Appendix III to OMB Circular No. A-130

Security of Federal Automated Information Resources

A. Requirements.

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.

Definitions

The term:

"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.

"application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

"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).

"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.

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:

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.

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.

Assignment of Responsibilities

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.

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.

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.

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.

Office of Personnel Management. The Director of the Office of Personnel Management shall:
2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

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;

Correction of Deficiencies and Reports

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

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.

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 enter 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.

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.

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.

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.

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.

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.

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).

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.

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.