level.

c. *Summaries of Security Plans.* Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act (44 U.S.C. 3506).

B. Descriptive Information

The following descriptive language is explanatory. It is included to assist in understanding the requirements of the Appendix.

The Appendix re-orients the Federal computer security program to better respond to a rapidly changing technological environment. It establishes government-wide responsibilities for Federal computer security and requires Federal agencies to adopt a minimum set of management controls. These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology.

For security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as an integral part of overall planning.

''Adequate security'' is defined as ''security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.'' This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in ''An Introduction to Computer Security: The NIST Handbook'' (March 16, 1995).

Discussion of the Appendix's Major Provisions. The following discussion is provided to aid reviewers in understanding the changes in emphasis in the Appendix.

Automated Information Security Programs. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. This Appendix emphasizes management controls affecting individual users of information technology. Technical and operational controls support management controls. To be effective, all must interrelate. For example, authentication of individual users is an important management control, for which password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

Four controls are set forth: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. The Appendix requires that these management controls be applied in two areas of management responsibility: one for general support systems and one for major applications.

The terms ''general support system'' and ''major application'' were used in OMB Bulletins Nos. 88–16 and 90–08. A general support system is ''an interconnected set of information resources under the same direct management control which shares common functionality.'' Such a system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support.

A major application is a use of information and information technology to satisfy a specific set of user requirements that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. All applications require some level of security, and adequate security for most of them should be provided by security of the general support systems in which they operate. However, certain applications, because of the nature of the information in them, require special management oversight and should be treated as major. Agencies are expected to exercise management judgement in determining which of their applications are major.

The focus of OMB Bulletins Nos. 88–16 and 90–08 was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information, and focuses extra security controls on a limited number of particularly high-risk or major applications.

a. *General Support Systems.* The following controls are required in all general support systems:

(1) *Assign Responsibility for Security.* For each system, an individual should be a focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. That responsibility should be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls such as user identification and authentication.

(2) *Security Plan.* The Computer Security Act requires that security plans be developed for all Federal computer systems that contain sensitive information. Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality, and therefore all systems require security plans.

Previous guidance on security planning was contained in OMB Bulletin No. 90–08. This Appendix supersedes OMB Bulletin 90–08 and expands the coverage of security plans from Bulletin 90–08 to include rules of individual behavior as well as technical security. Consistent with OMB Bulletin 90–08, the Appendix directs NIST to update and expand security planning guidance and issue it as a Federal Information Processing Standard (FIPS). In the interim, agencies should continue to use the Appendix of OMB Bulletin No. 90–08 as guidance for the technical portion of their security plans.

The Appendix continues the requirement that independent advice and comment on the security plan for each system be sought. The intent of this requirement is to improve the plans, foster communication between managers of different systems, and promote the sharing of security expertise.

This Appendix also continues the requirement from the Computer Security Act that summaries of security plans be included in agency strategic information resources management plans. OMB will provide additional guidance about the contents of those strategic plans, pursuant to the Paperwork Reduction Act of 1995.

The following specific security controls should be included in the security plan for a general support system:

(a) *Rules.* An important new requirement for security plans is the establishment of a set of rules of behavior for individual users of each general support system. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in ''An Introduction to Computer Security: The NIST Handbook'' (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training.

The development of rules for a system must take into consideration the needs of all parties who use the system. Rules should be as stringent as necessary to provide adequate security. Therefore, the acceptable level of risk for the system must be established and should form the basis for determining the rules.

Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Often rules should reflect technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Rules may be enforced through administrative sanctions specifically related to the system (e.g. loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

(b) *Training.* The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior—the rules of the system—before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules.

To assist agencies, the Appendix requires NIST, with assistance from the Office of Personnel Management (OPM), to update its existing guidance. It also proposes that OPM assure that its rules for computer security training for Federal civilian employees are effective.

(c) *Personnel Controls.* It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, ''least privilege,'' and separation of duties.

Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users.

Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Nevertheless, in some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of harm is high.

(d) *Incident Response Capability.* Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide.

The Appendix also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

(e) *Continuity of Support.* Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service.

Decisions on the level of service needed at any particular time and on priorities in service restoration should be made in consultation with the users of the system and incorporated in the system rules. Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.

(f) *Technical Security.* Agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. Often such techniques will correspond with system rules of behavior, such as in the proper use of password protection.

The Appendix directs NIST to continue to issue computer security guidance to assist agencies in planning for and using technical security products and techniques. Until such guidance is issued, however, the planning guidance included in OMB Bulletin 90–08 can assist in determining techniques for

effective security in a system and in addressing technical controls in the security plan.

(g) *System Interconnection.* In order for a community to effectively manage risk, it must control access to and from other systems. The degree of such control should be established in the rules of the system and all participants should be made aware of any limitations on outside access. Technical controls to accomplish this should be put in place in accordance with guidance issued by NIST.

There are varying degrees of how connected a system is. For example, some systems will choose to isolate themselves, others will restrict access such as allowing only e-mail connections or remote access only with sophisticated authentication, and others will be fully open. The management decision to interconnect should be based on the availability and use of technical and non-technical safeguards and consistent with the acceptable level of risk defined in the system rules.

(3) *Review of Security Controls.* The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A–123, ''Management Accountability and Control'' and the Federal Managers' Financial Integrity Act. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

(4) *Authorize Processing.* The authorization of a system to process information, granted by a management official, provides an important quality control (some agencies refer to this authorization as accreditation). By authorizing processing in a system, a manager accepts the risk associated with it. Authorization is not a decision that should be made by the security staff.

Both the security official and the authorizing management official have security responsibilities. In general, the security official is closer to the day-to-day operation of the system and will direct or perform security tasks. The authorizing official will normally have general responsibility for the organization supported by the system.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, the periodic review of controls should also contribute to future authorizations. Some agencies perform ''certification reviews'' of their systems periodically. These formal technical evaluations lead to a management accreditation, or ''authorization to process.'' Such certifications (such as those using the methodology in FIPS Pub 102 ''Guideline for Computer Security Certification and Accreditation'') can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by the Appendix.

Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

b. *Controls in Major Applications.* Certain applications require special management attention due to the risk and magnitude of harm that could occur. For such applications, the controls of the support system(s) in which they operate are likely to be insufficient. Therefore, additional controls specific to the application are required. Since the function of applications is the direct manipulation and use of information, controls for securing applications should emphasize protection of information and the way it is manipulated.

(1) *Assign Responsibility for Security.* By definition, major applications are high risk and require special management attention. Major applications usually support a single agency function and often are supported by more than one general support system. It is important, therefore, that an individual be assigned responsibility in writing to assure that the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

(2) *Application Security Plans.* Security for each major application should be addressed by a security plan specific to the application. The plan should include controls specific to protecting information and should be developed from the application manager's perspective. To assist in assuring its viability, the plan should be provided to the manager of the primary support system which the application uses for advice and comment. This recognizes the critical dependence of the security of major applications on the underlying support systems they use. Summaries of application security plans should be included in strategic information resource management plans in accordance with this Circular.

(a) *Application Rules.* Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

(b) *Specialized Training.* Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

(c) *Personnel Security.* For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware that there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties that an individual may perform.

(d) *Contingency Planning.* Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable back-up option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

(e) *Technical Controls.* Technical security controls, for example tests to filter invalid entries, should be built into each application. Often these controls will correspond with the rules of behavior for the application. Under the previous Appendix, application security was focused on the process by which sensitive, custom applications were developed. While that process is not addressed in detail in this Appendix, it remains an effective method for assuring that security controls are built into applications. Additionally, the technical security controls defined in OMB Bulletin No. 90–08 will continue, until that guidance is replaced by NIST's security planning guidance.

(f) *Information Sharing.* Assure that information which is shared with Federal

organizations, State and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application. Controls on the information may stay the same or vary when the information is shared with another entity. For example, the primary user of the information may require a high level of availability while the secondary user does not, and can therefore relax some of the controls designed to maintain the availability of the information. At the same time, however, the information shared may require a level of confidentiality that should be extended to the secondary user. This normally requires notification and agreement to protect the information prior to its being shared.

(g) *Public Access Controls.* Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as ''firewalls'' that are put in place for security of the general support system.

In general, it is more difficult to apply conventional controls to public access systems, because many of the users of the system may not be subject to individual accountability policies. In addition, public access systems may be a target for mischief because of their higher visibility and published access methods.

Official records need to be protected against loss or alteration. Official records in electronic form are particularly susceptible since they can be relatively easy to change or destroy. Therefore, official records should be segregated from information made directly accessible to the public. There are different ways to segregate records. Some agencies and organizations are creating dedicated information dissemination systems (such as bulletin boards or World Wide Web servers) to support this function. These systems can be on the outside of secure gateways which protect internal agency records from outside access.

In order to secure applications that allow direct public access, conventional techniques such as least privilege (limiting the processing capability as well as access to data) and integrity assurances (such as checking for viruses, clearly labeling the age of data, or periodically spot checking data) should also be used. Additional guidance on securing public access systems is available from NIST Computer Systems Laboratory Bulletin ''Security Issues in Public Access Systems'' (May, 1993).

(3) *Review of Application Controls.* At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application. A deficiency in any of these controls should be considered a deficiency pursuant to the Federal Manager's Financial Integrity Act and OMB Circular No. A–123, ''Management Accountability and Control.''

The review envisioned here is different from the system test and certification process required in the current Appendix. That process, however, remains useful for assuring that technical security features are built into custom-developed software applications. While the controls in that process are not specifically called for in this Appendix, they remain in Bulletin No. 90–08, and are recommended in appropriate circumstances as technical controls.

(4) *Authorize Processing.* A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high. The intent of this requirement is to assure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. The authorization should be based on the application security plan and any review(s) performed on the application. It should also take into account the risks from the general support systems used by the application.

4. *Assignment of Responsibilities.* The Appendix assigns government-wide responsibilities to agencies that are consistent with their missions and the Computer Security Act.

a. *Department of Commerce.* The Department of Commerce, through NIST, is assigned the following responsibilities consistent with the Computer Security Act.

(1) Develop and issue security standards and guidance.

(2) Review and update, with assistance from OPM, the guidelines for security training issued in 1988 pursuant to the Computer Security Act to assure they are effective.

(3) Replace and update the technical planning guidance in the appendix to OMB Bulletin 90–08 This should include guidance on effective risk-based security absent a formal risk analysis.

(4) Provide agencies with guidance and assistance concerning effective controls for systems when interconnecting with other systems, including the Internet. Such guidance on, for example, so-called ''firewalls'' is becoming widely available and is critical to agencies as they consider how to interconnect their communications capabilities.

(5) Coordinate agency incident response activities. Coordination of agency incident response activities should address both threats and vulnerabilities as well as improve the ability of the Federal government for rapid and effective cooperation in response to serious security breaches.

(6) Assess security vulnerabilities in new information technologies and apprise Federal agencies of such vulnerabilities. The intent of this new requirement is to help agencies understand the security implications of technology before they purchase and field it. In the past, there have been too many instances where agencies have acquired and implemented technology, then found out about vulnerabilities in the technology and had to retrofit security measures. This activity is intended to help avoid such difficulties in the future.

b. *Department of Defense.* The Department, through the National Security Agency, should provide technical advice and assistance to NIST, including work products such as technical security guidelines, which NIST can draw upon for developing standards and guidelines for protecting sensitive information in Federal computers.

Also, the Department, through the National Security Agency, should assist NIST in evaluating vulnerabilities in emerging technologies. Such vulnerabilities may present a risk to national security information as well as to unclassified information.

c. *Department of Justice.* The Department of Justice should provide appropriate guidance to Federal agencies on legal remedies available to them when serious security incidents occur. Such guidance should include ways to report incidents and cooperate with law enforcement.

In addition, the Department should pursue appropriate legal actions on behalf of the Federal government when serious security incidents occur.

d. *General Services Administration.* The General Services Administration should provide agencies guidance for addressing security considerations when acquiring information technology products or services. This continues the current requirement.

In addition, where cost-effective to do so, GSA should establish government-wide contract vehicles for agencies to use to acquire certain security services. Such vehicles already exist for providing system back-up support and conducting security analyses.

GSA should also provide appropriate security services to assist Federal agencies to the extent that provision of such services is cost-effective. This includes providing, in conjunction with the Department of Defense and the Department of Commerce, appropriate services which support Federal use of the National Information Infrastructure (e.g., use of digital signature technology).

e. *Office of Personnel Management.* In accordance with the Computer Security Act, OPM should review its regulations concerning computer security training and assure that they are effective.

In addition, OPM should assist the Department of Commerce in the review and update of its computer security awareness and training guidelines. OPM worked closely with NIST in developing the current guidelines and should work with NIST in revising those guidelines.

f. *Security Policy Board.* The Security Policy Board is assigned responsibility for national security policy coordination in accordance with the appropriate Presidential directive. This includes policy for the security of information technology used to process classified information.

Circular A–130 and this Appendix do not apply to information technology that supports certain critical national security

missions, as defined in 44 U.S.C. 3502 (9) and 10 U.S.C. 2315. Policy and procedural requirements for the security of national security systems (telecommunications and information systems that contain classified information or that support those critical national security missions (44 U.S.C. 3502 (9) and 10 U.S.C. 2315)) is assigned to the Department of Defense pursuant to Presidential directive. The Circular clarifies that information classified for national security purposes should also be handled in accordance with appropriate national security directives. Where classified information is required to be protected by more stringent security requirements, those requirements should be followed rather than the requirements of this Appendix.

5. *Reports.* The Appendix requires agencies to provide two reports to OMB:

The first is a requirement that agencies report security deficiencies and material weaknesses within their FMFIA reporting mechanisms as defined by OMB Circular No. A–123, ''Management Accountability and Control,'' and take corrective actions in accordance with that directive.

The second, defined by the Computer Security Act, requires that a summary of agency security plans be included in the information resources management plan required by the Paperwork Reduction Act.

Appendix IV to OMB Circular No. A–130—Analysis of Key Sections

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 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 of the Act provides authority to the Director, 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 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.

In addition, the Circular revises and consolidates policy and procedures in seven previous OMB directives and rescinds those directives, as follows:

A–3—Government Publications.

A–71—Responsibilities for the Administration and Management of Automatic Data Processing Activities Transmittal Memorandum No. 1 to Circular No. A–71—Security of Federal Automated Information Systems.

A–90—Cooperating with State and Local Governments to Coordinate and Improve Information Systems.

A–108—Responsibilities for the Maintenance of Records about Individuals by Federal Agencies

A–114—Management of Federal Audiovisual Activities

A–121—Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities

3. Analysis

Section 6, Definitions. Access and Dissemination. The original Circular No. A–130 distinguished between the terms ''access to information'' and ''dissemination of information'' in order to separate statutory requirements from policy considerations. The first term means giving members of the public, at their request, information to which they are entitled by a law such as the FOIA. The latter means actively distributing information to the public at the initiative of the agency. The distinction appeared useful at the time Circular No. A–130 was written, because it allowed OMB to focus discussion on Federal agencies' responsibilities for actively distributing information. However, popular usage and evolving technology have blurred differences between the terms ''access'' and ''dissemination'' and readers of the Circular were confused by the distinction. For example, if an agency ''disseminates'' information via an on-line computer system, one speaks of permitting users to ''access'' the information, and on-line ''access'' becomes a form of ''dissemination.''

Thus, the revision defines only the term ''dissemination.'' Special considerations based on access statutes such as the Privacy Act and the FOIA are explained in context.

Government Information. The definition of ''government information'' includes information created, collected, processed, disseminated, or disposed of both by and for the Federal Government. This recognizes the increasingly distributed nature of information in electronic environments. Many agencies, in addition to collecting information for government use and for dissemination to the public, require members of the public to maintain information or to disclose it to the public. Sound information resources management dictates that agencies consider the costs and benefits of a full range of alternatives to meet government objectives. In some cases, there is no need for the government actually to collect the information itself, only to assure that it is made publicly available. For example, banks insured by the FDIC must provide statements of financial condition to bank customers on request. Particularly when information is available in electronic form, networks make the physical location of information increasingly irrelevant.

The inclusion of information created, collected, processed, disseminated, or disposed of for the Federal Government in the definition of ''government information'' does not imply that responsibility for implementing the provisions of the Circular itself extends beyond the executive agencies to other entities. Such an interpretation would be inconsistent with Section 4, Applicability, and with existing law. For example, the courts have held that requests to Federal agencies for release of information under the FOIA do not always extend to those performing information activities under grant or contract to a Federal agency. Similarly, grantees may copyright information where the government may not. Thus the information responsibilities of grantees and contractors are not identical to those of Federal agencies except to the extent that the agencies make them so in the underlying grants or contracts. Similarly, agency information resources management responsibilities do not extend to other entities.

Information Dissemination Product. This notice defines the term ''information dissemination product'' to include all information that is disseminated by Federal agencies. While the provision of access to on-line databases and search software included on compact disk, read-only memory (CD-ROM) are often called information services rather than products, there is no clear distinction and, moreover, no real difference for policy purposes between the two. Thus, the term ''information dissemination product'' applies to both products and services, and makes no distinction based on how the information is delivered.

Section 8a(1). Information Management Planning. Parallel to new Section 7, Basic Considerations and Assumptions, Section 8a begins with information resources management planning. Planning is the process of establishing a course of action to achieve desired results with available resources. Planners translate organizational missions into specific goals and, in turn, into measurable objectives.

The PRA introduced the concept of information resources management and the principle of information as an institutional resource which has both value and associated costs. Information resources management is a tool that managers use to achieve agency objectives. Information resources management is successful if it enables managers to achieve agency objectives efficiently and effectively.

Information resources management planning is an integral part of overall mission

planning. Agencies need to plan from the outset for the steps in the information life cycle. When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, how they will protect its integrity, what provisions they will make for access to it, whether and how they will disseminate it, how they will store and retrieve it, and finally, how the information will ultimately be disposed of. They must also plan for the effects their actions and programs will have on the public and State and local governments.

The Role of State and Local Governments. OMB made additions at Sections 7a, 7e, and 7j, Basic Considerations and Assumptions, concerning State and local governments, and also in policy statements at Sections 8a(1)(c), (3)(f), (5)(d)(iii), and (8)(e).

State and local governments, and tribal governments, cooperate as major partners with the Federal Government in the collection, processing, and dissemination of information. For example, State governments are the principal collectors and/or producers of information in the areas of health, welfare, education, labor markets, transportation, the environment, and criminal justice.

The States supply the Federal Government with data on aid to families with dependent children; medicare; school enrollments, staffing, and financing; statistics on births, deaths, and infectious diseases; population related data that form the basis for national estimates; employment and labor market data; and data used for census geography. National information resources are greatly enhanced through these major cooperating efforts.

Federal agencies need to be sensitive to the role of State and local governments, and tribal governments, in managing information and in managing information technology. When planning, designing, and carrying out information collections, agencies should systematically consider what effect their activities will have on cities, counties, and States, and take steps to involve these governments as appropriate. Agencies should ensure that their information collections impose the minimum burden and do not duplicate or conflict with local efforts or other Federal agency requirements or mandates. The goal is that Federal agencies routinely integrate State and local government concerns into Federal information resources management practices. This goal is consistent with standards for State and local government review of Federal policies and programs.

Training. Training is particularly important in view of the changing nature of information resources management. Decentralization of information technology has placed the management of automated information and information technology directly in the hands of nearly all agency personnel rather than in the hands of a few employees at centralized facilities. Agencies must plan for incorporating policies and procedures regarding computer security, records management, protection of privacy, and other safeguards into the training of every employee and contractor.

Section 8a(2). Information Collection. The PRA requires that the creation or collection of information be carried out in an efficient, effective, and economical manner. When Federal agencies create or collect information—just as when they perform any other program functions—they consume scarce resources. Such activities must be continually evaluated for their relevance to agency missions.

Agencies must justify the creation or collection of information based on their statutory functions. Policy statement 8a(2) uses the justification standard—''necessary for the proper performance of the functions of the agency''—established by the PRA (44 U.S.C. 3508). Furthermore, the policy statement includes the requirement that the information have practical utility, as defined in the PRA (44 U.S.C. 3502(11)) and elaborated in 5 CFR Part 1320. Practical utility includes such qualities of information as accuracy, adequacy, and reliability. In the case of general purpose statistics or recordkeeping, practical utility means that actual uses can be demonstrated (5 CFR 1320.3(l)). It should be noted that OMB's intent in placing emphasis on reducing unjustified burden in collecting information, an emphasis consistent with the Act, is not to diminish the importance of collecting information whenever agencies have legitimate program reasons for doing so. Rather, the concern is that the burdens imposed should not exceed the benefits to be derived from the information. Moreover, if the same benefit can be obtained by alternative means that impose a lesser burden, that alternative should be adopted.

Section 8a(3). Electronic Information Collection. Section 7l articulates a basic assumption of the Circular that modern information technology can help the government provide better service to the public through improved management of government programs. One potentially useful application of information technology is in the government's collection of information. While some information collections may not be good candidates for electronic techniques, many are. Agencies with major electronic information collection programs have found that automated information collections allow them to meet program objectives more efficiently and effectively. Electronic data interchange (EDI) and related standards for the electronic exchange of information will ease transmission and processing of routine business transaction information such as invoices, purchase orders, price information, bills of lading, health insurance claims, and other common commercial documents. EDI holds similar promise for the routine filing of regulatory information such as tariffs, customs declarations, license applications, tax information, and environmental reports.

Benefits to the public and agencies from electronic information collection appear substantial. Electronic methods of collection reduce paperwork burden, reduce errors, facilitate validation, and provide increased convenience and more timely receipt of benefits.

The policy in Section 8a(3) encourages agencies to explore the use of automated techniques for collection of information, and sets forth conditions conducive to the use of those techniques.

Section 8a(4). Records Management. Section 8a(4) begins with the fundamental requirement for Federal records management, namely, that agencies create and keep adequate and proper documentation of their activities. Federal agencies cannot carry out their missions in a responsible and responsive manner without adequate recordkeeping. Section 7h articulates the basic considerations concerning records management. Policy statements concerning records management are also interwoven throughout Section 8a, particularly in subsections on planning (8a(1)(j)), information dissemination (8a(6)), and safeguards (8a(9)).

Records support the immediate needs of government—administrative, legal, fiscal—and ensure its continuity. Records are essential for protecting the rights and interests of the public, and for monitoring the work of public servants. The government needs records to ensure accountability to the public which includes making the information available to the public.

Each stage of the information life cycle carries with it records management responsibilities. Agencies need to record their plans, carefully document the content and procedures of information collection, ensure proper documentation as a feature of every information system, keep records of dissemination programs, and, finally, ensure that records of permanent value are preserved.

Preserving records for future generations is the archival mission. Advances in technology affect the amount of information that can be created and saved, and the ways this information can be made available. Technological advances can ease the task of records management; however, the rapid pace of change in modern technology makes decisions about the appropriate application of technology critical to records management. Increasingly the records manager must be concerned with preserving valuable electronic records in the context of a constantly changing technological environment.

Records schedules are essential for the appropriate maintenance and disposition of records. Records schedules must be prepared in a timely fashion, implement the General Records Schedules issued by the National Archives and Records Administration, be approved by the Archivist of the United States, and be kept accurate and current. (See 44 U.S.C. 3301 et seq.) The National Archives and Records Administration and the General Services Administration provide guidance and assistance to agencies in implementing records management responsibilities. They also evaluate agencies' records management programs to determine the extent to which they are appropriately implementing their records management responsibilities.

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

The FOIA requires each agency to publish in the Federal Register current descriptions

of agency organization, where and how the public may obtain information, the general methods and procedural requirements by which agency functions are determined, rules of procedure, descriptions of forms and how to obtain them, substantive regulations, statements of general policy, and revisions to all the foregoing (5 U.S.C. 552(a)(1)). The Privacy Act also requires publication of information concerning ''systems of records'' which are records retrieved by individual identifier such as name, Social Security Number, or fingerprint. The Government in the Sunshine Act requires agencies to publish meeting announcements (5 U.S.C. 552b (e)(1)). The PRA (44 U.S.C. 3507(a)(2)) and its implementing regulations (5 CFR Part 1320) require agencies to publish notices when they submit information collection requests for OMB approval. The public's right of access to government information under these statutes is balanced against other concerns, such as an individual's right to privacy and protection of the government's deliberative process.

As agencies satisfy these requirements, they provide the public basic information about government activities. Other statutes direct specific agencies to issue specific information dissemination products or to conduct information dissemination programs. Beyond generic and specific statutory requirements, agencies have responsibilities to disseminate information as a necessary part of performing their functions. For some agencies the responsibility is made explicit and sweeping; for example, the Agriculture Department is directed to ''. . . diffuse among people of the United States, useful information on subjects connected with agriculture. . . .'' (7 U.S.C. 2201) For other agencies, the responsibility may be much more narrowly drawn.

Information dissemination is also a consequence of other agency activities. Agency programs normally include an organized effort to inform the public about the program. Most agencies carry out programs that create or collect information with the explicit or implicit intent that the information will be made public. Disseminating information is in many cases the logical extension of information creation or collection.

In other cases, agencies may have information that is not meant for public dissemination but which may be the subject of requests from the public. When the agency establishes that there is public demand for the information and that it is in the public interest to disseminate the information, the agency may decide to disseminate it automatically.

The policy in Section 8a(5)(d) sets forth several factors for agencies to take into account in conducting their information dissemination programs. First, agencies must balance two goals: maximizing the usefulness of the information to the government and the public, and minimizing the cost to both. Deriving from the basic purposes of the PRA (44 U.S.C. 3501), the two goals are frequently in tension because increasing usefulness usually costs more. Second, Section 8a(5)(d)(ii) requires agencies to conduct information dissemination programs equitably and in a timely manner. The word ''equal'' was removed from this Section since there may be instances where, for example, an agency determines that its mission includes disseminating information to certain specific groups or members of the public, and the agency determines that user charges will constitute a significant barrier to carrying out this responsibility.

Section 8a(5)(d)(iii), requiring agencies to take advantage of all dissemination channels, recognizes that information reaches the public in many ways. Few persons may read a Federal Register notice describing an agency action, but those few may be major secondary disseminators of the information. They may be affiliated with publishers of newspapers, newsletters, periodicals, or books; affiliated with on-line database providers; or specialists in certain information fields. While millions of information users in the public may be affected by the agency's action, only a handful may have direct contact with the agency's own information dissemination products. As a deliberate strategy, therefore, agencies should cooperate with the information's original creators, as well as with secondary disseminators, in order to further information dissemination goals and foster a diversity of information sources. An adjunct responsibility to this strategy is reflected in Section 8a(5)(d)(iv), which directs agencies to assist the public in finding government information. Agencies may accomplish this, for example, by specifying and disseminating ''locator'' information, including information about content, format, uses and limitations, location, and means of access.

Section 8a(6). Information Dissemination Management System. This Section requires agencies to maintain an information dissemination management system which can ensure the routine performance of certain functions, including the essential functions previously required by Circular No. A–3. Smaller agencies need not establish elaborate formal systems, so long as the heads of the agencies can ensure that the functions are being performed.

Subsection (6)(a) carries over a requirement from OMB Circular No. A–3 that agencies' information dissemination products are to be, in the words of 44 U.S.C. 1108, ''necessary in the transaction of the public business required by law of the agency.'' (Circular No. A–130 uses the expression ''necessary for the proper performance of agency functions,'' which OMB considers to be equivalent to the expression in 44 U.S.C. 1108.) The point is that agencies should determine systematically the need for each information dissemination product.

Section 8a(6)(b) recognizes that to carry out effective information dissemination programs, agencies need knowledge of the marketplace in which their information dissemination products are placed. They need to know what other information dissemination products users have available in order to design the best agency product. As agencies are constrained by finite budgets, when there are several alternatives from which to choose, they should not expend public resources filling needs which have already been met by others in the public or private sector. Agencies have a responsibility not to undermine the existing diversity of information sources.

At the same time, an agency's responsibility to inform the public may be independent of the availability or potential availability of a similar information dissemination product. That is, even when another governmental or private entity has offered an information dissemination product identical or similar to what the agency would produce, the agency may conclude that it nonetheless has a responsibility to disseminate its own product. Agencies should minimize such instances of duplication but could reach such a conclusion because legal considerations require an official government information dissemination product.

Section 8a(6)(c) makes the Circular consistent with current practice (See OMB Bulletins 88–15, 89–15, 90–09, and 91–16), by requiring agencies to establish and maintain inventories of information dissemination products. (These bulletins eliminated annual reporting to OMB of title-by-title listings of publications and the requirement for agencies to obtain OMB approval for each new periodical. Publications are now reviewed as necessary during the normal budget review process.) Inventories help other agencies and the public identify information which is available. This serves both to increase the efficiency of the dissemination function and to avoid unnecessary burdens of duplicative information collections. A corollary, enunciated in Section 8a(6)(d), is that agencies can better serve public information needs by developing finding aids for locating information produced by the agencies. Finally, Section 8a(6)(f) recognizes that there will be situations where agencies may have to take appropriate steps to ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products.

Depository Library Program. Sections 8a(6)(g) and (h) pertain to the Federal Depository Library Program. Agencies are to establish procedures to ensure compliance with 44 U.S.C. 1902, which requires that government publications (defined in 44 U.S.C. 1901 and repeated in Section 6 of the Circular) be made available to depository libraries through the Government Printing Office (GPO).

Depository libraries are major partners with the Federal Government in the dissemination of information and contribute significantly to the diversity of information sources available to the public. They provide a mechanism for wide distribution of government information that guarantees basic availability to the public. Executive branch agencies support the depository library program both as a matter of law and on its merits as a means of informing the public about the government. On the other hand, the law places the administration of depository libraries with GPO. Agency responsibility for the depository libraries is limited to supplying government publications through GPO.

Agencies can improve their performance in providing government publications as well as electronic information dissemination products to the depository library program. For example, the proliferation of ''desktop publishing'' technology in recent years has afforded the opportunity for many agencies to produce their own printed documents. Many such documents may properly belong in the depository libraries but are not sent because they are not printed at GPO. The policy requires agencies to establish management controls to ensure that the appropriate documents reach the GPO for inclusion in the depository library program.

At present, few agencies provide electronic information dissemination products to the depository libraries. At the same time, a small but growing number of information dissemination products are disseminated only in electronic format.

OMB believes that, as a matter of policy, electronic information dissemination products generally should be provided to the depository libraries. Given that production and supply of information dissemination products to the depository libraries is primarily the responsibility of GPO, agencies should provide appropriate electronic information dissemination products to GPO for inclusion in the depository library program.

While cost may be a consideration, agencies should not conclude without investigation that it would be prohibitively expensive to place their electronic information dissemination products in the depository libraries. For electronic information dissemination products other than on-line services, agencies may have the option of having GPO produce the information dissemination product for them, in which case GPO would pay for depository library costs. Agencies should consider this option if it would be a cost effective alternative to the agency making its own arrangements for production of the information dissemination product. Using GPO's services in this manner is voluntary and at the agency's discretion. Agencies could also consider negotiating other terms, such as inviting GPO to participate in agency procurement orders in order to distribute the necessary copies for the depository libraries. With adequate advance planning, agencies should be able to provide electronic information dissemination products to the depository libraries at nominal cost.

In a particular case, substantial cost may be a legitimate reason for not providing an electronic information dissemination product to the depository library program. For example, for an agency with a substantial number of existing titles of electronic information dissemination products, furnishing copies of each to the depository libraries could be prohibitively expensive. In that situation, the agency should endeavor to make available those titles with the greatest general interest, value, and utility to the public. Substantial cost could also be an impediment in the case of some on-line information services where the costs associated with operating centralized databases would make provision of unlimited direct access to numerous users prohibitively expensive. In both cases, agencies should consult with the GPO, in order to identify those information dissemination products with the greatest public interest and utility for dissemination. In all cases, however, where an agency discontinues publication of an information dissemination product in paper format in favor of electronic formats, the agency should work with the GPO to ensure availability of the information dissemination product to depository libraries.

Notice to the Public. Sections 8a(6)(i) and (j) present new practices for agencies to observe in communicating with the public about information dissemination. Among agencies' responsibilities for dissemination is an active knowledge of, and regular consultation with, the users of their information dissemination products. A primary reason for communication with users is to gain their contribution to improving the quality and relevance of government information—how it is created, collected, and disseminated. Consultations with users might include participation at conferences and workshops, careful attention to correspondence and telephone communications (e.g., logging and analyzing inquiries), or formalized user surveys.

A key part of communicating with the public is providing adequate notice of agency information dissemination plans. Because agencies' information dissemination actions affect other agencies as well as the public, agencies must forewarn other agencies of significant actions. The decision to initiate, terminate, or substantially modify the content, form, frequency, or availability of significant products should also trigger appropriate advance public notice. Where appropriate, the Government Printing Office should be notified directly. Information dissemination products deemed not to be significant require no advance notice.

Examples of significant products (or changes to them) might be those that:

(a) Are required by law; e.g., a statutorily mandated report to Congress;

(b) Involve expenditure of substantial funds;

(c) By reason of the nature of the information, are matters of continuing public interest; e.g., a key economic indicator;

(d) By reason of the time value of the information, command public interest; e.g., monthly crop reports on the day of their release;

(e) Will be disseminated in a new format or medium; e.g., disseminating a printed product in electronic medium, or disseminating a machine-readable data file via on-line access.

Where members of the public might consider a proposed new agency product unnecessary or duplicative, the agency should solicit and evaluate public comments. Where users of an agency information dissemination product may be seriously affected by the introduction of a change in medium or format, the agency should notify users and consider their views before instituting the change. Where members of the public consider an existing agency product important and necessary, the agency should consider these views before deciding to terminate the product. In all cases, however, determination of what is a significant information dissemination product and what constitutes adequate notice are matters of agency judgment.

Achieving Compliance with the Circular's Requirements. Section 8a(6)(k) requires that the agency information dissemination management system ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, an orderly transition to compliance with the requirements of this Circular is made. For example, some agency information dissemination products may be priced at a level which exceeds the cost of dissemination, or the agency may be engaged in practices which are otherwise unduly restrictive. In these instances, agencies must plan for an orderly transition to the substantive policy requirements of the Circular. The information dissemination management system must be capable of identifying these situations and planning for a reasonably prompt transition. Instances of existing agency practices which cannot immediately be brought into conformance with the requirements of the Circular are to be addressed through the waiver procedures of Section 10(b).

Section 8a(7). Avoiding Improperly Restrictive Practices. Federal agencies are often the sole suppliers of the information they hold. The agencies have either created or collected the information using public funds, usually in furtherance of unique governmental functions, and no one else has it. Hence agencies need to take care that their behavior does not inappropriately constrain public access to government information.

When agencies use private contractors to accomplish dissemination, they must take care that they do not permit contractors to impose restrictions that undercut the agencies' discharge of their information dissemination responsibilities. The contractual terms should assure that, with respect to dissemination, the contractor behaves as though the contractor were the agency. For example, an agency practice of selling, through a contractor, on-line access to a database but refusing to sell copies of the database itself may be improperly restrictive because it precludes the possibility of another firm making the same service available to the public at a lower price. If an agency is willing to provide public access to a database, the agency should be willing to sell copies of the database itself.

By the same reasoning, agencies should behave in an even-handed manner in handling information dissemination products. If an agency is willing to sell a database or database services to some members of the public, the agency should sell the same products under similar terms to other members of the public, unless prohibited by statute. When an agency decides it has public policy reasons for offering different terms of sale to different groups in the public, the agency should provide a clear statement of the policy and its basis.

Agencies should not attempt to exert control over the secondary uses of their

information dissemination products. In particular, agencies should not establish exclusive, restricted, or other distribution arrangements which interfere with timely and equitable availability of information dissemination products, and should not charge fees or royalties for the resale or redissemination of government information. These principles follow from the fact that the law prohibits the Federal Government from exercising copyright.

Agencies should inform the public as to the limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity) so that users are fully aware of the quality and integrity of the information. If circumstances warrant, an agency may wish to establish a procedure by which disseminators of the agency's information may at their option have the data and/or value-added processing checked for accuracy and certified by the agency. Using this method, redisseminators of the data would be able to respond to the demand for integrity from purchasers and users. This approach could be enhanced by the agency using its authority to trademark its information dissemination product, and requiring that redisseminators who wish to use the trademark agree to appropriate integrity procedures. These methods have the possibility of promoting diversity, user responsiveness, and efficiency as well as integrity. However, an agency's responsibility to protect against misuse of a government information dissemination product does not extend to restricting or regulating how the public actually uses the information.

The Lanham Trademark Act of 1946, 15 U.S.C. 1055, 1125, 1127, provides an efficient method to address legitimate agency concerns regarding public safety. Specifically, the Act permits a trademark owner to license the mark, and to demand that the user maintain appropriate quality controls over products reaching consumers under the mark. See generally, McCarthy on Trademarks, Sec. 18.13. When a trademark owner licenses the trademark to another, it may retain the right to control the quality of goods sold under the trademark by the licensee. Furthermore, if a licensee sells goods under the licensed trademark in breach of the licensor's quality specifications, the licensee may be liable for breach of contract as well as for trademark infringement. This technique is increasingly being used to assure the integrity of digital information dissemination products. For example, the Census Bureau has trademarked its topologically integrated geographic encoding and referencing data product (''TIGER/Line''), which is used as official source data for legislative districting and other sensitive applications.

Whenever a need for special quality control procedures is identified, agencies should adopt the least burdensome methods and ensure that the methods chosen do not establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public. Agencies should not attempt to condition the resale or redissemination of its information dissemination products by members of the public.

User charges. Title 5 of the Independent Offices Appropriations Act of 1952 (31 U.S.C. 9701) establishes Federal policy regarding fees assessed for government services, and for sale or use of government property or resources. OMB Circular No. A–25, User Charges, implements the statute. It provides for charges for government goods and services that convey special benefits to recipients beyond those accruing to the general public. It also establishes that user charges should be set at a level sufficient to recover the full cost of providing the service, resource, or property. Since Circular No. A–25 is silent as to the extent of its application to government information dissemination products, full cost recovery for information dissemination products might be interpreted to include the cost of collecting and processing information rather than just the cost of dissemination. The policy in Section 8a(7)(c) clarifies the policy of Circular No. A–25 as it applies to information dissemination products. This policy was codified by the Paperwork Reduction Act of 1995 at 35 U.S.C. Section 3506(d)(4)(D).

Statutes such as FOIA and the Government in the Sunshine Act establish a broad and general obligation on the part of Federal agencies to make government information available to the public and to avoid erecting barriers that impede public access. User charges higher than the cost of dissemination may be a barrier to public access. The economic benefit to society is maximized when government information is publicly disseminated at the cost of dissemination. Absent statutory requirements to the contrary, the general standard for user charges for government information dissemination products should be to recover no more than the cost of dissemination. It should be noted in this connection that the government has already incurred the costs of creating and processing the information for governmental purposes in order to carry out its mission.

Underpinning this standard is the FOIA fee structure which establishes limits on what agencies can charge for access to Federal records. That Act permits agencies to charge only the direct reasonable cost of search, reproduction and, in certain cases, review of requested records. In the case of FOIA requests for information dissemination products, charges would be limited to reasonable direct reproduction costs alone. No search would be needed to find the product, thus no search fees would be charged. Neither would the record need to be reviewed to determine if it could be withheld under one of the Act's exemptions since the agency has already decided to release it. Thus, FOIA provides an information ''safety net'' for the public.

While OMB does not intend to prescribe procedures for pricing government information dissemination products, the cost of dissemination may generally be thought of as the sum of all costs specifically associated with preparing a product for dissemination and actually disseminating it to the public. When an agency prepares an information product for its own internal use, costs associated with such production would not generally be recoverable as user charges on subsequent dissemination. When the agency prepares the product for public dissemination, and disseminates it, costs associated with preparation and actual dissemination would be recoverable as user charges.

In the case of government databases which are made available to the public on-line, the costs associated with initial database development, including the costs of the necessary hardware and software, would not be included in the cost of dissemination. Once a decision is made to disseminate the data, additional costs logically associated with dissemination can be included in the user fee. These may include costs associated with modification of the database to make it suitable for dissemination, any hardware or software enhancements necessary for dissemination, and costs associated with providing customer service or telecommunications capacity.

In the case of information disseminated via cd-rom, the costs associated with initial database development would likewise not be included in the cost of dissemination. However, a portion of the costs associated with formatting the data for cd-rom dissemination and the costs of mastering the cd-rom, could logically be included as part of the dissemination cost, as would the cost associated with licensing appropriate search software.

Determining the appropriate user fee is the responsibility of each agency, and involves the exercise of judgment and reliance on reasonable estimates. Agencies should be able to explain how they arrive at user fees which represent average prices and which, given the likely demand for the product, can be expected to recover the costs associated with dissemination.

When agencies provide custom tailored information services to specific individuals or groups, full cost recovery, including the cost of collection and processing, is appropriate. For example, if an agency prepares special tabulations or similar services from its databases in answer to a specific request from the public, all costs associated with fulfilling the request would be charged, and the requester should be so informed before work is begun.

In a few cases, agencies engaging in information collection activities augment the information collection at the request of, and with funds provided by, private sector groups. Since the 1920's, the Bureau of the Census has carried out, on request, surveys of certain industries at greater frequency or at a greater level of detail than Federal funding would permit, because gathering the additional information is consistent with Federal purposes and industry groups have paid the additional information collection and processing costs. While the results of these surveys are disseminated to the public at the cost of dissemination, the existence and availability of the additional government data are special benefits to certain recipients beyond those accruing to the public. It is appropriate that those recipients should bear the full costs of information collection and processing, in addition to the normal costs of dissemination.

Agencies must balance the requirement to establish user charges and the level of fees

charged against other policies, specifically, the proper performance of agency functions and the need to ensure that information dissemination products reach the public for whom they are intended. If an agency mission includes disseminating information to certain specific groups or members of the public and the agency determines that user charges will constitute a significant barrier to carrying out this responsibility, the agency may have grounds for reducing or eliminating its user charges for the information dissemination product, or for exempting some recipients from the charge. Such reductions or eliminations should be the subject of agency determinations on a case by case basis and justified in terms of agency policies.

Section 8a(8). Electronic Information Dissemination. Advances in information technology have changed government information dissemination. Agencies now have available new media and formats for dissemination, including CD-ROM, electronic bulletin boards, and public networks. The growing public acceptance of electronic data interchange (EDI) and similar standards enhances their attractiveness as methods for government information dissemination. For example, experiments with the use of electronic bulletin boards to advertise Federal contracting opportunities and to receive vendor quotes have achieved wider dissemination of information about business opportunities with the Federal Government than has been the case with traditional notices and advertisements. Improved information dissemination has increased the number of firms expressing interest in participating in the government market and decreased prices to the government due to expanded competition. In addition, the development of public electronic information networks, such as the Internet, provides an additional way for agencies to increase the diversity of information sources available to the public. Emerging applications such as Wide Area Information Servers and the World-wide Web (using the NISO Z39.50 standard) will be used increasingly to facilitate dissemination of government information such as environmental data, international trade information, and economic statistics in a networked environment.

A basic purpose of the PRA is to ''provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology.'' (44 U.S.C. 3501(7)) Agencies can frequently enhance the value, practical utility, and timeliness of government information as a national resource by disseminating information in electronic media. Electronic collection and dissemination may substantially increase the usefulness of government information dissemination products for three reasons. First, information disseminated electronically is likely to be more timely and accurate because it does not require data re-entry. Second, electronic records often contain more complete and current information because, unlike paper, it is relatively easy to make frequent changes. Finally, because electronic information is more easily manipulated by the user and can be tailored to a wide variety of needs, electronic information dissemination products are more useful to the recipients.

As stated at Section 8a(1)(h), agencies should use voluntary standards and Federal Information Processing Standards to the extent appropriate in order to ensure the most cost effective and widespread dissemination of information in electronic formats.

Agencies can frequently make government information more accessible to the public and enhance the utility of government information as a national resource by disseminating information in electronic media. Agencies generally do not utilize data in raw form, but edit, refine, and organize the data in order to make it more accessible and useful for their own purposes. Information is made more accessible to users by aggregating data into logical groupings, tagging data with descriptive and other identifiers, and developing indexing and retrieval systems to facilitate access to particular data within a larger file. As a general matter, and subject to budgetary, security or legal constraints, agencies should make available such features developed for internal agency use as part of their information dissemination products.

There will also be situations where the agency determines that its mission will be furthered by providing enhancements beyond those needed for its own use, particularly those that will improve the public availability of government information over the long term. In these instances, the agency should evaluate the expected usefulness of the enhanced information in light of its mission, and where appropriate construct partnerships with the private sector to add these elements of value. This approach may be particularly appropriate as part of a strategy to utilize new technology enhancements, such as graphic images, as part of a particular dissemination program.

Section 8a(9). Information Safeguards. The basic premise of this Section is that agencies should provide an appropriate level of protection to government information, given an assessment of the risks associated with its maintenance and use. Among the factors to be considered include meeting the specific requirements of the Privacy Act of 1974 and the Computer Security Act of 1987.

In particular, agencies are to ensure that they meet the requirements of the Privacy Act regarding information retrievable by individual identifier. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. Individuals must be accorded access and amendment rights to records, as provided in the Privacy Act. To the extent that agencies share information which they have a continuing obligation to protect, agencies should see that appropriate safeguards are instituted. Appendix I prescribes agency procedures for the maintenance of records about individuals, reporting requirements to OMB and Congress, and other special requirements of specific agencies, in accordance with the Privacy Act.

This Section also incorporates the requirement of the Computer Security Act of 1987 that agencies plan to secure their systems commensurate with the risk and magnitude of loss or harm that could result from the loss, misuse, or unauthorized access to information contained in those systems. It includes assuring the integrity, availability, and appropriate confidentiality of information. It also involves protection against the harm that could occur to individuals or entities outside of the Federal Government as well as the harm to the Federal Government. Appendix III prescribes a minimum set of controls to be included in Federal automated information resources security programs and assigns Federal agency responsibilities for the security of automated information resources. The Section also includes limits on collection and sharing of information and procedures to assure the integrity of information as well as requirements to adequately secure the information.

Incorporation of Circular No. A–114. OMB Circular No. A–114, Management of Federal Audiovisual Activities, last revised on March 20, 1985, prescribed policies and procedures to improve Federal audiovisual management. Although OMB has rescinded Circular No. A–114, its essential policies and procedures continue. This revision provides information resources management policies and principles independent of medium, including paper, electronic, or audiovisual. By including the term ''audiovisual'' in the definition of ''information,'' audiovisual materials are incorporated into all policies of this Circular.

The requirement in Circular No. A–114 that the head of each agency designate an office with responsibility for the management oversight of an agency's audiovisual productions and that an appropriate program for the management of audiovisual productions in conformance with 36 CFR 1232.4 is incorporated into this Circular at Section 9a(10). The requirement that audiovisual activities be obtained consistent with OMB Circular No. A–76 is covered by Sections 8a(1)(d), 8a(5)(d)(i) and 8a(6)(b).

The National Archives and Records Administration will continue to prescribe the records management and archiving practices of agencies with respect to audiovisual productions at 36 CFR 1232.4, ''Audiovisual Records Management.''

Section 8b. Information Systems and Information Technology Management.

Section 8b(1). Evaluation and Performance Measurement. OMB encourages agencies to stress several types of evaluation in their oversight of information systems. As a first step, agencies must assess the continuing need for the mission function. If the agency determines there is a continuing need for a function, agencies should reevaluate existing work processes prior to creating new or updating existing information systems. Without this analysis, agencies tend to develop information systems that improve the efficiency of traditional paper-based processes which may be no longer needed. The application of information technology presents an opportunity to reevaluate existing organizational structures, work

processes, and ways of interacting with the public to see whether they still efficiently and effectively support the agency's mission.

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'' should be analyzed and documented 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.

Agencies should also weigh the relative benefits of proposed investments in information technology across the agency. Given the fiscal constraints facing the Federal government in the upcoming years, 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. OMB and GAO are creating a publication that will provide agencies with reference materials for setting up such evaluation processes.

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

Section 8b(2). Strategic Information Resources Management (IRM) Planning. Agencies should link to, and to the extent possible, integrate IRM planning with the agency strategic planning required by the Government Performance and Results Act (P.L. 103–62). Such a linkage ensures that agencies apply information resources to programs that support the achievement of agreed-upon mission goals. Additionally, strategic IRM planning by agencies may help avoid automating out-of-date, ineffective, or inefficient procedures and work processes.

Agencies should also devote management attention to operational information resources management planning. This operational IRM planning should provide a one to five year focus to agency IRM activities and projects. Agency operational IRM plans should also provide a listing of the major information systems covered by the management oversight processes described in Section 8b(3). Agency operational planning for IRM should also communicate to the public how the agency's application of information resources might affect them. For the contractor community, this includes articulating the agency's intent to acquire information technology from the private sector. These data should not be considered acquisition sensitive, so that they can be distributed as widely as possible to the vendor community in order to promote competition. Agencies should make these acquisition plans available to the public through government-wide information dissemination mechanisms, including electronic means.

Operational planning should also include initiatives to reduce the burden, including information collection burden, an agency imposes on the public. Too often, for example, agencies require personal visits to government offices during office hours inconvenient to the public. Instead, agencies should plan to use information technology in ways that make the public's dealing with the Federal government as ''user-friendly'' as possible.

Each year, OMB issues a bulletin requesting copies of agencies' latest strategic IRM plans and annual updates to operational plans for information and information technology.

Section 8b(3). Information Systems Management Oversight. Agencies should consider what constitutes a ''major information system'' for purposes of this Circular when determining the appropriate level of management attention for an information system. The anticipated dollar size of an information system or a supporting acquisition is only one determinant of the level of management attention an information system requires. Additional criteria to assess include the maturity and stability of the technology under consideration, how well defined user requirements are, the level of stability of program and user requirements, and security concerns.

For instance, certain risky or ''cutting-edge'' information systems require closer scrutiny and more points of review and evaluation. This is particularly true when an agency uses an evolutionary life cycle strategy that requires a technical and financial evaluation of the project's viability at prototype and pilot testing phases. Projects relying on commercial off-the-shelf technology and applications will generally require less oversight than those using custom-designed software.

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 should 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.

The policy statements in this Circular describe an information system life cycle. It does not, however, make a definitive statement that there must be 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. As a result, life cycle management techniques that agencies can use may vary depending on the complexity and risk inherent in the project.

One element of this management oversight policy is the recognition of imbedded and/or parallel life cycles. Within an information system's life cycle there may be other subsidiary life cycles. For instance, most Federal information systems projects include an acquisition of goods and services that have life cycle characteristics. Some projects include software development components, which also have life cycles. Effective management oversight of major information systems requires a recognition of all these various life cycles and an integrated information systems management oversight with the budget and human resource management cycles that exist in the agency.

Section 8b(2) of the Circular underscores the need for agencies to bring an agency-wide perspective to a number of information resources management issues. These issues include policy formulation, planning, management and technical frameworks for using information resources, and management oversight of major information systems. Agencies should also provide for coordinated decision making (Section 8b(3)(f)) in order to bring together the perspectives from across an agency, and outside if appropriate. Such coordination may take place in an agency-wide management or IRM committee. Interested groups typically include functional users, managers of financial and human resources, information resources management specialists, and, as appropriate, the affected public.

Section 8b(4). Use of Information Resources. Agency management of information resources should be guided by management and technical frameworks for agency-wide information and information technology needs. The technical framework should serve as a reference for updates to existing and new information systems. The

management framework should assure the integration of proposed information systems projects into the technical framework in a manner that will ensure progress toward achieving an open systems environment. Agency strategic IRM planning should describe the parameters (e.g., technical standards) of such a technical framework. The management framework should drive operational planning and should describe how the agency intends to use information and information technology consistent with the technical framework.

Agency management and technical frameworks for information resources should address agency strategies to move toward an open systems environment. These strategies should consist of one or multiple profiles (an internally consistent set of standards), based on the current version of the NIST's Application Portability Profile. These profiles should satisfy user requirements, accommodate officially recognized or de facto standards, and promote interoperability, application portability, and scalability by defining interfaces, services, protocols, and data formats favoring the use of nonproprietary specifications.

Agencies should focus on how to better utilize the data they currently collect from the public. Because agencies generally do not share information, the public often must respond to duplicative information collections from various agencies or their components. Sharing of information about individuals should be consistent with the Privacy Act of 1974, as amended, and Appendix I of this Circular.

Services provided by IPSOs to components of their own agency are often perceived to be ''free'' by the service recipients because their costs are budgeted as an ''overhead'' charge. Service recipients typically do not pay for IPSO services based on actual usage. Since the services are perceived to be free, there is very little incentive for either the service recipients or the IPSO managers to be watchful for opportunities to improve productivity or to reduce costs. Agencies are encouraged to institute chargeback mechanisms for IPSOs that provide common information processing services across a number of agency components when the resulting economies are expected to exceed the cost of administration.

Section 8b(5). Acquisition of Information Technology. Consistent with the requirements of the Brooks Act and the Paperwork Reduction Act, agencies should acquire information technology to improve service delivery, reduce the cost of Federal program administration, and minimize burden of dealing with the Federal government. Agencies may wish to ask potential offerors to propose different technical solutions and approaches to fulfilling agency mission requirements. Evaluating acquisitions of information technology must assess both the benefits and costs of applying technology to meet such requirements.

The distinction between information system life cycles and acquisition life cycles is important when considering the implications of OMB Circular A–109, Acquisition of Major Systems, to the acquisition of information resources. Circular A–109 presents one strategy for acquiring information technology when:

(i) The agency intends to fund operational tests and demonstrations of system design;

(ii) The risk is high due to the unproven integration of custom designed software and/or hardware components;

(iii) The estimated cost savings or operational improvements from such a demonstration will further improve the return on investment; or

(iv) The agency wants to acquire a solution based on state-of-the-art, unproven technology.

Agencies should comply with OMB Circular A–76, Performance of Commercial Activities, when considering conversion to or from in-house or contract performance.

Agencies should ensure that acquisitions for new information technology comply with GSA regulations concerning information technology accessibility for individuals with disabilities [41 C.F.R. 201–20.103–7].

Section 9a(11). Ombudsman. The senior agency official 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 senior information resources management officials are responsible for ensuring that their agency practices are in compliance with OMB policies. It is envisioned that the agency senior information resources management official will work as an ombudsman to investigate alleged instances of agency failure 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.

Section 9b. International Relationships. The information policies contained in the PRA and Circular A–130 are based on the premise that government information is a valuable national resource, and that the economic benefits to society are maximized when government information is available in a timely and equitable manner to all. Maximizing the benefits of government information to society depends, in turn, on fostering diversity among the entities involved in disseminating it. These include for-profit and not-for-profit entities, such as information vendors and libraries, as well as State, local and tribal governments. The policies on charging the cost of dissemination and against restrictive practices contained in the PRA and Circular A–130 are aimed at achieving this goal.

Other nations do not necessarily share these values. Although an increasing number are embracing the concept of equitable and unrestricted access to public information—particularly scientific, environmental, and geographic information of great public benefit—other nations are treating their information as a commodity to be ''commercialized''. Whereas the Copyright Act, 17 U.S.C. 105, has long provided that ''[c]opyright protection under this title is not available for any work of the United States Government,'' some other nations take advantage of their domestic copyright laws that do permit government copyright and assert a monopoly on certain categories of information in order to maximize revenues. Such arrangements tend to preclude other entities from developing markets for the information or otherwise disseminating the information in the public interest.

Thus, Federal agencies involved in international data exchanges are sometimes faced with problems in disseminating data stemming from differing national treatment of government copyright. For example, one country may attempt to condition the sharing of data with a Federal agency on an agreement that the agency will withhold release of the information or otherwise restrict its availability to the public. Since the Freedom of Information Act does not provide a categorical exemption for copyrighted information, and Federal agencies have neither the authority nor capability to enforce restrictions on behalf of other nations, agencies faced with such restrictive conditions lack clear guidance as to how to respond.

The results of the July 1995 Congress of the World Meteorological Organization, which sought to strike a balance of interests in this area, are instructive. Faced with a resolution which would have essentially required member nations to enforce restrictions on certain categories of information for the commercial benefit of other nations, the United States proposed a compromise which was ultimately accepted. The compromise explicitly affirmed the general principle that government meteorological information—like all other scientific, technical and environmental information—should be shared globally without restriction; but recognized that individual nations may in particular cases apply their own domestic copyright and similar laws to prevent what they deem to be unfair or inappropriate competition within their own territories. This compromise leaves open the door for further consultation as to whether the future of government information policy in a global information infrastructure should follow the ''open and unrestricted access'' model embraced by the United States and a number of other nations, or if it should follow the ''government commercialization'' model of others.

Accordingly, since the PRA and Circular A–130 are silent as to how agencies should respond to similar situations, we are providing the following suggestions. They are intended to foster globally the open and unrestricted information policy embraced by the United States and like minded nations, while permitting agencies to have access to data provided by foreign governments with restrictive conditions.

Release by a Federal agency of copyrighted information, whether under a FOIA request or otherwise, does not affect any rights the copyright holder might otherwise possess. Accordingly, agencies should inform any concerned foreign governments that their copyright claims may be enforceable under United States law, but that the agency is not authorized to prosecute any such claim on behalf of the foreign government.

Whenever an agency seeks to negotiate an international agreement in which a foreign party seeks to impose restrictive practices on information to be exchanged, the agency

should first coordinate with the State Department. The State Department will work with the agency to develop the least restrictive terms consistent with United States policy, and ensure that those terms receive full interagency clearance through the established process for granting agencies authority to negotiate and conclude international agreements.

Finally, whenever an agency is attending meetings of international or multilateral organizations where restrictive practices are being proposed as binding on member states, the agency should coordinate with the State Department, the Office of Management and Budget, the Office of Science and Technology Policy, or the U.S. Trade Representative, as appropriate, before expressing a position on behalf of the United States.

[FR Doc. 96–3645 Filed 2–16–96; 8:45 am]

BILLING CODE 3110–01–P