OFFICE OF MANAGEMENT AND BUDGET

Security of Federal Automated Information

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

ACTION: Proposed revision of OMB Circular No. A–130 Appendix III.

SUMMARY: The Office of Management and Budget (OMB) is proposing to revise Appendix III of Circular No. A–130, ''Security of Federal Automated Information Systems.'' This is the third stage of revisions to Circular No. A–130, ''Management of Federal Information Resources.'' The first stage addressed information management policy (Section 8a) and Appendix I, ''Federal Agency Responsibilities for Maintaining Records About Individuals'' (June 25, 1993). That revision focussed on information exchanges with the public. The second revision addressed agency management practices for information systems and information technology (Section 8b) (July 25, 1994). That revision 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 proposal is intended to guide agencies in securing information 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, rather than technical controls. For example, it would require agencies to assure that risk-based rules of behavior are established, that employees are trained in them, and that the rules are enforced. The proposal would also better integrate security into program and mission goals, reduce the need for centralized reporting of paper security plans, emphasize the management of risk rather than its measurement and revise government-wide security responsibilities to be consistent with the Computer Security Act.

DATES: Persons who wish to comment on the proposed revision to OMB Circular No. A–130, Appendix III should submit their comments no later than June 2, 1995.

ADDRESSES: Comments should be addressed to: Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236, New Executive Office Building, Washington, DC 20503.

Electronic Availability and Comments. This document is 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/a130app3.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 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 a130app3.txt as the first line of the body of the message. Comments may be sent via electronic mail to a130@a1.eop.gov (note that the address contains the number 1 not the letter L) and will be included as part of the official record. For assistance using FTP, mail query, or electronic mail, please contact your system administrator.

FOR FURTHER INFORMATION CONTACT: Ed Springer, 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. That Appendix, and its predecessor, Transmittal Memorandum No. 1 to OMB Circular No. A–71, (July 27, 1978), defined controls that were 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. This shift has increased both risks and vulnerabilities. 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. 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 proposed revision of Appendix III to OMB Circular A–130 incorporates and updates the policies set out in those Bulletins.

The report of the National Performance Review, ''Creating a Government That Works Better and Costs Less: Reengineering Through Information Technology'' (September 1993), recommends that Circular A–130 be revised to: (1) Require an information security plan to be part of each agency's strategic IT plan; (2) require that computer security be identified as a material weakness in the Federal Managers' Financial Integrity Act report, if security does not meet established thresholds; (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 proposed 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 Managers' Financial Integrity Act (FMFIA). The proposed Appendix 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, the three agencies 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 the proposed 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.

The Proposed Appendix

The Appendix proposes to reorient 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 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 would no longer require the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of 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 complex risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This 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.

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 proposal emphasizes management controls affecting individual users of information technology. Technical and operational controls are linked to management controls regarding user behavior. Four interrelated management controls are proposed: 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 Bulletin 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 support 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 Federal information requires some level of protection. However, certain applications, because of the information in them, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the general support systems in which they operate.

The focus of OMB Bulletins No. 88–16 and 90–08 was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix proposes to establish security controls in all general support systems, under the presumption that all contain some sensitive information, and focus extra security controls on a limited number of particularly high risk or major applications.

Discussion of the Appendix's Major Provisions.

The following discussion is provided to aid reviewers in understanding the changes in emphasis proposed in the Appendix.

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 to an official trained in the technology used in the system and in providing security for such technology.

(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 and therefore require security plans.

Current guidance on security planning is contained in OMB Bulletin 90–08. The Appendix will supersede Section 6 of Bulletin 90–08. The Appendix also expands the coverage of security plans to address 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 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.

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. 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 software, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Often rules will address technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

(b) *Awareness and Training.* The Computer Security Act requires mandatory periodic training for everyone with access to Federal computer systems. This includes contractors, employees of other agencies, and members of the public. The Appendix proposes to enforce such mandatory awareness and training by requiring its completion prior to granting access to the system. Each new user, in some sense, introduces a risk to all other users of a general support system. Therefore, each user should be versed in acceptable behavior—the rules of the system—before being allowed to use the system. Awareness and training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Awareness and training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Awareness and training may be presented in stages, for example as more access is granted. In some cases, the awareness and 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 atrophy. 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 proposes that NIST, with assistance from the Office of Personnel Management (OPM), update its existing awareness and training 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 comes from authorized users 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.

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 critical 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 technical and operational controls in order to perform system administration and maintenance functions. Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of loss or 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. Agencies should coordinate assistance and sharing through the Forum of Incident Response & Security Teams (FIRST).

The Appendix also directs the Department of Justice to develop 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. Moreover, 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 advanced 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 loss or 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. 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. Some agencies refer to this authorization as an accreditation.

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.

b. *Controls in Major Applications.* Certain applications require special management attention due to the risk and magnitude of loss or 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 to assure that the particular application has adequate security. To be effective, this individual should be knowledgeable in the information processed by the application and in the management, 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 shown 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.

(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. Such rules should include, for example, limitations on changing data, searching data bases, or divulging information.

(b) *Specialized Awareness and Training.* Awareness and training should vary depending on the type of access allowed and the risk that access represents to the security of information in the application. 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. 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.

(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 in the event of an emergency. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans may create a false sense of ability to recover in a timely manner.

(e) *Technical Controls.* Technical security controls, for example software edits that limit data that can be entered into certain files, should be built into each application. Often these controls will correspond with the rules of behavior for the application. Under the current Appendix, application security is focused on the process by which sensitive, custom applications are developed. Given the increasing reliance on commercial off-the-shelf software, that process is not addressed in detail in this Appendix. However, some custom-developed applications will remain. For them 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 relative 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 may require agreements to protect such 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, a review or audit of the security controls for each major application should be performed. 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 than 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 the new 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 periodically authorized by the management official responsible for the function supported by the application. 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 awareness and 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.

(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. This is already underway through the Forum for Incident Response Teams (FIRST).

(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. *Security Policy Board.* The Security Policy Board is assigned responsibility for national security policy coordination in accordance with appropriate Presidential directive.

c. *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.

d. *Office of Personnel Management.* In accordance with the Computer Security Act, the Office of Personnel Management 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.

e. *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 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).

f. *Department of Justice.* The Department of Justice should provide 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.

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 five-year information resources management plan required by the Paperwork Reduction Act.

Accordingly, Appendix III of Circular A–130 is proposed to be revised to read as set forth below.

Sally Katzen.

Appendix III—To OMB Circular No. A–130, Security of Federal Automated Information

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 share common functionality. A system normally includes hardware, software, information, data, applications, 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 information requires 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 should 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 should 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 should 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 official knowledgeable in the information technology used in the system and in providing security for such technology.

(2) *System Security Plan.* Plan for the security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan should be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan should be solicited prior to the plan's implementation. A summary of the security plans should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans should 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 should be based on the needs of the various users of the system. The security required by the rules should be only as stringent as necessary to provide adequate security for information in the system. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should also include appropriate limits on interconnections to other systems and should define service provision and restoration priorities. Finally, they should be clear about the consequences of behavior not consistent with the rules.

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

(c) *Personnel Controls.* Screen all individuals who are authorized to bypass technical and operational security controls of the system (e.g., LAN administrators or system programmers) commensurate with the risk and magnitude of loss or harm they could cause. Such screening should occur prior to the individuals' 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 should coordinate with those in other organizations 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 should be established which are consistent with the rules of the system and in accordance with guidance from NIST.

(3) *Review of Security Controls.* Periodically review the security controls in each system commensurate with the acceptable level of risk for the system established in its rules, especially when significant modifications are made and at least every 3 years. 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 in 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 should be reauthorized 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 processed by the application and in the management, operational, and technical controls used to protect it. This official should assure that effective security products and techniques are appropriately used in the application and should 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 should be consistent with guidance issued by NIST. Advice and comment on the plan should 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 should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act. Application security plans should include:

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

(b) *Specialized Awareness and Training.* Before allowing individuals access to the application, ensure that all individuals receive specialized awareness and training focused on their responsibilities and the application rules. This may be in addition to the awareness and training required for access to a system. Such awareness and 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 as appropriate. In cases where such controls cannot adequately protect the application and information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening should 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 accordance with guidance issued by NIST.

(f) *Information Sharing.* Ensure that information shared from the application is protected appropriately, relative 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 should be added to protect the integrity of the application and the confidence the public has in the application. Such controls should include segregating information made directly accessible to the public from official agency records (e.g., by putting information onto a bulletin board).

(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 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 should be a factor in management authorizations. The application should 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 should:

(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 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. *Security Policy Board.* The Security Policy Board should:

(1) Act, in accordance with applicable national security directives, to coordinate the security activities of the Federal Government regarding the security of automated information systems that process national security information;

c. *Department of Defense.* The Secretary of Defense should:

(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.

d. *Office of Personnel Management.* The Director of the Office of Personnel Management should:

(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.

e. *General Services Administration.* The Administrator of General Services should:

(1) Assure that the Federal Information Resources Management Regulation provides 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 contract).

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

f. *Department of Justice.* The Attorney General should:

(1) Provide 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.

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, if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it should be included in the annual FMFIA report. Less significant deficiencies should 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 five-year plan required by the Paperwork Reduction Act (44 U.S.C. 3505).

[FR Doc. 95–8055 Filed 3–31–95; 8:45 am]

BILLING CODE 3110–01–P