13 May 1992

DRAFT

IDA DOCUMENT D-967

INTEGRITY-ORIENTED CONTROL OBJECTIVES: PROPOSED REVISIONS TO THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC), DoD 5200.28-STD

Terry Mayfield

John M. Boone

Steven R. Welke

August 1991

Prepared for

National Security Agency

INSTITUTE FOR DEFENSE ANALYSES

1801 N. Beauregard Street, Alexandria, Virginia 22311

DRAFT

1. INTRODUCTION

1.1 PURPOSE

This document proposes new and revised versions of the control objectives contained in the Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD [TCSEC 1985, pp. 57-63]. These modifications extend the existing control objective statements to encompass the promotion and preservation of data and systems integrity. They are intended to be used as a strawman to foster further research and debate aimed at developing a new or revised set of product evaluation criteria that addresses integrity as well as confidentiality.

1.2 BACKGROUND

Control objectives are the fundamental computer security requirements as they apply to general purpose automated information systems (AISs). As such, they serve as guidance to the development of more specific evaluation criteria. Evaluation criteria, in turn, are intended to ``... (a) provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for processing classified or other sensitive information; (b) provide guidance to manufacturers as to what to build into their new widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications; and (c) provide a basis for specifying security requirements in acquisition specifications" [TCSEC 1985, p. v].

Given the rather far reaching implications of evaluation criteria, it is vital that such criteria be built upon a clear and complete foundation. The modified control objectives presented in this document represent only one step towards that foundation. This step, directed towards enhancing the set of control objectives to address the needs of integrity, begins the enabling for the development of new criteria. However, the proposed control objectives are not intended to be adopted without further research and debate to derive the best possible foundation for further development work.

1.3 SCOPE

This document extends the integrity framework developed in [Mayfield 1991] and takes another step in developing and evolving product criteria that include integrity. The document only addresses control objectives; specific criteria addressing integrity concerns remain as future work. The document is complementary to other ongoing research work in the topic of integrity, e.g., the electronic forum for the development of new formal models of integrity in preparation for The Computer Security Foundations Workshop IV which was held in Franconia, New Hampshire, 18-20 June 1991. The document assumes that the control objectives for confidentiality, as contained in the TCSEC, are adequate for that purpose. Through the study of relevant policies, we have come to believe that the control objectives need to extend to applications running on a vendor's system product in order to adequately address boundaries of responsibility and criteria for implementing protection controls. However, this study concentrates primarily on control objectives from a systems perspective-the issues involved with extending the control objectives to applications cannot be explored in depth until a systems perspective has been established. We do not make use of a particular formal model of integrity, but rather use some of the concepts developed and modeled by various model authors to arrive at our specific version of each control objective.

We have purposefully tried to not depart radically from the TCSEC. Our thinking was that it would be much more beneficial to show minimal changes while increasing support to various integrity policies than to try and "reinvent the wheel." To some, these changes may still seem too radical, to others they will be insufficient. We hope that in both cases our proposals serve to enhance the debate.

The major policy documents, with respect to integrity in AISs, are listed in Table 1.1. These documents are addressed individually in separate sections in Appendix A. Each

individual section devoted to a particular document contains (a) a brief overview of the document, (b) a listing of selected source text from the document, (c) a cross-reference from the source text to affected integrity control objectives, and (d) a commentary section. The commentary section is, in essence, a set of interpretive notes about control aspects of the source text. We developed them to partially confirm, from a policy point of view, what we had discovered in [Mayfield 1991] through an analysis of various integrity-supporting mechanisms about possible objectives for control.

These government documents provide policy and guidance for controlling and protecting information. Their contents can be interpreted in at least three distinct ways: (1) having direct applicability to the certification of an Agency's system as part of the process of obtaining an accreditation for system operations, (2) having direct applicability to general application subsystems as evaluated subsystem products, and (3) having applicability across a wide range of applications wherein the protection mechanisms might generally provided by the underlying computer system (i.e., hardware, operating system, and communications subsystems). While our control objectives are directed at the third interpretation, the reader will find that we did not similarly confine our commentary notes on the selected policy text contained in Appendix A. Our intention in the latter was to take a much broader system perspective and then selectively use the material in supporting the specific wording of our control objective proposals.

TABLE 1.1. List of Policy Documents

POLICY DOCUMENT

TITLE

FEDERAL LAWS

Public Law 92-579

The Privacy Act of 1974

Public Law 101-508

Computer Matching and Privacy Protection Amendments of 1990

Public Law 96-511

The Paperwork Reduction Act of 1980

Public Law 97-255

Federal Manager's Financial Integrity Act of 1982

Public Law 97-86

DoD Authorization Act of 1982

Public Law 100-235

Computer Security Act of 1987

EXECUTIVE/LEGISLATIVE

OMB Circular No. A-127

Financial Management Systems

OMB Circular No. A-130

Management of Federal Information Resources

OMB Circular No. A-123

Internal Control Systems

OMB Bulletin No. 90-08

Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

OMB IC Guidelines

Internal Control Guidelines

GAO Title II

GAO Policy and Procedures Manual for Guidance of Federal Agencies-Title 2 - Accounting

DEPARTMENT OF DEFENSE

DoD Directive 5010.38

Internal Management Control Program

DoD Directive 5200.28

Security Requirements for Automated Information Systems

DoD Directive 7740.1

DoD Information Resource Management Program

DoD Guideline 7740.1-G

ADP Internal Control Guideline

DoD Directive 7750.5

Management and Control of Information Requirements

2. PROPOSED CONTROL OBJECTIVES

The proposed control objective revisions contain the following major elements: (1) an introduction to the control objective, (2) the original and revised control objectives, and (3) a discussion of issues and rationale for revising the control objective. The discussion and supporting rationale are intended to be useful whether the original control objectives are to be modified as we propose, or entirely new control objectives are to be developed.

When broadening the scope of the TCSEC to include integrity, we must consider the effect upon the existing control objectives. There are two basic considerations: (1) whether integrity policies call for additional technical features to be included in the control statements, and (2) whether the existing abstractions currently associated with the statements of control are adequate, given the increased scope of protection. Each factor could have a subsequent effect on the control objective. The requirement for additional technical features would compel a modification to the control objective itself and is reflected in the proposed revisions. Generalizing control abstractions would require a change in the interpretation of the statements of control. These interpretation changes are noted in the discussion section of each affected revision.

As stated in the TCSEC [1985, p. 71], ``There is a large body of policy laid down in the form of Regulations, Directives, Office of Management and Budget (OMB) Circulars,

Presidential Executive Orders, and Laws that form the basis for the handling and processing of Federal information in general and classified information specifically." We follow the TCSEC's example and illustrate the relationship of pertinent integrity policy to product evaluation criteria using excerpts from Federal laws and Executive, Legislative, and Department of Defense (DoD) policy documents.

The set of policy statements and guidance that are related to integrity in automated information systems (AISs) are discussed in Appendix A. The security policy to be specified for a given system should be derivable from this set of policies in conjunction with those already cited in the TCSEC. The policy statements of interest originate from one of three sources: the Federal or Executive branches of government, or the DoD.

Federal law addressing issues of integrity in information processing is best interpreted not only by examining the Acts of Congress but also their legislative histories, which aids one in understanding the establishment or modification of law.

The Executive branch of government, in implementing the laws passed by Congress, issues directives and broad guidance to departments and agencies. The most significant of these OMB (policy) Circulars are summarized with respect to their effect on integrity. The General Accounting Office (GAO) is tasked by Congress to provide auditing and accountability services to the Legislative Branch of Government. In providing such services GAO issues related guidelines and standards for the Federal government. These guidelines and standards are cited as references in various policy statements included in our study, and hence are relevant to those policies of interest.

The DoD has the responsibility for interpreting and implementing the policy issuances from higher authority. This is done via DoD Directives, regulations, manuals and other guidance formats. Each of these DoD policy issuances must be interpreted and

implemented by the DoD Components and Agencies.

2.1 SECURITY POLICY

In general, a security policy states what protection controls should be provided in the administration or operational management of a set of valued resources. A security policy may define the protection requirements in terms of perceived threats, risks, and/or goals of an organization. Security policy from the highest levels of Government (e.g., Laws and Executive Orders) is put into force through its promulgation in subordinate Agency or Component implementation directives. Each subsequent level refines the implementation detail for protection. When these implementation details are carried out, the policy is enforced. As the general policy statements are refined, the resulting statements of specific requirements serve to drive product specifications for the design and operation of policy enforcement mechanisms. Thus, ``a given system can only be said to be secure with respect to its enforcement of some specific policy" [TCSEC 1985, p. 59].

2.1.1 Original and Revised Security Policy Control Objectives

Original

A statement of intent with regard to control over access to and dissemination of information, to be known as the security policy, must be precisely defined and implemented for each system that is used to process sensitive information. The security policy must accurately reflect the laws, regulations, and general policies from which it is derived [TCSEC 1985, p. 59].

Revised

A set of statements of intent with regard to controls over computing resources and information processing including origination, acquisition, access, use, maintenance, dissemination, and disposal of information within computer systems, to be known collectively as the security policy, must be precisely defined and implemented for each system that is used to process classified and sensitive information. The security policy must accurately reflect the laws, regulations, and general policies from which it is derived.

2.1.2 Discussion

Automated information system security policy is a set of statements indicating the protection controls that should be focused on computing resources and on how information within computer systems is originated, acquired, accessed, used, maintained, disseminated, or disposed. The current Security Policy control objective is limited by the breadth and scope of the laws, regulations, and general policies from which it is drawn, i.e., non-disclosure of classified and other sensitive information. To extend the breadth and scope of the TCSEC Security Policy control objective to integrity, one must first examine the regulations, policies, and/or laws that might be applicable.

Although existing policy [DoD 5200.28-D] states that safeguards for the preservation of systems and data integrity shall be in place in DoD computers, implementing

regulations and manuals do not precisely define the means for providing these safeguards. This is in contrast to the uniform system for safeguarding national security information as prescribed by Executive Order 12356 [EO 12356], which specifically assigns responsibility to promulgate implementing regulations for confidentiality protection. This assignment of responsibility has led to well-defined regulations for protection against unauthorized disclosure, (e.g., [DoD 5200.1-R]). There appear to be no Executive Orders of equivalent weight and specificity for the direct establishment of regulations for integrity, and thus regulations applicable to system or data integrity are not as specific and well-defined.

There are Federal laws and policies which both directly and indirectly address integrity issues. We assert both as being applicable to integrity protection. They address, in an overlapping fashion, requirements for automated information security, information and internal management, and internal controls. These laws and policies are individually summarized in Appendix A. In addition to current TCSEC policy guidance on confidentiality, the integrity requirements and guidelines provided by these laws and policies should be used to shape the detailed security policy into a clear specification of what must be done to preserve and promote both confidentiality and integrity.

The essence of these laws and policies with respect to information security pertains to the definitions of sensitive government information and sensitive applications, and the protection of sensitive information from loss, misuse, unauthorized access, or modification. Specific to integrity, these laws and policies require that information must be protected from unauthorized, unanticipated or unintentional modification including the detection of such activities. Personnel, life support, safety critical and financial transaction systems are cited as sensitivity examples. The laws and policies define restrictions on the collection, use, and maintenance of information in Federal AISs, including timeliness, accuracy, and completeness, and relevance to the agencies needs. They require appropriate safeguards and individual accountability. The essence of the laws and policies with respect to information and internal management pertains to the definition of information and computer resources as assets that must be managed, and to the establishment of management controls. These management controls include internal management control procedures, general supervision, input/output and procedural controls for information processing operations, system administration, information resource management, training, responsibility assignments, resource allocation, and vulnerability assessments.

The essence of laws and policies with respect to internal controls pertains to individual competence, authorization, and accountability; data and application validation; data completeness, accuracy, and timeliness; and auditability and other procedures to maintain and to periodically determine the extent of conformance with legal and ethical standards.

Several Federal laws, along with their implementing policies, mandate action to preserve and promote data and systems integrity and considerably broaden the scope of protection requirements over those requirements for confidentiality. The proposed revision reflects these broader protection requirements by modifying the original TCSEC version to allow a comprehensive coverage of controls. This modification preserves the intent of the original objective with respect to control for confidentiality and allows for

the incorporation of additional controls for integrity.

The modification pluralizes the ``statement of intent'' and the term ``control'' to recognize a wider variety of protection intents and controls and then collectively terms them ``the security policy.'' Further, it removes the more narrowly focused words ``access to and dissemination of information'' from the original objective statement and replaces those words with the phrase ``information processing including origination, acquisition, access, use, maintenance, dissemination, and disposition of information within computer systems.'' Each of these elements should have a precise statement of enforcement requirements with the collective statement resulting in a consistent and complete security policy.

2.2 MANDATORY CONTROL

Mandatory security is based on laws or regulations which establish the rules that must be enforced and the designations of attributes to be used by these rules. Thus, it is often referred to as ``rule-based'' security. In the TCSEC, mandatory security refers to the enforcement of a set of access control rules that constrains an individual's access to information on the basis of a comparison of attributes that designate an individual's clearance and/or authorization to the information, the classification and/or sensitivity designation of the information, and the form of access being mediated. In general, system enforcement of mandatory policies either requires or can be satisfied by systems that implement a partial ordering or mathematical lattice of such designations [TCSEC 1985, p. 60].

2.2.1 Original and Revised Mandatory Security Control Objectives

Original

Security policies defined for systems that are used to process classified or other specifically categorized sensitive information must include provisions for the enforcement of mandatory access control rules. That is, they must include a set of rules for controlling access based directly on a comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information being sought and indirectly on considerations of physical and other environmental factors of control. The mandatory access control rules must accurately reflect the laws, regulations, and general policies from which they are derived.

Revised

Security policies defined for systems that are used to process classified or other specifically categorized sensitive information must include provisions for the enforcement of mandatory access control rules. That is, they must include a set of rules for controlling access based directly on (1) a comparison of the individual`s clearance or authorization for the information and the classification or sensitivity designation of the information being sought, and/or (2) a comparison of the duty to be performed with the duties mapped in the individual's current role, and indirectly on (3) considerations of physical and other environmental factors of control. The mandatory access control rules must accurately reflect the laws, regulations, and general policies from which they are derived.

2.2.2 Discussion

Integrity protection requires that user actions be constrained by mandatory controls beyond the traditional specification of a sensitivity label and a formal authorization that form a ``confidentiality'' lattice. These additional constraints will be described in this discussion.

It is Federal law that any information which could adversely affect the national interest must be protected from loss, misuse, unauthorized access, and unauthorized modification [CSA 1987]. It is also Federal law that ``internal accounting and administrative controls... shall provide reasonable assurances that [resources] are safeguarded against waste, loss, unauthorized use, or misappropriation'' [FMFIA 1982]. Federal and DoD policy reflect these protection requirements in their implementing directives. For example, it is Federal policy that resources must be ``protected against fraud, waste, mismanagement or misappropriation'' [OMB A-123, p. 1].

Separation of duties is a mandatory policy that has been implemented, particularly in the commercial sector, to address fraud, misuse, etc. Separation of duties also is cited explicitly as an internal control standard [GAO 1983] and is required in several Federal and DoD policies. DoD's directive on its internal management control program, [DoD 5010.38-D], in discussing dependencies for internal control, provides rationale for this mandatory policy. ``Internal control depends largely on the elimination of opportunities to conceal errors or irregularities. This, in turn, depends on the assignment of work in such a fashion that no one individual controls all phases of an activity or transaction'' [DoD 5010.38-D, Encl.3]. From this requirement to separate duties or phases of an activity, we derive the need for implementing the concept of roles. To separate duties, attributes must be identified that will allow duties to be categorized into different sets. We define a duty to be an operation on an object, class of objects, or defined system resource; it provides the binding for objects and operations. Each set of duties is mapped to a role. Thus, a role is an encapsulation that defines which duties (i.e., manual or automated operations on particular objects, classes of objects, or system resources) a user possessing the designation of that role is allowed to perform (invoke). In essence, a role conveys a ``privilege'' to perform a set of duties; it provides the binding for users, operation, and objects. Roles aggregate users, duties aggregate objects and their operations.

Where separation is required, two roles may have partially but not totally overlapping duties; no single role can encompass all of the duties required to complete a sensitive activity or transaction. Roles may be assigned as expressly permitted or denied, or they may be enabled by a sequence of events performed by another role. Once the duties are divided between different roles, the system or role administrator must ensure that a single individual is not given multiple roles that would effectively allow that individual to perform all duties required to process a sensitive transaction. For example, if duties A, B, and C are required to perform a particular transaction, the system might assign duties A and B to role 1 and duty C to role 2 to achieve separation of duties. But, in order to maintain the separation, the system or role administrator must ensure that the same individual is not assigned to both role 1 and role 2.

Roles must be registered in the system for all operations on objects, classes of objects, and system resources. Newly created operations cannot be invoked without the intervention of a system or human administrator to register the operation's associated roles. Roles assigned to individuals must relate to roles assigned to operations according to mandatory rules, (e.g., separation of duties must be enforced). These role designations can provide partial ordering and dominance relations necessary for the mechanics of a lattice.

DoD policy constrains the concept of separation of duties even further by requiring ``authorized [resource] access and [transaction] execution'' [DoD 5010.38-D, Encl.3]. From this mandatory policy requirement, we derive the joining together of the (authorized) individual, in a specific role, executing a specified duty (i.e., operation), on a specific resource (i.e., data object). By combining access to data with separation of duties, the computer system must implement user-program-data bindings to control which users can invoke which programs on particular data items. A model for achieving user-program-data bindings is given in [Clark 1987, 1989]. Our approach is to use roles and duties as the bindings. Lee [1988] discusses an alternative approach using roles in a lattice to implement the Clark and Wilson model.

Mandatory controls address more than access control, they also address information flow. Where the integrity issue of ``contamination'' of high quality information with low quality information from low quality sources is a mandatory concern, the ability to attribute subjects and objects with a designated quality grade will be required. Biba [1977], in his integrity model, introduced the term integrity grade to designate gradations of quality for subjects and objects. In essence, an integrity grade is a determination of a subject or object's quality with respect to a defined standard. In this respect, such a grade can be thought of as analogous to a classification or a sensitivity label in the DoD scheme. These integrity designations also would provide partial ordering and dominance relations necessary for the mechanics of a lattice structure.

DoD requirements for integrity grades for subjects are derivable from the statement that ``managers and employees shall have personal and professional integrity and shall maintain a level of competence that allows them to accomplish their assigned duties...'' [DoD 5010.38-D, Encl.3]. This ``competency'' requirement implies some specific standard of quality associated with an individual (e.g., a level of professional maturity). It further implies that individuals not meeting a certain level of quality should not be allowed to perform certain duties, because they may lack competence to successfully accomplish such duties. Thus, we derive a mandatory requirement to characterize individuals, in conjunction with their role specification, with a level of quality that reflects their ability to carry out specified duties (e.g., apprentice, journeyman, master, supervisor).

Integrity grades for objects are not always directly derivable from formal standards or policy, but often can be derived from experience. Here, we are concerned with attributes of information that indicate the information's ``maturity'' (e.g., initial, preliminary, and final versions) that convey a degree of effort placed into developing the information and the results of that effort to a subjective or objective standard. In this case, the idea of maturity recognizes that earlier versions of information may not have as high a ``quality'' as later versions. Similar attributes, some with specific standards such as

precision, accuracy, etc., can be addressed under the rubric of information quality.

Where contamination is an issue, a specific set of information flow rules must be established. For example, a rule based on the competency of individuals might state that information entered by an expert cannot be modified by a novice. A rule based on the maturity of information (e.g., unedited version vs. final product version) might state that the ``quality'' of the information increases only by progressing the information through specific events (e.g., editing and formal review). It is through this event progression that the effort put into the information's development is seen to produce measurable results (e.g., edited and approved versions). As a further requirement, the information maturity rule might state that a proper sequence of such events must be followed. To be enforceable, these potential mandatory quality rules will require some form of integrity grade designation implementation. The standards for such integrity designation requirements have not been developed for widespread use, and attributing subjects and objects with gradation designations may not be as straightforward for integrity policies as was the case for confidentiality policies.

The additional comparisons added to the mandatory controls are seen to be vital in preserving the integrity of systems and data. With these comparisons, we recognize that there are at least two levels of mandatory control. The first level provides a reference monitor which is invoked to meet the requirements of preventing disclosures of classified information and/or preventing contamination of high quality information with low quality information. Notice that although the same wording used in the original control objective has been used in (1), it is interpreted to imply the extension of integrity grades to prevent contamination. The second level provides mandatory indirection between a user and system resources to enforce separation of duty as well as control of object execution, modification, or manipulation. This second level of mandatory control extends the notion of a reference monitor provided by the first level, and provides more discrete control by binding the user authorization to a particular action upon a particular object.

2.3 DISCRETIONARY CONTROL

The concept of discretionary control extends from the principle of ownership, providing for user-controlled sharing that promotes the maximum efficiency of system data and resource administration while retaining protection effectiveness. Efficiency is gained by reducing central system administration and effectiveness is maintained by bounding an individual's discretion. Thus, discretionary control is the administration of data and resources by individuals who are provided with a set of explicit and/or implicit privileges to operate on sets of those data and resources, and with the ability to grant or deny (at their discretion) privileges for the data and resources under their control to other individuals. Because it is related to explicitly identifying individuals, this form of control often is termed identity-based control. The original Discretionary Security control objective was derived from DoD confidentiality policy requiring each individual, in addition to being cleared for access, to also have been determined by a competent authority to have a need-to-know for particular items of information for the performance of that individual's job. The concepts and mechanisms developed originally to implement controlled sharing were employed to enforce need-to-know.

2.3.1 Original and Revised Discretionary Security Control Objectives

Original

Security policies defined for systems that are used to process classified or other sensitive information must include provisions for the enforcement of discretionary access control rules. That is, they must include a consistent set of rules for controlling and limiting access based on identified individuals who have been determined to have a need-to-know for the information [TCSEC 1985, p. 61].

Revised

Security policies defined for systems that are used to process classified or other sensitive information must include provisions for the enforcement of discretionary control rules. That is, they must include a consistent set of rules for controlling and limiting (1) access based on identified individuals who have been determined to have a need-to-know for the information, and (2) execution of duties based on identified roles and individuals who have been determined to have a need-to-perform those duties.

2.3.2 Discussion

The wording of the existing control objective reflects its original focus. The term ``need-to-know'' is relevant only to confidentiality, and has no essential bearing in terms of integrity policies. It can be argued that beyond this single instance, the wording of the existing control objective is general enough to apply to integrity protection. However, although the term ``access'' is currently interpreted in the general sense for AIS security [NCSC 1988, p. 3], in many regulations its meaning is strictly limited to confidentiality. Examples of more narrow usage can be found in [DoD 5200.1-R] and the Privacy Act of 1974 [PA 1974]. Still, if the over-specificity of its terms were its only deficiency, the existing control objective could serve the purposes of integrity with relatively minor changes.

The restricted scope of the existing control objective also results in a more fundamental flaw when considering integrity protection at a purely functional level. Because integrity protection is concerned with the flow of information into an object, ``proper'' modifications can only be defined in terms of the particular code segment (e.g., program) which performs a modification. In particular, the code which manipulates an object must do so by adhering to the object's format, at a minimum. Because functional concerns require the binding of particular code to a particular object or class of objects for integrity protection, it follows that ``privileges'' should not allow a less restrictive binding. The generality implied by ``controlling and limiting access to... information,'' is simply insufficient to convey the required degree of protection. This concept is expressed through the definition of a duty, as discussed in Section 2.2.2, under Mandatory Control.

One needs to consider the differences between the basic concerns of confidentiality and integrity to understand why this additional degree of control is required. Confidentiality protection is concerned with preventing the unauthorized flow of information from one object to another. This flow is characterized essentially by one class of operation

performed by a system (i.e., ``read''). In terms of information flow, each and every ``read'' operation can be considered equivalent. Such a simplification is not possible for integrity protection. The inward-directed information flow is, similar to confidentiality, characterized by a single class of operation (i.e., ``write''). However, in contrast to the apparent equivalence of all read operations, write operations are distinguished by the context in which they are performed. For example, two programs, each performing a series of write operations upon an object, may produce entirely different effects in terms of the object's integrity. In this regard a ``write'' privilege, in giving a user the right to modify an object in a very general manner, does not provide the correct level of abstraction in specifying privileges in terms of integrity protection.

A relationship between mandatory and discretionary controls has been assumed in the preceding discussion: the rules specifying what is allowable under mandatory controls are expressed at the same level of abstraction at which discretionary controls are applied. For instance, the Bell-La Padula model definition of allowable operations for both mandatory and discretionary controls are equivalent sets (i.e., read, write, and execute operations) [Bell 1975]. It should not be assumed that this equivalence relation must always be present. It is possible for discretionary controls to exist in the absence of mandatory controls. In such a case, an equivalence relation is neither possible nor necessary. The converse case, where mandatory controls exist in the absence of discretionary controls, is not explicitly excluded by the original TCSEC control objectives, although it is excluded in the actual Criteria. However, it is likely that this converse case may be more acceptable in practice for integrity protection than for confidentiality protection, and subsequent evaluation criteria should address such a possibility. In addition, we assert that whenever both mandatory and discretionary protection is provided by a system, there must be an equivalence relation between mandatory and discretionary control abstractions.

A consequence of this relationship is the complementary role in which mandatory and discretionary controls provide comprehensive protection. If ``privileges'' are expressed using identical abstractions, mandatory controls can enforce the context in which a privilege is valid, while discretionary controls imply the permission to exercise the privilege, given a valid context. One way of looking at this relationship is that mandatory controls specify what is potentially allowed, while discretionary controls specify what is intentionally allowed. The two sets of controls are complementary in that access is dependent upon passing both mandatory and discretionary tests. This complementing property can only exist if the operational classes at both the mandatory and discretionary levels are equivalent, as discussed above. We assume that such a complementing property between mandatory and discretionary controls for integrity protection would be desirable, as has been the case for confidentiality protection. We have discussed under the Mandatory Control (Section 2.2.2) the basic abstractions, defined as roles and duties, which capture the necessary elements for integrity protection.

Bacic [1989], in addressing integrity as set forth in the Clark and Wilson Model [Clark 1987], suggests that discretionary controls for integrity are user-defined execution controls. Bacic notes that these discretionary controls operate at the user level, provide access only to executable objects, and are confined to a set of duties (i.e., the role) for an

individual as prescribed by mandatory controls. Bacic's discretionary execution controls (DECs) complement his mandatory execution controls (MECs) and can be viewed as a logical extension of discretionary access controls. They relate a user to a set of processes (e.g., a program) that fulfills a set of duties which can only execute on particular sets of data objects. We find that integrity protection can be provided only by addressing discretionary concerns at these (more complex) levels of specification and abstraction. However implemented, execution controls essentially define roles. As such, the proposed control objective addresses the appropriate relationship between roles and duties for discretionary integrity protection with the term ``need-to-perform."

In addition to proposing changes to the existing control objective, we need to examine the traditional abstractions associated with discretionary controls, in order to interpret the subject in the context of integrity protection. The distinguishing feature of existing discretionary controls is the capability they provide to allow an individual to control access to resources, based on a ``principle of ownership." An ``owner" (often the creator) of a resource possesses a set of privileges over that resource, of which each may be granted explicitly to other users. In some implementations, the ``grant" privilege itself may be conveyed to other users, either for singular privileges or for the entire set of privileges inherent to the owner.

The principle of ownership must be generalized for integrity protection to embody role administration. The administrator of a set of resources should not have the privileges that the analogous ``owner" of property has; rather, ownership should be considered a special case of administration. The definitions for sensitive data and sensitive application found in [OMB A-130, p. 52742] imply that an individual creating, using, or maintaining sensitive resources should have strictly limited administrative rights to those resources. For example, a user creating an object associated with sensitive information or a sensitive application should not necessarily have the ability to destroy that object at the user's discretion. Therefore, an AIS should support the ability to restrict the set of default privileges associated with the administration of resources, on a per-application basis. Additionally, an AIS should support the ability to designate individuals (other than the creator) as having discretionary administrative control over a particular resource or set of resources.

Similarly, an administrator of a set of resources should not, in general, be able to grant privileges to other entities simply because he possesses such privileges. In other cases, it may be appropriate for an administrative user to grant certain privileges to other users which are unavailable to the administrator. This issue is related to a broader area of concern: the control over propagation of privileges. A user receiving access to a resource via discretionary controls should not, in general, be able to arbitrarily pass that privilege on to other entities, nor to amplify the privilege in any way. Therefore, an AIS should support measures to arbitrarily define which discretionary privileges are ``grantable" and provide a means to prevent the (undesired) propagation of privileges, on a case-by-case basis (i.e., per application).

These discretionary issues must be addressed through use of the same abstraction(s) in which mandatory controls are expressed (i.e., roles). The role-implementing features of a system must therefore address three different areas of functionality. The first area is the definition of roles with respect to a set of processing resources. This set of resources can

be described as the domain to which the defined roles are applicable. The definition of roles within a domain is an administrative function associated with mandatory policies. Also, this definition must include the specification of which users are authorized to operate within the defined domain. The second area which must be addressed is the discretionary administration of the system-defined roles. Conceptually, this area implements the ``ownership'' of roles, under which domain-specific roles can be allocated or assigned. The third area which must be provided by the system is the binding of a subject (i.e., a user-process pair) to only those actions defined by its operational role.

Note that together these three areas of functionality provide an equivalence set between mandatory and discretionary controls to provide complementary protection mechanisms. The mandatory specification defines which resources, roles, and individuals are available, and who has discretionary control over the assignment of roles. The ``owner'' or role administrator of the domain assigns roles and resources to individuals. For a user to operate within a role, that user must be specified through the mandatory definition as being allowed to operate within that domain, and be assigned a role and resources by the ``owner'' of the domain.

Clark and Wilson [Clark 1987, 1989] provide a set of extended access controls which address some of the deficiencies associated with the traditional notion of discretionary controls in providing integrity protection. In their model, access control is specified (via ``triples'') in terms of controlling accesses by identifiable segments of code (i.e., the ``transformation procedure'' or TP) to specified objects. This additional restriction is similar to the type enforcement mechanisms of certain programming languages, although it is applied at the system level. Thus, this feature of the model can be considered to involve a finer specificity of control than contained in traditional DAC. However, the notion of ``discretion'' in [Clark 1989] is distinct in that there is no explicit mechanism by which (non-administrative) users can transfer privileges to others. Although the concept of ``triples'' is identity based, triples are not discretionary but are, in fact, mandatory.

This is not to say that extensions to the Clark and Wilson model could not address discretion access controls, however. The set of all triples which apply to particular user-object pairs is conceptually similar to our notion of a role definition.1 One can hypothesize a privilege-granting TP in which the object acted upon is the specification of privileges (i.e., a set of triples) for some other object. The triple specifying such a privilege-granting TP would give the specified user the ability to control access to particular objects under that user's administration, similar to the ability of owners to alter an access control list in

---

1. Roles, for different implementations, might also be interpreted as either the set of triples associated with a single object or those associated with a single user.

---

more traditional models. Thus, any particular subject may be an ``administrator'' with

respect to an arbitrary set of objects. This administrative user need not be privileged with respect to the system, nor to other resources outside a particular administrative domain. It may also be possible to construct arbitrary, discretionary control domains (e.g., hierarchical, independent, or overlapping), while retaining the beneficial extensions offered in the original Clark and Wilson model.

The proposed control objective revision recognizes that discretionary controls in support of data and systems integrity require extensions to traditional access control. Specifically, they require the ability of the user to specify-and the system to test for-the identity and authorization of an individual and that individual's role, as well as specific duties within the role that specify the functionality associated with the access. In essence, the integrity revision constrains discretionary control to user operations on executable objects. The term ``need-to-perform'' is intended to capture this essence of discretionary control with respect to integrity, as discussed in the previous review of [Bacic 1989]. Such controls necessarily would be further constrained by mandatory controls.

2.4 MARKING CONTROL

Marking is the concept of designating or providing information attributes, (e.g., classification or sensitivity), each having a specified range of values, that can be used in rule-based mechanisms to implement mandatory security policies. A clear implication of mandatory controls is that the system must assure that the mandatory security designations cannot be arbitrarily changed since such changes could permit individuals to access information in unauthorized ways.

Marking control is necessary to ensure accurate and consistent internal rule-based decision making and also necessary to ensure that, when the information is transformed to an external representation, the marking conveys how the information is to be handled in the external world. Since these attribute values, or labels, are key to decision making, it is important that they remain essentially stable. Labels should be created and maintained by the system, or installed and maintained by specified systems administrators, and only changed in a well-defined manner so that a label continues to be consistent with the sensitivity of the information that the label represents.

2.4.1 Original and Revised Marking Control Objectives

Original

Systems that are designed to enforce mandatory security policy must store and preserve the integrity of classification or other sensitivity labels for all information. Labels exported from the system must be accurate representations of the corresponding internal sensitivity labels being exported [TCSEC 1985, p. 61].

Revised

Systems that are designed to enforce mandatory security policy must store and preserve the integrity of classification, other sensitivity, or integrity labels for all information. The labeling must be sufficient to implement rule-based checking of mandatory linkages between subjects, data, and operations upon the data as required by the mandatory control objective. Labels exported from the system must be accurate representations of

the corresponding internal labels being exported.

2.4.2 Discussion

Identification of attributes used in mandatory rule-based decisions are key to marking requirements. Many of these attributes may be developed in the context of an application rather than at the operating system level. It is important that the overall protection system maintain the integrity of any labels required by the marking policy even if the labels are developed at the application level.

The marking policy and specific marking requirements for handling classified information to prevent unauthorized disclosure are well covered in the TCSEC. Numerous policy documents are cited in the TCSEC with clear confidentiality marking requirements. There are no similar ``clear'' statements in policy to convey the marking requirements for integrity.

Given the integrity constraints described under the proposed mandatory control objective, we can now derive marking requirements for integrity. From the mandatory requirement for separation of duties, we derived the need to identify within the system a set of roles, each with a unique set of duties. Roles themselves can be used as marking designations, as can the duties they encapsulate. Each duty is mapped to specific system operations on objects and resources. At some level of abstraction, separated duties may be identified as either ``enabling'' or ``completing'' functions [Guttman 1991], and the same individual should not have the ability to perform both in the same role. This constraint may imply the requirement that certain objects carry an ``enabled'' label.

From the mandatory requirement to join together an individual, in a specific role, executing a specified program on a specific data set, we derived the need to effectively implement user-program-data bindings. Here, the options may be to use some variation of Clark and Wilson ``triples'' [Clark 1987]. Variations could include labeling each system operation with the set of roles established for manipulating the specified data set (e.g., use of abstract data types (ADTs)), with each individual user or process being linked to a specified set of ADTs. This set of rules acts as an access control list (ACL) such that each individual user or process gains access only to specified operations. For finer granularity, the set of roles also could be used as labels on individual data items with the user or process gaining access to a specified operation on the specified date item only if the user or process role matched a role on the data item's list of roles.

To prevent the contamination of high quality information with low quality information, we derive a requirement to mark subjects (in conjunction with the use of roles) and objects with a level of quality, or integrity grade. For subjects, the integrity grade should reflect an individual's ability to carry out specified duties (e.g., apprentice, journeyman, master, supervisor). For objects, the integrity grade should reflect the data's quality (e.g., initial draft, preliminary strawman, final prototype, final finished product). Such terms again indicate a level of quality, maturity, or competence against some objective or subjective standard.

The marking changes extend labeling to integrity attributes of information and require labels to support the mandatory integrity linkages (i.e., separation of duties, user

program data bindings, and integrity grades) made in the mandatory control objective.

2.5 ACCOUNTABILITY CONTROL

The concept of holding an individual accountable for his actions is fundamental to policy enforcement. Accountability can be defined, traditionally, as ``the property that enables activities on a system to be traced to individuals who may then be held responsible for their actions" [NCSC 1988, p. 4]. The concept requires the ability to continuously identify individuals with their actions and with those of their surrogates within the system. To be effective, mandatory and discretionary security policies are dependent upon a system's ability to adequately identify, authenticate, maintain individuation, and account for those individuals to which access controls are applied. The ability to record and review the (system-related) actions of individuals provides (1) a deterrent to malicious actions, (2) a means to detect malicious actions or attempts, and (3) the ability to undertake preventive measures when attacks are detected. Thus, the concept further requires that a history of an individual's actions and the system's reactions be continuously maintained and protected from unauthorized manipulation for real-time or subsequent use in auditing analyses.

2.5.1 Original and Revised Accountability Control Objectives

Original

Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability, the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty [TCSEC 1985, p. 62].

Revised

Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Systems must assure that the accountability for individual performance of duties can be determined through an independent consistency check between internal representations of information within the system and the external information being represented. Systems must maintain the required degree of logical consistency for duplicate, identically derived, and/or corresponding internal instances of the same information throughout the existence of such information on the system. Furthermore, to assure individual accountability, the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty.

2.5.2 Discussion

It is the policy of the U.S. Government that agencies ``shall establish and maintain a cost-effective system of internal controls to provide reasonable assurance that Government resources are protected against fraud, waste, mismanagement, or misappropriation..." [OMB A-123, p. 1].

DoD policy requires that each DoD component maintain accountability over their assets and that they implement a comprehensive system for internal management control that provides reasonable assurance: obligations and costs comply with applicable law; assets are safeguarded against waste, loss, unauthorized use, and misappropriation; revenues and expenditures applicable to DoD operations are recorded and accounted for properly [DoD 5010.38-D, pp. 1-2].

AIS internal control is defined within DoD guidelines as ``the steps taken... and all the methods and techniques used to safeguard AIS resources and provide reasonable assurance of the accuracy and reliability of computer-based input, processing and output; ensure the adherence to applicable laws, regulations and policies; and promote the effectiveness, efficiency and economy of AIS operations and systems" [DoD 7740.1-G, p. 1-4]. The DoD guidelines include the following specific forms of application control: authorized transactions, valid transactions, complete information, accurate information, timely information, secure system and data, and auditable system.

Accountability is fundamental to internal control and, as such, is a vital aspect of promoting and preserving systems and data integrity. Internal control adds another dimension to accountability, the application dimension.

The TCSEC's original control objective appears sufficiently general to include the specific requirements for integrity with respect to user activity on a system. However, there is no stipulation for the assignment of responsibility for actions which need to be performed and yet are not properly carried out. This ``deficiency" of action may affect, most characteristically, the internal and external consistency of the information maintained by a system. In many applications, the concept of accountability may require the synchronized comparison of internal information states with the external world the information represents.

As a result of this increase in scope for accountability, additional functionality will be required of systems conforming to this new control requirement. It would no longer be enough for a system to passively monitor and record user access activity, and provide the means to adequately review user access activity information. Instead, a system would need to be able to enforce authorized actions with respect to ``valid" objects, where an object's validity is determined through some measure of its internal and external consistency. This implies that a system would need to (1) define, specify, and enforce valid state transitions for objects, or (2) dynamically validate an object's state.

Both of these notions are presented by Clark and Wilson in [Clark 1987]. In their notation, an Integrity Verification Procedure (IVP) performs a dynamic check to determine whether objects controlled under the system's integrity policy conform to its specification, and a TP guarantees valid state-to-state transitions for controlled objects. Thus, an IVP may verify that an object accurately reflects the current status of an inventory item (external consistency), and a TP may guarantee that all copies of a particular object are updated concurrently (internal consistency). Individuals are directly linked to the execution of a TP or an IVP on a specific set of data.

The proposed changes to this control objective reflect an extension to traditional scope of

accountability. This revision is driven by internal management control policy requirements which outline the need for application controls including the proper correspondence between external information and the representation of that information on a system (i.e., data). In essence, this correspondence cannot occur without the proper recording of this external information and adequate reviewing procedures to verify that system data is accurate. These procedures are at least partially external to the system, and thus are best described as ``accountability'' control. Additionally, the individual's or system's initiation, use, and maintenance of duplicate or redundant data raise integrity issues with respect to accuracy, timeliness, and the effect of those attributes on the internal (logical) representations of information. The procedures to properly constrain these actions are policy driven and are, therefore, subject to accountability controls.

2.6 ASSURANCE CONTROL OBJECTIVE

The concept of assurance is concerned with the measures taken to guarantee that the implementation of protection features is correct and that it properly enforces security policies. A consideration for ``proper enforcement'' is whether the protection features accomplish what they are designed to do, but nothing else (i.e., there are no unspecified features implemented). The TCSEC defines two types of required assurance: life cycle and operational. Life-cycle assurance deals with the management of system design, development, and maintenance. In essence, lifecycle assurance provides confidence that a system's protection features are themselves protected from attack throughout the lifetime of the system. Life-cycle assurance includes the control of design changes and the effect changes may have in enforcement of the defined security policies. Operational assurance ``focuses on features and system architecture used to ensure that the security policy is uncircumventably enforced during system operation'' [TCSEC 1985, p. 63].

2.6.1 Original and Revised Assurance Control Objectives

Original

Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle [TCSEC 1985, p. 63].

Revised

Systems that are used to pro cess or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policies and must not distort the intent of those policies. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle. Application subsystems used to process or handle classified or other sensitive information must be designed, implemented, controlled, and operated in a manner which provides assurance that the goals of both application-specific security policies and system-wide security policies are met without circumvention.

2.6.2 Discussion

Although this control objective is sufficiently general to include the specific requirements for integrity, it should be noted that integrity requirements may have a different emphasis than confidentiality requirements. Because integrity dependencies are more likely to be domain specific as opposed to system wide, the development and introduction of any new application dealing with a particular (sensitive) data set will need to be tightly controlled. The ``correct implementation and operation'' concerns most likely will be interpretable primarily in the domain of the application. Thus, assurance control needs to be extended from the current systems domain to each specific application domain resident on the system.

The proposed assurance control objective recognizes that there exists the possibility of multiple, application-specific security policies which may apply only to particular subsets of resources within the system. Software residing within a particular application domain should only extend the degree of control over resources, and should in no manner nullify the degree of control required for all system resources or for resources within a different application domain. Assurance must be provided that application and system software meets the security policy objectives for both the system and the application. The ``adequacy'' of this assurance must be determined strictly in terms of the sensitivity of the application and resources within that domain.

2.7 FAULT TOLERANCE CONTROL

The concept of fault tolerance extends from the need to continue operations in the presence of faults. As there are no guarantees of the absence of some form of fault, risk reduction becomes the focus of this control. Tolerance is established through a robust ability to detect and correct faults, and through a risk analysis that enables the setting of thresholds to maintain an acceptable degree of processing robustness in degraded operational modes.

Increasing complexity of systems yields an increase in the number of potential failure points and places a greater demand for fault tolerant system implementations. Electronic parts fail, waveforms get scrambled, magnetic properties of media deteriorate, etc. With more complex computers being incorporated into more complex commercial and military aircraft flight control systems, industrial controllers, space applications, banking systems, etc., erroneous computer performance can be devastating to financial records, environmental safety, national security, and even human life. Therefore, when faced with potential failures in complex systems, fault tolerance plays an important part in maintaining data and systems integrity.

2.7.1 Original and Revised Fault Tolerance Control Objectives

Original

[There is no original control objective for fault tolerance contained in the TCSEC.]

Revised

Systems that support safety or mission-critical applications must provide measures to promote continued safe or correct operation, within defined tolerances, in the presence

of integrity failures. Systems must include provisions for detecting integrity failures, even if those failures cannot be corrected, and provisions for correcting integrity failures when possible. System designs must include provisions for identifying and classifying potential integrity failures, determining the likelihood of such failures, and possible outcomes of such failures.

2.7.2 Discussion

Fault tolerance essentially involves two parts. The first part is the detection of errors. Detection is necessary for a system to determine when a failure has occurred. Detecting errors that are corrected by the system is as essential as detecting failures that cannot be corrected, since such failures may indicate a potential degradation of system performance, or may indicate that the system is approaching a threshold at which errors are no longer correctable.

The second part of fault tolerance is the attempted correction of errors. In addition to simply detecting incorrect data, it is possible to use methods to correct errors in the data. The simplest approach to error detection would be to provide a certain number of redundant copies of the data, possibly by different channels, and then to compare these when determining whether the data integrity has been violated. This approach can be extended to error correction if it is possible to tell which of the redundant copies of the data has not been altered. Various error correction methods give varying probabilities of retrieving the original, unaltered data.

Applying the concept of fault tolerance is commonly associated with redundant processing. Redundancy in computer systems is a risk-reducing concept that involves the duplication of hardware, software, information, time, or other resources to detect the failure of a single duplicate component and to continue to obtain correct results despite the failure [Johnson 1989]. The same processing is performed by more than one process, and the results are compared to ensure that they match. The need for redundancy varies depending on the application. Redundant processing is commonly used in the implementation of critical systems in which a need for high reliability exists.

In some situations, it is sufficient to shut down a system when a failure occurs and is detected. This solution is not very efficient, but it may be the safest solution and at least it eliminates incorrect operations by the system. In many other situations, however, it is more important that the system continue to operate, even if the performance is degraded. For example, it may be more important for communications to continue during a time of war, even if many of the transmissions have to be ignored due to static, jamming, etc. In addition, it is important to ensure that safety or mission-critical applications that are time sensitive are guaranteed to execute within their time limitations. For example, an order to ``attack at dawn'' is not useful if it is not delivered until the next afternoon.

Systems that support safety or mission-critical applications must not only preserve integrity to the extent possible, but also must continue to operate in a safe or correct manner in the presence of integrity failures that result from unavoidable situations, such as physical failures of equipment or media. Fault tolerance requirements define what is meant by safe or correct operation, and the level of redundancy will vary depending on

these requirements. The system must detect when a failure has occurred before it can take any action. Once a failure is detected, there may be enough redundancy for correct operation to continue or it may be necessary to take action to correct the failure.

REFERENCE LIST

[1] Bacic 1989 - Bacic, E.M. 1989. Process Execution Controls as a Method for Ensuring Integrity. In Report of the Invitational Workshop on Data Integrity, January 25-27, 1989, Gaithersburg, Maryland, B.2-1B.2-8. Gaithersburg, MD: National Institute of Standards and Technology. NIST Special Publication 500-168.

[2] Bell 1975 - Bell, D. and L. La Padula. 1975. Secure Computer System: Unified Exposition and Multics Interpretation. Bedford, MA: MITRE Corporation. MITRE Technical Report 2997.

[3] Biba 1977 - Biba, K.J. 1977. Integrity Considerations for Secure Computer Systems. Bedford, MA: MITRE Corporation. MITRE Technical Report 3135.

[4] Clark 1987 - Clark, D.D. and D.R. Wilson. 1987. A Comparison of Commercial and Military Computer Security Policies. Proceedings of the IEEE Symposium on Security and Privacy, April 27-29, Oakland, California, 184-194. Washington, D.C.: IEEE Computer Society Press.

[5] Clark 1989 - Clark, D.D. and D.R. Wilson. 1989. Evolution of a Model for Computer Integrity. In Report of the Invitational Workshop on Data Integrity, January 25-27, 1989, Gaithersburg, Maryland, A.2-1A.2-13. Gaithersburg, MD: National Institute of Standards and Technology.

[6] CMPPA 1990 - U.S. Congress. Computer Matching and Privacy Protection Amendments of 1990. Public Law 101-508. November 5, 1990. Washington, D.C.: U.S. Government Printing Service.

[7] CSA 1987 - U.S. Congress. House. Computer Security Act of 1987. Public Law 100-235. January 8, 1988. H. R. 145. Washington, D.C.: U.S. Government Printing Service.

[8] DoD 5200.1-R - Department of Defense. 1986. Information Security Program Regulation. DoD Regulation 5200.1-R. Washington, D.C.: U.S. Government Printing Office.

[9] DoD 5200.28-D - Department of Defense. 1988. Security Requirements for Automated Information Systems (AISs). DoD Directive 5200.28-D. Washington, D.C.: U.S. Government Printing Office.

[10] DoD 5200.28-M - Department of Defense. 1973. ADP Security Manual. DoD Manual 5200.28-M. Washington, D.C.: U.S. Government Printing Office.

[11] DoD 5010.38-D - Department of Defense. 14 April 1987. Internal Management Control Program. DoD Directive 5010.38-D. Washington, D.C.: U.S. Government Printing Office.

[12] DoD 7740.1-D - Department of Defense. 20 June 1983. DoD Information Resources Management Program. DoD Directive 7740.1-D. Washington, D.C.: U.S. Government

Printing Office.

[13] DoD 7740.1-G - Department of Defense. Office of the Assistant Secretary of Defense (Comptroller). July 1988. ADP Internal Control Guideline. DoD Guideline 7740.1-G. Washington, D.C.: U.S. Government Printing Office.

[14] DoD 7750.5-D - Department of Defense. 7 August 1986. Management and Control of In-
formation Requirements. DoD Directive 7750.1-D. Washington, D.C.: U.S. Government Printing Office.

[15] DoDAA 1982 - U.S. Congress. Senate. Department of Defense Authorization Act, 1982.
Public Law 97-86. December 1, 1981. S. 815. Washington, D.C.: U.S. Government Printing Service.

[16] EO 12356 - The White House. 2 April 1982. National Security Information. Executive Order 12356. Washington, D.C.: U.S. Government Printing Office.

[17] FMFIA 1982 - U.S. Congress. House. Federal Managers' Financial Integrity Act of 1982. Public Law 97-255. September 8, 1982. H. R. 1526. Washington, D.C.: U.S. Government Printing Service.

[18] GAO 1983 - Government Accounting Office. 1 June 1983. Office of the Comptroller. Standards for Internal Control in the Federal Government. Washington, D.C.: U.S. Government Printing Office.

[19] GAO Title 2 - Government Accounting Office. August 1987 (Revised May 1988). Office of Policy. GAO Policy and Procedures Manual for Guidance of Federal Agencies-Title 2, Accounting. Washington, D.C.: U.S. Government Printing Office.

[20] Guttman 1991 - Guttman, Joshua. 4 March 1991. Private communication with authors.

[21] H. Rept. 100-153(I) - U.S. Congress. House. Committee on Science, Space, and Technology. Legislative History of the Computer Security Act of 1987. June 11, 1987. House Report No. 100-153(I). Washington, D.C.: U.S. Government Printing Service.

[22] Johnson 1989 - Johnson, Barry W. 1989. Design and Analysis of Fault-Tolerant Digital Systems. Reading, MA: Addison-Wesley.

[23] Lee 1988 - Lee, Theodore M.P. 1988. Using Mandatory Integrity to Enforce ``Commercial'' Security. In Proceedings of the IEEE Symposium on Security and Privacy, April 18-21, 1988, Oakland, California, 140-146. Washington, D.C.: IEEE Computer Society Press.

[24] Mayfield 1991 - Mayfield, Terry, J. Eric Roskos, John M. Boone, Stephen R. Welke, and Catherine W. McDonald. 1991. Integrity in Automated Information Systems. Alexandria, VA: Institute for Defense Analyses. IDA Paper P-2316.

[25] NCSC 1988 - National Computer Security Center (NCSC). 1988. Glossary of Computer Security Terms. Washington, D.C.: U.S. Government Printing Office.

[26] OMB 1991 - Office of Management and Budget. 4 March 1991. ``Advance Notice of Plans for Revision of OMB Circular A-130," in the Federal Register, Vol. 56, No. 42., pp. 9026-9028. Washington D.C.: U.S. Government Printing Office.

[27] OMB ICG - Office of Management and Budget. December 1982. Internal Control Guide-
lines: Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government. Washington, D.C.: U.S. Government Printing Office.

[28] OMB 90-08 - Office of Management and Budget. 9 July 1990. Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information. OMB Bulletin No. 90-08. Washington, D.C.: U.S. Government Printing Service.

[29] OMB A-123 - Office of Management and Budget. 4 August 1986. OMB Circular No. A-
123, Revised. Internal Control Systems. Washington, D.C.: U.S. Government Printing Service.

[30] OMB A-127 - Office of Management and Budget. 19 December 1984. OMB Circular No. A-127. Financial Management Systems. Washington, D.C.: U.S. Government Printing Service.

[31] OMB A-130 - Office of Management and Budget. 12 December 1985. OMB Circular No. A-130. Management of Federal Information, in the Federal Register, Vol. 50, No. 247. Washington D.C.: U.S. Government Printing Office.

[32] PA 1974 - U.S. Congress. Senate. Privacy Act of 1974. Public Law 92-579. S. 3418. Washington, D.C.: U.S. Government Printing Service.

[33] PRA 1980 - U.S. Congress. House. Paperwork Reduction Act of 1980. Public Law 96-511. December 11, 1980. H. R. 6410. Washington, D.C.: U.S. Government Printing Service.

[34] Russell 1991 - Russell, Deborah and G. T. Gangemi Sr. 1991. Computer Security Basics. Sebastopol, CA: O'Reilly & Associates, Inc.

[35] TCSEC 1985 - Department of Defense. 1985. DoD Trusted Computer System Evaluation Criteria. DoD Standard 5200.28-STD. Washington, D.C.: U.S. Government Printing Office.

ACRONYMS

ADP Automated Data Processing

ADT Abstract Data Type

AIS Automated Information System

DAA Designated Approval Authority

DAC Discretionary Access Control

DBMS Data Base Management System

DEC Discretionary Execution Control

DoD Department of Defense

EFT Electronic Funds Transfer

EPL Evaluated Products List

FIPS Federal Information Processing Standard

FMS Financial Management System

GAO General Accounting Office

IC Internal Control

IDA Institute for Defense Analyses

IG Inspector General

IMC Internal Management Control

IRM Information Retrieval Management (Program)

IVP Integrity Verification Procedure

MCP Management Control Plan

MEC Mandatory Execution Control

OMB Office of Management of Budget

NCSC National Computer Security Center

NIST National Institute of Standards and Technology

NSA National Security Agency

TCSEC Trusted Computer System Evaluation Criteria

TP Transformation Procedure

USC United States Code

APPENDIX A

A. SOURCE TEXT AND CROSS-REFERENCES

This Appendix contains a subsection for each policy document used in our formulation

of integrity-related control objectives. Each subsection is arranged in identical fashion. First, a brief overview of the policy document is provided. This overview concentrates on the AIS-integrity relevant aspects of the document rather than providing a comprehensive summary. The overview is followed by a listing of ``Selected Source Text'' (i.e., material quoted directly from the original document). Following the Selected Source Text is a ``Cross-Reference'' section. The Cross-Reference section contains a table indicating which statements from the Selected Source Text have affected our formulation of (proposed) changes to the current TCSEC control objectives. In the table, statement numbers from the Selected Source Text material are cross-referenced to each current control objective by marking an ``X'' in the appropriate row-column intersection. Each row is associated with a single section or statement from the Selected Source Text while each column is associated with a single control objective.

The meaning associated for each ``X'' in the table (indicating a cross-reference) is that the associated statement from the Source Text either (a) has implications for modifying the original control objective, or (b) has implications for interpreting the proposed control objective. Specific implications considered include the following:

· a new topic;

· a new viewpoint;

· suggests specific mechanisms, policies, or controls;

· demands interpretation;

· demands modification; and

· touches, influences, or constrains control.

Following the table is a list of comments (one for each ``X'' in the table) which provides details for the implications of particular policy statements upon each control objective. These comments represent notes made in analyzing the policy documents, and in determining the adequacy of the original control objectives in light of the increased scope of AIS security policy. The comments in this section are ``informal'' in the sense that they were not written to stand independently, outside the context of the included source text and related comments. In general, the comments do not attempt to address each issue comprehensively, and some issues may not receive equal treatment in different comments.

Some entries cross-referenced under the Security Policy heading are not further specified under MAC, DAC, or Marking headings. These additional headings are left blank whenever the security policy implications might be considered organization or application specific and do not clearly indicate specific MAC, DAC, or Marking ramifications, or particular technical implementations.

We have found that the topic of accountability should be generalized from its current focus on ``user accountability'' as stated in the existing control objective. From the policy documents we have studied, an expansion of the concept of accountability to include user, organization, and general accountability concepts with respect to both applications

and systems would be useful. Our comments under specific Accountability cross-references indicate such an expanded approach. Such an approach represents the concept of a ``total sense'' of accountability (i.e., its most general meaning). As such, some accountability features may in fact be external to a system. The exact placement and nature of mechanisms is neither predetermined nor explicitly considered in our comments.

In addition, we have assumed a similar generalization in addressing the topic of assurance. In particular, we have found policy statements which address assurance (i.e., the ``trustedness'') of controls extending to (a) entities external to the traditional bounds of AISs, and/or (b) to areas outside the traditional scope of protection mechanisms (e.g., application sub-systems).

Some material provided in the ``Selected Source Text'' does not have a cross-reference. Such material was included if it provided valuable background, context, or general information which might aid in understanding either the source text itself or related comments. Additionally, in some instances the selected source text is formatted and/or numbered slightly differently from the original; this was intended to clarify the presentation of this material-care was taken not to misrepresent the intent or meaning of the original material.

A.1 Privacy Act of 1974-Public Law 93-579

Public Law 93-579 requires the U.S. government to safeguard personal data processed by federal agency computer systems. This Act also requires the government to provide ways for individuals to find out what personal information is being recorded and to correct inaccurate information. The Act spells out physical security procedures, information management practices, and computer and network controls. This act also mandated the creation of the Privacy Protection Study Commission [Russell 1991, p. 287].

This Act extends the responsibility for management and protection of information resources to the area of privacy. The Act notes that the increasing use of computer and information technology has greatly magnified the potential harm to individuals that can occur from any collection, maintenance, use, or dissemination of personal information. The Act requires the Federal agencies to issue appropriate administrative orders, provide personnel sanctions, and establish appropriate technical and physical safeguards to ensure the security of the information system and the confidentiality of the data. The Act further requires that the information is as timely, complete, accurate, and relevant to its intended use as possible, and that ``adequate safeguards'' to prevent misuse are provided. Also required are administrative actions to keep account of the employees, other individuals and organizations having access to the system or file, and the disclosures and uses made of the information.

The Act requires that Federal agencies establish rules of conduct with regard to the ethical and legal obligations in developing and operating a computerized data system and in handling personal data, and take action to instruct all employees of such obligations. As ``privacy'' is used in the Act, information management responsibility includes the proper collection, maintenance, use, and dissemination of any information

which can be associated with a particular individual. The Act specifies that punitive actions can be levied against the Government for failure to uphold these responsibilities. We conclude that other factors which must be considered include (1) the moral obligation of government officials to maintain the constitutional rights of its citizens, (2) the adverse affect on government functioning in the absence of accurate information, and (3) the penalties associated with adverse public opinion which are likely to result from any breach of privacy as defined in the Act.

The following table contains selected sections of Public Law 93-579. The cross-reference table and comments appear in the next section.

TABLE A-2. Privacy Act of 1974-Selected Source Text

Sec. 2(a) The Congress finds that-

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Sec. 2(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to-

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the

information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

A.1.1 Cross-References and Comments

TABLE A-3. Privacy Act of 1974-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

Sec.2(b)(1)

X

X

Sec.2(b)(2)

X

X

Sec.2(b)(3)

X

X

X

Sec.2(b)(4)

X

X

X

X

X

X

Sec.2(b)(5)

X

X

Sec.2(b)(6)

X

Sec.2(b)(1)

[Security Policy] The type(s) of information about a particular individual, represented as records which are stored and processed by an agency, must be releasable to that individual. [Accountability] An agency is accountable for the accurate and timely response to individuals requesting the types of privacy information collected, maintained, used, or disseminated by that agency.

Sec.2(b)(2)

[Security Policy] The capability for an individual to restrict subsequent, additional uses of personal information which was collected for a particular use is implied. [Accountability] An appropriate history of the actual uses of personal information must be maintained.

Sec.2(b)(3)

[Security Policy] Individuals have to right to obtain copies of personal information held by an agency. A process to correct or amend personal information must exist. [Accountability] All corrections and amendments of individual records should be auditable. [Assurance] Appropriate controls on the correction and amendments process should exist. These controls should include the validation of source data used in modifying a record.

Sec.2(b)(4)

[Security Policy] Safeguards must exist to prevent misuse of information. Federal agencies are constrained to necessary and lawful purposes in collecting, maintaining, using, or disseminating personal information. In addition to disclosure, privacy concerns include the acquisition, storage, and manipulation of information relating to individuals. [MAC, DAC] Collection, maintenance, use, and dissemination of personal information are subject to mandatory controls. [Marking] Information associated with a particular in-

dividual must be appropriately marked. [Accountability] The actual use of information must be audited whenever such use does not comply with standing policies. [Assurance] Information must be current and accurate with respect to its intended use.

Sec.2(b)(5)

[Security Policy] The capability to permit exemptions via override of normal controls is required. Such exemptions may remain subject to other mandatory controls. For instance, certain records about individuals held by the Internal Revenue Service may not, under normal operating procedures, be accessed by the Federal Bureau of Investigation (FBI); these records may become releasable to the FBI during the course of an investigation, but only after a valid warrant has been issued. [Accountability] Exemptions to normal operating policies may require auditing. The exemption categories listed by this Act may each have unique auditing requirements.

Sec.2(b)(6)

[Accountability] An agency is held accountable for all its uses of personal information. Individuals having administrative control over personal information must be held accountable for their actions with respect to uses of that information.

A.2 Computer Matching and Privacy Protection Amendments of 1990-
Public Law 101-508

Public Law 101-508 provides protection against privacy violations due to information matching policies of the Federal government [Russell 1991, p. 288]. This Act amends 5 USC 552a, the codified version of the Privacy Act of 1974. It sets forth requirements for the independent verification of information about individuals produced by ``matching programs,'' i.e., through automated techniques. The Act requires that such information be verified before any adverse action-such as the denial of payment under a Federal benefit program-is carried out. The essence of this law with respect to integrity-related control objectives is to impose procedural controls on the modification of data. Also specified in this Act are the notification requirements of an agency to an individual who is subject to adverse action.

The following table contains selected sections of Public Law 101-508. The cross-reference table and comments appear in the next section.

TABLE A-4. Computer Matching and Privacy Protection Amendments of 1990-Selected Source Text

Sec. 7201. Computer Matching of Federal Benefits Information and Privacy Protection.

(b) Verification Requirements Amendment.-- (1) Subsection (p) of section 552a of title 5, United States Code, is amended to read as follows:

(p) Verification and Opportunity to Contest Findings.--

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment un-

der a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until--

(A) (i) the agency has independently verified the information; or (ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that-- (I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and (II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C) (i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or...

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of--

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

A.2.1 Cross-References and Comments

TABLE A-5. Computer Matching and Privacy Protection Amendments of 1990-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

(p)(1)

X

(p)(1)(A)

X

(p)(1)(B-C)

X

X

(p)(2)(A-C)

X

(p)(3)

X

(p)(1)

[Security Policy] One may not directly modify data based on the results of automated ``matching programs." Procedural controls and control information are required to verify information which forms the basis of an adverse action throughout the process of carrying out the adverse action against an individual. May apply to application-specific security policies, with some applications having unique requirements.

(p)(1)(A)

[Assurance] The information which forms the basis of an adverse action must either (i) be independently verified or (ii) be limited in scope, with a high degree of confidence in its accuracy.

(p)(1)(B-C)

[Marking] The capability to enable or disable transactions conferring benefits is implied. Transaction of adverse action requires marking to indicate expiration of a grace period and/or an individual's possible response (i.e., a pending challenge to decision). Transaction of adverse action requires marking that individual has received notice. [Accountability] Procedural controls must exist to ensure that no adverse action proceeds without first meeting verification and/or control information requirements. The system must be

able to record and collate appropriate historical information related to benefits transactions. The system must keep account of the initiation, length, and expiration of the grace period.

(p)(2)(A-C)

[Assurance] Independent verification requires investigation and confirmation of specific information which forms the basis of an adverse action.

(p)(3)

[Security Policy] Stated requirements are subject to exemption when considering additional policies (i.e., public health and public safety policies).

A.3 Paperwork Reduction Act of 1980-Public Law 96-511

Public Law 96-511 promotes the use of efficient office systems (e.g., electronic mail, document storage, and electronic imaging systems) under the management of OMB [Russell 1991, p. 279]. This Act simultaneously encourages the automation of information services and adds responsibilities for the use of automation. Under this Act, automation must be used to improve both services provided by, and management of, Federal Agencies. Additionally, such automation must be cost effective (maximizing usefulness of information while minimizing costs to collect, maintain, use, and disseminate information) and supportive of ``uniform'' Federal information policies.

The following table contains selected sections of Public Law 96-511. The cross-reference table and comments appear in the next section.

TABLE A-6. Paperwork Reduction Act of 1980-Selected Source Text

Sec.2.(a) Chapter 35 of title 44, United States Code, is amended to read as follows:

3501. Purpose The purpose of this chapter is-

(1) to minimize the Federal paperwork burden for individuals, small business, State and local governments, and other persons;

(2) to minimize the cost to the Federal Government of collecting, maintaining, using, and disseminating information;

(3) to maximize the usefulness of information collected by the Federal Government;

(4) to coordinate, integrate and, to the extent practicable and appropriate, make uniform Federal information policies and practices;

(5) to ensure that automatic data processing and telecommunications technologies are acquired and used by the Federal Government in a manner which improves service delivery and program management, increases productivity, reduces waste and fraud, and, wherever practicable and appropriate, reduces the information processing burden for the Federal Government and for persons who provide infor-

mation to the Federal Government; and

(6) to ensure that the collection, maintenance, use and dissemination of information by the Federal Government is consistent with applicable laws relating to confidentiality, including section 552a of title 5, United States Code, known as the Privacy Act.

3506. Federal agency responsibilities

(a) Each agency shall be responsible for carrying out its information management activities in an efficient, effective, and economical manner, and for complying with the information policies, principles, standards, and guidelines prescribed by the Director.

A.3.1 Cross-References and Comments

TABLE A-7. Paperwork Reduction Act of 1980-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

3501(4)

X

3506(a)

X

X

3501(4)

[Security Policy] The essence of this law affects Security Policy in that its purpose is to coordinate, integrate, and make uniform Federal information policies and practices. One integration framework might include the information life cycle (e.g., origin or acquisition through final disposition). Factors to consider include cost effectiveness and risk reduction relating to information processing activities. Cost effectiveness is a function of the cost of controls versus the degree of acceptable risk.

3506(a)

[Security Policy] Information management must be efficient, effective, and economical. Minimizing the paperwork burden and associated costs of collecting, maintain, using, and disseminating information are required. Automated systems are required to improve service delivery, program management, productivity, and to reduce waste, fraud, and information processing burden. Confidentiality policies must also be enforced. Information which is not useful should not be collected. Maximizing the usefulness of collected information is required. Information that is no longer useful should not be maintained. Systems are required to enforce integrated policies. This implies a significant effort must be undertaken to address the overall system security policy, and in particular the issue where different component policies might produce conflicts. [Accountability] Compliance with multiple policies, standards, and guidelines is required.

A.4 Department of Defense Authorization Act of 1982-Public Law 97-86

The Warner Amendment to Public Law 97-86 exempts certain types of DoD procurements from the Automatic Data Processing Equipment Act (Public Law 89-306, also know as the Brooks Act). The exempted procurements includes those in which the function, operation, or use of a particular piece of equipment or a service involves one or more categories related to national security or military interests [Russell 1991, p. 280].

The following table contains selected sections of Public Law 97-86. The cross-reference table and comments appear in the next section.

TABLE A-8. DoD Authorization Act of 1982-Selected Source Text

Sec. 908.(a)(1) Chapter 137 of title 10, United States Code, is amended by adding at the end thereof the following new section:

2315. Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes

(a) Section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 795) is not applicable to the procurement by the Department of Defense of automatic data processing equipment or services if the function, operation, or use of the equipment or services-

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves the command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system; or

(5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions.

(b) Subsection (a)(5) does not include procurement of automatic data processing equip-

ment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)...

A.4.1 Cross-References and Comments

TABLE A-9. DoD Authorization Act of 1982-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

2315(a)(1-5)

X

2315(b)

X

2315(a)(1-5)

[Security Policy] This Act excludes certain systems, during acquisition, from the application of specific aspects of Federal law. The exclusions named in this Act, relating to the procurement of automatic data processing (ADP) equipment or services, extend to most of all the other Acts applying to Federal systems. Most of these exclusion categories relate to systems requiring secrecy and integrity protection. Simply having authorization to be exempt does not make it a good practice to avoid a thorough analysis of a system's protection needs. Each acquisition should address its protection needs through the formulation and analysis of a systems security policy that will enable a more informed decision regarding invocation of this Act.

2315(b)

[Security Policy] Explicitly precludes from ``mission critical'' exemption many DoD auto mated systems relating to routine administrative and business applications. Therefore, many systems used within the DoD are subject to Federal laws.

A.5 Federal Managers' Financial Integrity Act of 1982-Public Law 97-255

This Act extends security policies into the realm of internal controls. Systems of internal control are of interest when considering integrity in AISs because (a) primary

applications, which are the focus of traditional internal controls, are being automated to greater degrees, and (b) internal control systems themselves are being automated to greater degrees. Internal controls are usually associated with assets having ``value.'' Information within Federal AISs is readily termed a valuable asset according to [OMB A-130]. This Act requires adherence to the Comptroller General's (GAO) Standards for Internal Control in the Federal Government [GAO 1983], which are incorporated into [GAO Title 2, App.II].

The following table contains selected sections of Public Law 97-255. The cross-reference table and comments appear in the next section.

TABLE A-10. Federal Managers' Financial Integrity Act of 1982-Selected Source Text

Sec. 2. Section 113 of the Accounting and Auditing Act of 1950 (31 U.S.C. 66a) is amended by adding at the end thereof the following new subsection:

(d)(1)(A) To ensure compliance with the requirements of subsection (a)(3) of this section, internal accounting and administrative controls of each executive agency shall be established in accordance with standards prescribed by the Comptroller General, and shall provide reasonable assurance that-

(i) obligations and costs are in compliance with applicable law;

(ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and

(iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

(B) The standards prescribed by the Comptroller General under this paragraph shall include standards to ensure the prompt resolution of all audit findings....

(3)... the head of each executive agency shall... prepare a statement-

(A) that the agency's systems of internal accounting and administrative control fully comply with the requirements of paragraph (1); or

(B) that such systems do not fully comply with such requirements.

(5) The statements and reports required by this subsection... shall also be made available to the public, except that, in the case of any such statement or report containing information which is-

(A) specifically prohibited from disclosure by any provision of law; or

(B) specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs, such information shall be deleted prior to the report or statement being made available to the public.

A.5.1 Cross-References and Comments

TABLE A-11. Federal Managers' Financial Integrity Act of 1982-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

(d)(1)(A)(i-iii)

X

X

X

X

X

X

(d)(1)(B)

X

(d)(3)

X

(d)(5)

X

X

X

X

X

(d)(1)(A)(i-iii)

[Security Policy] Legal compliance related to organizational obligations and costs (e.g., contracts, logistics, funds transfer, services, etc.) must be considered in the formulation of Security Policy. Security policy must address waste, loss, unauthorized use, and mis-appropriation in terms of both AIS assets as well as other assets, whenever these non-AIS assets are either represented within or controlled via AISs. [MAC, DAC, Marking] Because the control of ``unauthorized use'' is explicitly called for, authorization features are required. [Accountability] Costs and obligations must be internally accounted for within an organization to the level of a responsible individual acting within the scope of his authority. [Assurance] Reasonable assurance is required.

(d)(1)(B)

[Accountability] Prompt resolution of audit findings requires specific features for AIS systems. These may include audit reduction tools, real-time alerts, etc.

(d)(3)

[Assurance] The head of each executive agency is required to produce a report on the state of that agency's internal control system.

(d)(5)

[Security Policy] Mandated disclosure of information is also subject to restrictions of national security and other (confidentiality) policies. [MAC, DAC, Marking] The overlapping of confidentiality and integrity policy coverage has implications for MAC policy with regard to information sanitation and downgrading of classified or sensitive information. There are also implications for DAC policy with regard to the designated individuals performing these types of operations. [Accountability] Auditing of all downgrading and sanitation activity shall be performed.

A.6 Computer Security Act of 1987-Public Law 100-235

Public Law 100-235 expands the definition of computer security protection and clarifies the role of the (NBS now the National Institute of Standards and Technology) [Russell 1991, p. 283]. A primary function of this Act is to prescribe authority and assign responsibilities for developing security standards and guidelines for Federal computer systems. This Act has broadens the scope of applicability for security policies in three areas: the range of resources, the type(s) of information, and the types of systems.

Significantly, this Act also increases types of computers under consideration as well as the scope of information which must be protected. The Act defines computer systems broadly and includes support services as an area which must be considered. This can be interpreted to mean that effective controls must exist over AIS support systems and personnel, as well as those individuals who operate the primary applications. The traditional scope of information protection was increased as well. Previously, explicit protection policy applied only to ``classified'' and ``specifically categorized sensitive'' information. This Act applies to a more encompassing term, ``sensitive information,'' which is defined in detail below.

The following table contains selected sections of Public Law 100-235. The cross-reference table and comments appear in the next section.

TABLE A-12. Computer Security Act of 1987-Selected Source Text

Sec.2. Purpose.

(a) In General.-The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) Specific Purposes.-The purposes of this Act are-

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

Sec.3. Establishment of Computer Standards Program.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended-

(2)... by inserting... ``Sec.20''

(d) As used in this section-

(1) the term ``computer system''-

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes-

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(iv) related resources as defined by regulations issued by the Administrator for General Services . . .

(4) the term `sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled . . . , but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy;

Legislative History [The Legislative History of the Computer Security Act of 1987 [H. Rept. 100-153(I), p. 24] gives examples of that which should be considered ``sensitive information:''

. . . information which if modified, destroyed or disclosed in an unauthorized manner could cause:

Loss of life;

Loss of property or funds by unlawful means;

Violation of personal privacy or civil rights;

Gaining of an unfair commercial advantage;

Loss of advanced technology, useful to a competitor; or

Disclosure of proprietary information entrusted to the government.]

Sec.5. Amendment to Brooks Act.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the [National Institute of Standards and Technology] . . . promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. . . .

(d)(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(d)(4) The Administrator shall revise the Federal information resources manage-

ment regulations . . . to be consistent with the standards and guidelines promulgated by the Secretary of Commerce.

Sec.6. Additional Responsibilities for Computer Systems Security and Privacy.

(a) Identification of Systems That Contain Sensitive Information.- . . . each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) Security Plan.- . . . each agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. . . .

A.6.1 Cross-References and Comments

TABLE A-13. Computer Security Act of 1987-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

Sec.3(2)(d)(1)

X

Sec.3(2)(d)(4)

X

X

X

X

Sec.3(Leg.His.)

X

X

X

Sec.5(d)(1,2,4)

X

Sec.6(a-b)

X

Sec.3(2)(d)(1)

[Security Policy] This Act applies to ``computer systems,'' a range of resources including equipment, software, services, and related resources. This implies an increased scope of system Security Policies with regard to the range of applicable resources.

Sec.3(2)(d)(4)

[Security Policy] By defining the type of applicable information, this Act explicitly increases the scope of the Security Policy-in particular, the systems containing ``sensitive information'' must provide protection for that information. [MAC, DAC, Marking] Because the control of ``unauthorized use'' is explicitly called for, authorization features are required.

Sec.3(Leg.His.)

[Security Policy, Assurance, Fault Tolerance] The considerations for ``loss of life'' greatly increases the scope of systems which are applicable under this Act. The inclusion of computer systems which control machinery or processes also has important implications for the scope of the Security Policy. In particular, the inclusion of safety-critical systems is implied, although there is currently a lack of explicit policy statements in this area.

Sec.5(d)(1,2,4)

[Security Policy] The Act contains details relevant to the formulation of individual (agency) Security Policies. These show that the agencies involved might have to prescribe and integrate different security policies and standards to meet their unique needs.

Sec.6(a-b)

[Security Policy] All systems identified as containing sensitive information are subject to Security Policy requirements. An organization (agency) must develop individual security plans for computer systems containing ``sensitive information.'' These plans may provide greater insight into Security Policy needs.

A.7 OMB Circular No. A-127-Financial Management Systems

OMB Circular No. A-127 establishes a program to assure the integrity of Federal financial management systems (FMSs) by prescribing policies and procedures for executive departments and agencies. Financial management systems are of interest primarily because the control of revenue, expenditure, funds, property, and other assets are often-either partially or totally-implemented via AISs. Therefore, policy related to FMSs must be effectively enforced on these related AISs.

There are five particular control areas for FMSs called for under this Circular [OMB A-127, p. 4]: FMS operations, FMS integrity, support for budgets, support for management, and full financial disclosure. Each of these areas has specific implications for integrity when considering (possible) automated features of an FMS.

The most demanding and significant implications for AIS integrity fall under the area of FMS operations. Specific objectives for FMS operations address the areas of usefulness, timeliness, reliability and completeness, comparability and consistency, and efficiency and economy. The use of automated systems to help achieve these objectives is explicitly called for [OMB A-127, p. 4].

Any particular executive department or agency may have unique requirements for one or more of the preceding control areas or FMS control objectives. The importance of this Circular is not in calling out specific, detailed requirements, but in recognizing specific areas in which controls must exist to enforce financial management policies. These areas must be addressed by AIS integrity policies on automated implementations of FMSs. This Circular has implications for both system and application-oriented security policies.

The following table contains selected sections of OMB Circular No. A-127. The cross-reference table and comments appear in the next section.

TABLE A-14. OMB Circular No. A-127-Selected Source Text

1. Purpose. This Circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems.

2. Background. The Budget and Accounting Procedures Act of 1950, the Federal Managers' Financial Integrity Act, and related legislation . . . provide that:

-- Establishing and maintaining systems of accounting and reporting is the responsibility of the executive branch.

-- Agency systems shall provide for:

· complete disclosure of the financial results of the activities of the agency,

· adequate financial information for agency management and for formulation and execution of the budget,

· effective control over revenue, expenditure, funds, property, and other assets.

3. Policy. The financial management system of each agency shall meet the objectives set

forth in Section 6 of this Circular. These objectives are intended to establish a framework for complying with applicable law, appropriate budget and accounting principles and standards, Treasury reporting requirements, and the best contemporary financial practice. Systems developed and operated under this Circular shall be the source for financial information used in the budget, Treasury financial statements, financial reports to the Congress, and other financial reports.

Agencies shall establish and maintain a single, integrated financial management system, which may be supplemented by subsidiary systems. Data needed in this system and other agency systems shall be entered only once and transferred automatically to appropriate accounts or other parts of the system or systems. New or substantially revised systems shall be developed on an inter-agency basis and designed to meet the needs of all participating agencies. Funds shall be expended only for systems that meet the requirements of this Circular.

6. Financial Management System Objectives. The following objectives shall be met by the agency financial management system in complying with applicable law and appropriate guidance of GAO, Treasury, and OMB. . . .

a. Systems operations -- the agency financial management system shall use the best of acceptably priced, contemporary technology -- including automated data entry and edit, data management, data base dictionaries, electronic communications between systems, flexible report formats, and controlled access to data bases by personal computers and other means -- to achieve the following objectives.

(1) Usefulness -- financial management data shall be gathered and processed only where necessary to meet specific internal management needs or external requirements. Reports shall be tailored to specific user needs and if report usages does not justify cost, reports shall be terminated. Usefulness shall be determined in part through consultation with users as part of the reviews required by Section 7b of this Circular. (2) Timeliness -- financial management data shall be recorded as soon as practicable after the occurrence of the event, and relevant preliminary data shall be made available to managers by the fifth working day following the end of the reporting period. Other standards of timeliness may be established where the agency has inventoried reports and set specific standards, with user participation. Final, corrected data shall be available in time to meet external reporting requirements.

(3) Reliability and completeness -- financial management information shall be reasonably complete and accurate, shall be verifiable and ordinarily be drawn from the official records and systems, and shall be no more detailed than necessary to meet the needs of management and external requirements.

(4) Comparability and consistency -- financial management data shall be recorded and reported in the same manner throughout the agency, using uniform definitions. Accounting shall be synchronized with budgeting. Consistency over time shall be maintained. New and revised systems shall adopt common, existing definitions and classifications.

(5) Efficiency and economy -- the agency financial management system shall be designed and operated with reasonable total costs and transaction costs, in accordance with OMB guidelines. Financial systems which are excessively costly shall be identified and phased out. This shall be accomplished through installation of effective systems of planning and evaluation, sharing of data, elimination of overlap and duplication, and use of the best contemporary technology, including commercially available packages with proven success in other agencies or the private sector.

b. Systems integrity -- the agency financial management system shall feature reasonable controls designed, operated, and evaluated in accordance with OMB Circular A-123, Internal Control Systems, and A-71 [rescinded by A-130], Responsibilities for the Administration and Management of Automatic Data Processing Facilities.

c. Support for budgets -- financial management data shall be recorded, stored, and reported to facilitate budget preparation, analysis, and execution. Data shall be classified uniformly and that classification, at a minimum, shall be at a level of detail that directly supports execution of enacted budgets and formulation of proposed budgets, without excessive aggregation or disaggregation. . . .

d. Support for management -- data shall be recorded and reported in a manner to facilitate carrying out the responsibilities of both program and administrative managers. The agency financial management system shall provide for a coherent, timely, and accurate financial management data base. It should be supplemented as necessary to meet agency management and Executive Office requirements for administrative data, such as the Financial and Administrative Management Information System 1. . . .

e. Full financial disclosure -- financial management data shall be recorded, and reported as specifically required by OMB or Treasury, to provide for full financial disclosure and accountability in accordance with appropriate budget and accounting principles and standards. . . .

A.7.1 Cross-References and Comments

TABLE A-15. OMB Circular No. A-127-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

3

X

X

X

X

6(a)

X

X

X

X

X

X

6(a)(1)

X

X

6(a)(2)

X

X

X

6(a)(3)

X

X

X

6(a)(4)

X

6(a)(5)

X

X

6(b)

X

X

6(c)

X

6(d)

X

X

X

6(e)

X

X

X

3

[Security Policy, Accountability] AIS portions of financial management systems must comply with applicable law, budget and accounting principles and standards, Treasury reporting requirements, and the best contemporary financial practice. A specific administrative policy is cited in regard to data handling and security controls. [Assurance, Fault Tolerance] The single point-of-entry requirement for input of data to the system, specifying automatic transfer of data to required locations, implies rigorous administrative and reliability features.

6(a)

[Security Policy] The use of AISs to implement financial management systems is explicitly called for. Controlled access to data bases is required. [MAC, DAC, Marking] Providing controlled access implies that these control objectives will be affected. [Accountability] This is implied when access control is required. [Assurance] Particular automated features called for implies the need for assurance measures with rigor defined by acceptable risk and reasonable cost as well as the need for a thorough risk analysis.

6(a)(1)

[Security Policy] Financial management data shall be gathered and processed only where necessary to meet specific internal management needs or external requirements. [Accountability] Reports are tailored to specific user needs.

6(a)(2)

[Security Policy, Accountability] Financial management data shall be recorded as soon as possible and made available in a timely manner. Specific standards of timeliness may be established. This implies the need for internal timing attributes and control policies related to timing. [Assurance] Corrected data shall be available in time to meet external reporting requirements.

6(a)(3)

[Security Policy] Financial management information shall be reasonably complete and accurate. This implies specifications for completeness and accuracy that can be monitored and reacted to when the specified attributes or attribute values do not meet specified thresholds. [Accountability] Further, it implies identified responsibility for all actions taken on the specified information. Accountability is also implied by the verification requirement. [Assurance] That information should be verifiable implies reconciling transactions with starting and ending totals, dual-entry accounting, or external ``safety paper'' (e.g., checks, withdrawal slips, and/or deposit slips).

6(a)(4)

[Security Policy] Uniform system definitions (process and data) for related systems are required. Consistency of financial management data over time is required. Synchronized functions (e.g., accounting and budgeting) are required.

6(a)(5)

[Security Policy, Assurance] Operational costs must be reasonable and in accordance with OMB guidelines. Effective planning and evaluation, sharing of data, elimination of duplication, and the use of the best contemporary technology is required. This implies that a thorough risk analysis must be performed to ascertain protection requirements.

6(b)

[Security Policy, Assurance] AIS portions of financial management systems must feature reasonable controls designed, operated, and evaluated in accordance with OMB policy. Again, the implication for a thorough risk analysis for protection controls is established by the use of the term ``reasonable.''

6(c)

[Security Policy] Uniform system of data categorization is required. The budget process shall be supported. Excessive aggregation or disaggregation is not acceptable. This is an application-specific security policy issue.

6(d)

[Security Policy, Accountability, Assurance] Data shall be recorded and reported in a manner to facilitate carrying out the responsibilities of managers. The financial management system shall be coherent, timely, and accurate.

6(e)

[Security Policy, Accountability] Financial management data shall be recorded. Reports shall provide full financial disclosure and accountability in accordance with appropriate budget and accounting principles and standards. [Assurance] Accuracy and completeness of data being disclosed has implications for assurance.

A.8 OMB Circular No. A-130-Management of Federal Information Resources

OMB Circular No. A-130 establishes requirements for effective and efficient management of federal information resources. This Circular requires all agency information systems to provide a level of security commensurate with the sensitivity of the information, the risk of its unauthorized access, and the harm that could result from improper access. It also requires all agencies to establish security programs to safeguard the sensitive information that they process [Russell 1991, p. 282]. As such, it sets forth policy regarding information management within Federal agencies that bear directly on the protection issues of confidentiality, integrity, and availability. That these issues are intended to be within the scope of this Circular is explicitly stated in Appendix IV [p. 52749]:

Security of information systems means both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more. Information system security entails management controls to ensure the integrity of operations including such matters as proper access to the information in the systems and proper handling of input and output. In this sense, security of information is first and foremost a management issue and only secondly a technical problem of computer security. . . . Protecting personal, proprietary, and other sensitive data from unauthorized access or misuse; detecting and preventing computer related fraud and abuse; and assuring continuity of operations of major information systems in the event of emergency related disruptions are increasingly serious policy issues. . . .

The Paperwork Reduction Act of 1980 establishes a broad mandate for efficient, effective, and economical performance of information activities by agencies. Circular No. A-130 implements OMB authority under the 1980 Act with respect to general information policy, records management, privacy, and Federal automatic data processing and telecommunications. In addition, it also implements sections of the Privacy Act of 1974 as well as other Federal Laws and Executive policy statements.

Circular No. A-130 revises and consolidates policy and procedures in five previous OMB directives, which were rescinded through this Circular. One reason for issuing this Circular was OMB's determination that it was important to distinguish the statement of policies from the procedures for implementing those policies. As a result, the main body of the Circular is a statement of basic considerations and assumptions, policies, and responsibility assignments. Appendices I, II, and III to the Circular consist of procedures

for implementing various policies. These Appendices have the same prescriptive force as the Circular itself, and hence, were included in the extraction of Selected Source Text, below. Appendix IV to the Circular is an explanatory document, and was used in our analysis of the Source Text.

Appendix III of this Circular, together with OMB Circular No. A-123 (Internal Control Systems), provide the evaluation and reporting requirements for the systems integrity objective contained in OMB Circular No. A-127 (Financial Management Systems).

Due to a similar treatment of the subject, this Circular [App.III, Sec.(2)(c)] appears to be the source of the definition of ``sensitive information'' used in The Computer Security Act of 1987. Significantly, the Circular [App.III, manner which has particular significance for policy related to safety-critical systems.

This Circular is undergoing revision with a version available for public comment expected in the near future. Although the exact changes to be incorporated in revision have not been determined, the available information indicates that the major focus of change will be on policy regarding public access to agency information holdings and the dissemination of electronic information products to Federal depository libraries. Also incorporated will be changes called for by legislation passed since the 1985 publication of this Circular. OMB plans call for work on the revised Circular to continue through 1992 [OMB 1991, p. 9026].

The following table contains selected sections of OMB Circular No. A-130. The cross-reference table and comments appear in the next section.

TABLE A-16. OMB Circular No. A-130-Selected Source Text

7. Basic Considerations and Assumptions:

b. Government information is a valuable national resource. It provides citizens with knowledge of their government, society, and economy-past, present, and future; is a means to ensure the accountability of government; is vital to the healthy performance of the economy; is an essential tool for managing the government's operations; and is itself a commodity often with economic value in the marketplace.

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

d. In order to minimize the cost and maximize the usefulness of government information activities, the expected public and private benefits derived from government information, insofar as they are calculable, should exceed the public and private costs of the information.

f. The use of up-to-date information technology offers opportunities to improve the management of government programs, and access to, and dissemination of, government information. . . .

8. Policies

a. Information Management. Agencies shall:

(1) Create or collect only that information necessary for the proper performance of agency functions and that has practical utility, and only after planning for its processing, transmission, dissemination, use, storage, and disposition; (2) Seek to satisfy new information needs through legally authorized inter-agency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(3) Limit the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions;

(4) Maintain and protect individually identifiable information and proprietary information in a manner that precludes:

(a) Unwarranted intrusion upon personal privacy (see Appendix I); and

(b) Violation of confidentiality;

(5) Provide individuals with access to, and the ability to amend errors in, systems of records, consistent with the Privacy Act;

(6) Provide public access to government information, consistent with the Freedom of Information Act.

(7) Ensure that agency personnel are trained to safeguard information resources.

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

(9) Disseminate such information products and services as are:

(a) Specifically required by law; or

(b) Necessary for the proper performance of agency functions, . . .

(10) Disseminate significant new, or terminate significant existing, information products and services only after providing adequate notice to the public;

(11) Disseminate such government information products and services:

(a) In a manner that ensures . . . the public . . . have a reasonable ability to acquire the information;

(b) In a manner most cost effective for the government, . . .

(c) So as to recover costs of disseminating the products or services . . .

(12) Establish procedures for:

(a) Reviewing periodically the continued need for and manner of dissemination of the agency's information products or services; and

(b) Ensuring that government publications are made available to depository libraries as required by law.

b. Information Systems and Information Technology Management. Agencies shall:

(1) Establish multi-year strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the bases for their budget requests;

(2) Establish systems of management control that document the requirements that each major information system is intended to serve; and provide for periodic review of those requirements over the life of the system . . .

(3) Make the official whose program an information system supports responsible and accountable for the products of that system;

(4) Meet information processing needs through inter-agency sharing and from commercial sources, when it is cost effective, before acquiring new information processing capacity;

(5) Share available information processing capacity with other agencies to the extent practicable and legally permissible;

(6) Acquire information technology in a competitive manner that minimizes total life cycle costs;

(7) Ensure that existing and planned major information systems do not unnecessarily duplicate information systems . . .

(8) Acquire off-the-shelf software . . . unless the cost effectiveness of developing custom software is clear and has been documented;

(9) Acquire or develop information systems in a manner that facilitates necessary compatibility;

(10) Assure that information systems operate effectively and accurately;

(11) Establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems (See Appendix III);

(12) Assure that only authorized personnel have access to information systems;

(13) Plan to provide information systems with reasonable continuity of support should their normal operations be disrupted in an emergency;

(14) Use Federal Information Processing and Telecommunications Standards except where it can be demonstrated that the costs of using a standard exceed the benefits or the standard will impede the agency in accomplishing its mission;

(15) Not require program managers to use specific information technology facilities or services unless it is clear and convincingly documented, subject to periodic review, that such use is the most cost effective method for meeting program requirements.

(16) Account for the full costs of operating information technology facilities and recover such costs from government users . . .

(17) Not prescribe Federal information system requirements that unduly restrict the prerogatives of heads of State and local government units;

(18) Seek opportunities to improve the operation of government programs or to realize savings for the government and the public through the application of up-to-date information technology to government information activities.

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

4. Reporting Requirements.

b. New and Altered System Reports. . . .

(1) Altered System of Records. . . . The following changes are those for which a report is required:

(b) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would require a report.

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

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

Supplemental Information.

Several commentators believed that requiring full costs to be recovered from all users within an agency would not be cost effective. OMB disagreed with this viewpoint and retained the draft Circular's formulation. Viable management of a large information technological facility requires that managers know the amount of resources devoted to each user when providing services. Furthermore, effective management of the use of information technology requires that the user have responsibility for and control over the resources consumed by use of the facility. . . .

Appendix III to OMB Circular No. A-130-Security of Federal

Automated Information Systems

1. Purpose. This Appendix establishes a minimum set of controls to be included in Federal automated information systems security programs; assigns responsibilities for the security of agency automated information systems; and clarifies the relationship between such agency security programs and internal control systems established in accordance with OMB Circular A-123, Internal Control Systems. The Appendix revises procedures formerly contained in Transmittal Memorandum No. 1 to OMB Circular No. A-71, now rescinded, and incorporates responsibilities from applicable national security directives.

2. Definitions.

c. The term ``sensitive data'' means data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

d. The term ``sensitive application'' means an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

3. Automated Information Systems Security Programs. Agencies

shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Specifically, agencies shall:

- Assure that automated information systems operate effectively and accurately;

- Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems; and

- Assure the continuity of operation of automated information systems that support critical agency functions.

Agencies shall implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. This program will be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Agency programs shall incorporate additional requirements for securing national security information in accordance with appropriate national security directives. Agency programs shall, at a minimum, include four primary elements: applications security, personnel security, information technology installation security, and security awareness and training.

a. Applications Security.

(1) Management Control Process and Sensitivity Evaluation. Agencies shall establish a management control process to assure that appropriate administra-

tive, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications. Management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified. For those applications considered sensitive, the management control process shall, at a minimum, include security specifications and design reviews and systems tests. . . .

(2) Periodic Review and Re-certification. . . . Audits or reviews shall evaluate the adequacy of implemented safeguards, assure they are functioning properly, identify vulnerabilities that could heighten threats to sensitive data or valuable resources, and assist with the implementation of new safeguards where required. . . .

A.8.1 Cross-References and Comments

TABLE A-17. OMB Circular No. A-130-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

8(a)(1)

X

X

X

8(a)(2)

X

X

X

X

X

8(a)(3)

X

8(a)(4)

X

8(a)(5)

X

X

X

8(a)(6)

X

8(a)(7)

X

X

8(a)(8-11)

X

8(a)(12)

X

X

8(b)(1)

X

8(b)(2)

X

8(b)(3)

X

8(b)(4-5)

X

8(b)(6)

X

8(b)(8)

X

X

8(b)(9)

X

8(b)(11)

X

X

8(b)(12)

X

X

X

X

X

X

8(b)(13)

X

X

X

8(b)(15)

X

X

App.I(4)

X

App.II(Sup.Info.)

X

X

App.III(2)(c)

X

X

X

X

X

App.III(2)(d)

X

X

X

X

X

App.III(3)

X

App.III(3)(a)(1-2)

X

8(a)(1)

[Security Policy] Each phase of the information life cycle (e.g., origin or acquisition through final disposition). should be considered in formulating the Security Policy. Only information necessary for proper performance of agency functions, and that has practical utility shall be created or collected. Practical utility includes characteristics ``pertaining to the quality of information such as accuracy, adequacy, and reliability.'' In the case of general purpose statistics or record keeping, practical utility means that ``actual uses can be demonstrated . . .'' [OMB A-130, p. 52746]. Execution authority is derived from the required, approved plans for the processing, transmission, dissemination, use, storage, and disposition of necessary information. The delegation of authority and allocation of resource responsibilities shall be performed for each aspect of the information life cycle. [Accountability] This implies that individuals should be held accountable to performing within the scope of their authority. [Assurance] The documentation of required planning may be used as an assurance measure.

8(a)(2)

[Security Policy] This implies that the Security Policy must address the protection of shared information. Sharing should be done under the concept of ``due care'' (i.e., protection commensurate with the risk and magnitude of loss). [MAC, DAC, Marking] The establishment of information sharing agreements must include confirmation that the receiving Agency can mark and protect the shared information as required by the providing Agency. If such protection is not possible, then the providing Agency must determine the need to desensitize the information to the degree commensurate with the maximum protection capabilities of the receiving Agency prior to actual sharing. [Accountability] The receiving Agency should be accountable for the protection of any shared information it receives. The providing Agency is accountable for the sharing of sensitive information for which the receiving Agency does not have the capabilities to protect.

8(a)(3)

[Security Policy] The collection of individually identifiable and proprietary information must be limited to that which is legally authorized and necessary for agency functions.

8(a)(4)

[Security Policy] Confidentiality requirements must be addressed in the Security Policy.

8(a)(5)

[Security Policy] Providing a process for individuals to gain access to personal information is required. [Accountability, Assurance] An amendment and error correcting process for private information must exist.

8(a)(6)

[Security Policy] Providing a process for public access may be required. This process shall be consistent with Freedom of Information Act requirements and exemptions.

8(a)(7)

[Accountability] This implies that individuals shall be held accountable for adhering to doctrine and procedures in which they have been trained. [Assurance] Security training and documentation in support of security training is required. Such documentation should cover the information life cycle processes, safeguards employed, and individual responsibilities.

8(a)(8-11)

[Security Policy] Dissemination of information on Agency information life cycle processes is required, as required under applicable laws or other relevant policies.

8(a)(12)

[Accountability] Procedures for periodic reviews of information life cycle processes are required. [Assurance] Assurance of compliance to laws for dissemination is required.

8(b)(1)

[Accountability] Technical protection of information as a part of program and mission needs must be planned for, taking into account budget constraints. The Paperwork Reduction Act requires that OMB: ``promote the use of the technology to improve governmental efficiency and effectiveness. . . .''

8(b)(2)

[Assurance] Information systems requirements documentation is necessary. Periodic reviews are required.

8(b)(3)

[Accountability] Overall information product accountability is user based. Specific accountability for information products is established at the supported program official.

8(b)(4-5)

[Security Policy] Requirements for the sharing of information are outlined. Specific Agency policies regarding information sharing should be established.

8(b)(6)

[Assurance] Total life cycle costs must be considered in protection technology acquisition. This should be coupled to the Agency risk assessment.

8(b)(8)

[Security Policy] The use (in terms of trustedness) of commercial, off-the-shelf software must be reflected in the Security Policy. [Assurance] ``Trustedness'' implies that process for evaluation of the vulnerabilities of commercial, off-the-shelf software should be established. The evaluated software must be placed under configuration management once it is accepted.

8(b)(9)

[Assurance] Necessary compatibility is considered because ``compatibility among information systems has . . . emerged as a significant information resources management problem . . .'' [OMB A-130, p. 52749]. Necessary compatibility for integrity protection is required.

8(b)(11)

[Security Policy, Assurance] Security features must be adequate for protection with regards to the sensitivity of the information and/or application as determined by the Agency risk assessment.

8(b)(12)

[Security Policy, MAC, DAC, Marking, Accountability, Assurance] Authorized access to information systems must be assured. This implies an extension of authorized access to specific information.

8(b)(13)

[Security Policy, Fault Tolerance] Reasonable continuity of support shall be provided for information systems. [Assurance] Contingencies should not only be planned for but also routinely exercised whenever practicable.

8(b)(15)

[Security Policy] This implies a thorough risk assessment has been conducted and that specific protection policy enforcement needs have been identified as being both required and cost effective. [Assurance] Periodic reviews are required.

App.I(4)

[Accountability] Changes to types or categories of information being maintained, or the purposes to which information is being put to use, must be reported.

App.II Sup.Info.

[Security Policy] A user has control over assigned resources. [Accountability] A manager must know the amount of resources consumed by each user. A user is responsible for assigned resources.

App.III(2)(c)

[Security Policy] Defines the type of information applicable under this Circular. Indicates an increased scope of Security Policy-in particular, the systems containing ``sensitive information'' must be protected. [MAC, DAC] Because the control of ``unauthorized use'' is explicitly called for, authorization features are required. [Marking] ``Sensitive information'' must be identifiable. [Accountability] Authorization implies the requirement for accountability for acting within the scope of authority.

App.III(2)(d)

[Security Policy] Defines the type of application applicable under this Circular. The assessment of risk, loss, or harm resulting from improper operation or deliberate manipulation of an application should be applied to all applications, including embedded application or control systems, in order to determine their ``sensitivity.'' [MAC, DAC] Because the control of ``improper operation'' or ``deliberate manipulation'' is explicitly called for, authorization features are required. [Marking] ``Sensitive applications'' must be identifiable. [Accountability] Authorization implies the requirement for accountability for acting within the scope of authority.

App.III(3)

[Security Policy] Requires the preparation and maintenance of security policies, standards, and procedures. Outlines basic considerations and the sources of policy for security programs.

App.III (3)(a)(1-2)

[Assurance] Agencies shall assure that appropriate safeguards are incorporated into all new or modified applications. The adequacy of implemented safeguards shall be evaluated and vulnerabilities identified. Periodic reviews are required.

A.9 OMB Circular No. A-123-Internal Control Systems

OMB Circular No. A-123 directs agency heads and managers to set up management plans and to take responsibility for eliminating fraud, waste, and abuse in government programs. The aim of this program is to establish confidence and accountability in the protection of Federal operations [Russell 1991, p. 279].

Internal controls are of significance primarily because of the increasing use of automation for both the major applications and the internal control systems of government programs. The Budget and Accounting Act of 1950 sets forth the requirement for each department and agency to establish and maintain adequate systems of internal control. The Federal Managers' Financial Integrity Act amended this earlier Act, adding requirements for (a) the development of internal accounting and administrative control standards by the General Accounting Office, (b) annual evaluations of internal accounting and administrative control systems in accordance with guidelines established by OMB, and (c) annual statements on the status of the agency's system of internal controls. AISs which are integral to internal control systems must adhere to the standards and guidelines prescribed in this Circular.

The following table contains selected sections of OMB Circular No. A-123. The cross-reference table and comments appear in the next section.

TABLE A-18. OMB Circular No. A-123-Selected Source Text

1. Purpose. This circular prescribes policies and procedures to be followed by executive departments and agencies in establishing, maintaining, evaluating, improving, and reporting on internal controls in their program and administrative activities.

4. Policy. Agencies shall establish and maintain a cost effective system of internal controls to provide reasonable assurance that Government resources are protected against fraud, waste, mismanagement or misappropriation and that both existing and new program and administrative activities are effectively and efficiently managed to achieve the goals of the agency. The system shall comply with the Integrity Act and the internal control standards developed by the General Accounting Office and implemented by this circular. All levels of management shall be involved in ensuring the adequacy of controls. Internal control does not encompass such matters as statutory development or interpretation, determination of program need, resource allocation, rule-making, or other discretionary policy-making processes in an agency.

7. Objectives of Internal Control. The objectives of internal control apply to all program and administrative activities. Internal control systems are to provide management with reasonable assurance that:

a. Obligations and costs comply with applicable law.

b. Assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

c. Revenues and expenditures applicable to agency operations are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and accountability of the assets may be maintained.

d. Programs are efficiently and effectively carried out in accordance with applicable law and management policy.

8. Required Agency Actions. Each agency shall meet the following requirements in a cost-effective manner.

a. Maintain a current internal control directive assigning management responsibility for internal controls in accordance with this circular and the [OMB] Internal Control Guidelines with the following provisions. Provide for coordination on internal control matters among the designated internal control official, heads of agency components, program managers and staffs, and the IG [Inspector General] office or its equivalent. Establish administrative procedures to enforce the intended functioning of internal controls. . . .

b. Develop a Management Control Plan (MCP) or plans to be updated annually. The primary purpose of an MCP is to identify component inventory, to show risk rating of component (high, medium, low), and to provide for necessary evaluations over a five-year period. Material weaknesses and other areas of management concern may also be monitored through the plan. High risk components and material weaknesses must be acted upon during the first year of the plan. The plan should be based upon the schedule of actions in each major component, and identify the senior managers responsible. Management should utilize the plan for monitoring progress and ensuring that planned actions are in fact taken. MCP's are intended to be part of each agency's overall planning process and at a minimum should be linked to activities under [OMB Circulars] A-127 and A-130. . . .

c. Make risk assessments to identify potential risks in agency operations which require corrective action or further investigation through internal control evaluations or other actions. These may follow the vulnerability assessment procedures in the [OMB] Internal Control Guidelines or may be based on a systematic review building on management's knowledge, information obtained from management reporting systems, previous risk assessments, audits, etc. . . . Risk assessment on new or substantially revised programs should occur as part of planning for implementation and the results reflected in the MCP. Risk assessments are to be considered as part of developing the MCP.

d. Make internal control evaluations using the procedures in the [OMB] Internal Control Guidelines or alternative reviews to determine whether the internal control system is effective and is operating in compliance with the Integrity Act and this circular. These reviews should identify internal controls that need to be strengthened or streamlined. The composite of all information that management relies upon to judge their systems effectiveness must include information on the results

of tests of their operating internal control systems

e. Implement corrective actions identified by agency internal control evaluation efforts on a timely basis. A formal follow-up system should be established that records and tracks recommendations and projected action dates, and monitors whether the changes are made as scheduled. The tracking systems should be made part of broader agency management reporting systems whenever feasible.

A.9.1 Cross-References and Comments

TABLE A-19. OMB Circular No. A-123-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

4

X

X

X

X

X

X

7(a)

X

X

7(b)

X

7(c)

X

8(a)

X

X

X

8(b)

X

X

X

8(c)

X

X

8(d)

X

X

8(e)

X

X

4

[Security Policy, MAC, DAC, Marking] An internal control system shall protect against fraud, waste, mismanagement, and misappropriation. Implementation of internal control systems must be in accordance with GAO standards. Efficient and effective management of program activities implies the implementation of abstractions to bind users with actions (roles) and actions with appropriate object types (duties). This implies both systems and application-specific security policies. [Accountability, Assurance] Program and administrative activities must be effective and efficient. Reasonable assurance is required.

7(a)

[Security Policy] Applicable laws related to obligations and costs must be addressed. [Accountability] Obligations and costs must be adequately recorded and reported.

7(b)

[Security Policy] AIS resources which represent program assets must be safeguarded against waste, loss, unauthorized use, and misappropriation.

7(c)

[Accountability] Operational revenue and expenditures must be recorded and reported.

8(a)

[Security Policy] Each agency shall maintain a current directive which implements internal control policy in accordance with this Circular and OMB guidelines. [Accountability] Coordination with other entities is required. [Assurance] Administrative procedures to enforce internal controls must be established. The implication that some of these procedures may be implemented (either partially or totally) within AISs requires that all procedures should be well-documented and that agency personnel must be trained properly to carry them out.

8(b)

[Security Policy, Accountability] Development and maintenance of a Management Control Plan is required. Component inventories must be established. Monitoring of weaknesses implies features for tracking and reporting. [Assurance] Evaluation and risk rating of internal controls is required.

8(c)

[Accountability, Assurance] Risk assessments for agency operations is required. Risk assessments may require follow-on, corrective actions.

8(d)

[Accountability] This implies that responsibilities for internal control systems have been established and that the responsible individuals shall be held accountable for the proper functioning of those systems. [Assurance] Internal control evaluations are required. Identification of weaknesses is required. Results of tests must be relied upon for management to judge systems' effectiveness.

8(e)

[Accountability, Assurance] Corrective actions must be implemented on a timely basis. Recording and monitoring of identified corrective actions is required.

A.10 OMB Bulletin No. 90-08-Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

This Bulletin provides guidance for computer security planning activities required under the Computer Security Act of 1987. The Bulletin does not apply to systems that contain classified information, systems involving intelligence activities, cryptologic activities related to national security, or direct command and control of military forces. The Bulletin also does not apply to equipment that (a) is integral to a weapons system,

(b) is used in the direct fulfillment of military or intelligence missions, or (c) to mixed classified and unclassified systems, if such systems are always operated under rules for protecting classified information.

Computer security planning is intended to improve protection of information and other information processing resources. In order to be adequate for the protection of resources, computer security plans must address the areas of loss, misuse, unauthorized access or modification, unavailability, and undetected activities. The controls to be addressed by computer security planning described in this Bulletin address both major applications and general support systems. These controls are derived from requirements and guidance in the Computer Security Act of 1987, OMB Circular No. A-130, and applicable Federal Information Processing Standards (FIPS) and Special Publications produced by NIST.

The following table contains selected sections of OMB Bulletin No. 90-08. The cross-reference table and comments appear in the next section.

TABLE A-20. OMB Bulletin No. 90-08-Selected Source Text

1. Purpose. The purpose of this Bulletin is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. This Bulletin supersedes OMB Bulletin No. 88-18, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information (July 6, 1988).

3. Objectives of the Security Planning Process. The security planning process is designed to reduce the risk and magnitude of harm that could result from the loss, misuses or unauthorized access to or modification of information in Federal computer systems. . . .

6. Action Required.

a. Every agency must implement security plans for systems which contain sensitive information, incorporating appropriate advice and comment from NIST/NSA.

b. Every agency must prepare a new computer security plan for each system that contains sensitive information, if:

(1) the system is new or significantly modified; or

(2) a plan for the system was not previously sent to NIST/NSA for advice and comment (particular emphasis should be on contractor, State, and local systems operated on behalf of the agency to perform a Federal function); or

(3) staff members of NIST/NSA advised the agency they were unable to provide advice and comment on the previous plan for the system.

c. Every agency must establish a process to ensure that independent advice and comment on each plan developed in accordance with Section 6.b, above, is provided. Such advice and comment should be provided prior to developing a new system or significantly modifying an existing system.

d. Every agency must ensure that security plans incorporate appropriate internal control corrective actions identified pursuant to OMB Circular No. A-123.

e. Every agency must prepare materials as described in Section 8, meet with OMB, NIST, and NSA staff as described in Section 7, and work with NIST and NSA to improve agency computer security.

7. Assistance Visits.

a. Agencies will be scheduled for visits by OMB, NIST, and NSA staff.

b. Among the items to be discussed will be:

(1) The completeness of identification of sensitive computer systems;

(2) The quality, scope, and thoroughness of security plans;

(3) Any internal control weaknesses identified pursuant to OMB Circular No. A-123 related to computer systems, and plans for addressing those weaknesses;

(4) For agencies subject to OMB Bulletin No. 89-17, ``Federal Information Systems and Technology Planning'' their response to that Bulletin;

(5) Material available in accordance with Section 8, below.

c. Agencies should also be prepared to discuss the approach that is being taken to ensure that computer security plans for new or modified computer systems are prepared and reviewed.

8. Material for Meetings. Agencies should, at a minimum, have the following information available:

a. agency-wide computer security policies and a summary of agency computer security procedures, standards, and requirements;

b. agency assignment of responsibilities for implementation and operation of the security program;

c. the agency management plan for ensuring implementation of system computer security plans that includes a description of:

(1) the involvement of agency management,

(2) how computer security plans are being integrated into information resources management plans,

(3) the approach for ensuring that funds, personnel and equipment are planned for and budgeted, and

(4) the implementation schedule;

d. the method used to identify the agency's sensitive systems;

e. any know agency needs for guidance or assistance.

Appendix A-Instructions for Preparing System Security Plans

I. System Identification

This section of the plan contains basic identifying information about the system.

C. System Category - Categorize each system as either a major application, or as a general support system, in line with the primary management responsibility for the system.

Major application. These are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components.

General support system. These consist of hardware and software that provide general ADP or network support for a variety of users and applications. Individual applications may be less easily distinguishable than in the previous category, but such applications may contain sensitive information. Even if none of the individual applications are sensitive, however, the support system itself may be considered sensitive if overall, the aggregate of applications and support provided are critical to the mission of the agency.

II. Sensitivity of Information Handled

This section should provide a description of the types of information handled by the system and thus provide the basis for the system's security requirements. It should contain the following information:

A. Applicable Laws or Regulations Affecting the System . . .

B. General Description of Information Sensitivity - The purpose of this section is to indicate the type and relative importance of protection needed for the identified system. A system may need protection for one or more of the following reasons:

Confidentiality - The system contains information that requires protection from unauthorized disclosure. Examples: timed dissemination (e.g., crop report data), personal data (covered by Privacy Act), proprietary business information.

Integrity - The system contains information which must be protected from authorized, unanticipated or unintentional modification, including the detection of such activities. Examples: systems critical to safety or life support, financial transaction systems.

Availability - The system contains information or provides services which

must be available on a timely basis to meet mission requirements or to avoid substantial losses. Examples: air traffic control, economic indicators, or hurricane forecasting.

III. System Security Measures

C. Security Control Measures - Two sets of controls are discussed on subsequent pages - one for Major Applications and the other for General Support Systems . . .

E. Security Controls Measures for Major Applications

1. Management Controls - overall management controls of the application system.

a. Assignment of Security Responsibility - Responsibility for the security of the application should be assigned.

b. Personnel Screening - Personnel security policies and procedures should be in place and working to limit access to and processing within the application system to those with a need for such access. Where appropriate, the duties of those with access should be separated. Additionally, requirements such as screening individuals with access to the application as well as those participating in the design, development, operation, or maintenance of it may be used.

2. Development/Implementation Controls - procedures to assure protection is built into the system, especially during system development.

a. Security Specification - Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application. . . .

b. Design Review and Testing . . .

c. Certification - Prior to the application being put into operation, and agency official should certify that the application meets all applicable Federal policies, regulations, and standards, and that the protection measures appear adequate. . . .

3. Operational Controls - day-to-day procedures and mechanisms to protect operational application systems (or planned applications when they become operational). . . .

a. Physical & Environmental Protection . . .

b. Production, I/O Controls - Controls over the proper handling, processing, storage, and disposal of input and output data and media, as well as access controls (such as labeling and distribution procedures) on the data and media. . . .

c. Emergency, Backup, and Contingency Planning . . .

d. Audit and Variance Detection - Controls which allow management to conduct an independent review or records and activities to test the adequacy of controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such things as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles.

e. Application Software Maintenance Controls - Controls used to monitor the installation of the updates to application software to ensure that the software functions as expected and that an historical record is maintained of application system changes. Such controls also help to ensure that only authorized software is allowed on the systems. These controls may include software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include some products used for ``virus'' protection.

f. Documentation . . .

4. Security Awareness and Training . . .

5. Technical Controls - hardware and software controls used to provide automated and/or facilitate manual protection. Normally these types of controls are coordinated with the network and/or data center manager.

a. User Identification and Authentication - Controls used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information, to perform an activity, or to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Such controls include the use of passwords, tokens, biometrics or other personal mechanisms to authenticate identity.

b. Authorization/Access Controls - Hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

c. Data Integrity/Validation Controls - Controls used to protect data from accidental or malicious alteration or destruction, and provide assurance to the user that the data meets an expectation about its quality (e.g., [electronic funds transfer] EFT message authentication). Validation controls refer to tests and evaluations used to determine compliance with security specification and requirements.

d. Audit Trails and Journaling - Controls that provide a transaction monitoring capability with a chronological record of application activities. This enables reconstruction of a transaction from its inception to final results-including any modification of files.

F. Security Controls Measures for General Support Systems

1. Management Controls - overall management controls of the general support system.

a. Assignment of Security Responsibility . . .

b. Risk analysis . . .

c. Personnel Screening - Personnel security policies and procedures should be in place and working to control access to and within the support system to assure that only those with a need for access have it. Such policies and procedures may include requirements for screening individuals involved in the operation, management, security, design, programming, or maintenance of the system.

2. Acquisition/Development/Installation Controls - procedures to assure that protection is built into the system.

a. Acquisition Specifications - Appropriate technical, administrative, physical, and personnel security requirements are to be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services.

b. Accreditation/Certification . . .

3. Operational Controls - day-to-day procedures and mechanisms to protect operational systems.

a. Physical & Environmental Protection . . .

b. Production, I/O Controls - Controls over the handling, processing, storage, and disposal of input and output from the support system (e.g., controlled or locked output boxes, tape or data screening, etc.).

c. Emergency, Backup, and Contingency Planning . . .

d. Audit and Variance Detection . . .

e. Hardware and System Software Maintenance Controls . . .

f. Documentation . . .

4. Security Awareness and Training . . .

5. Technical Controls - hardware and software controls to protect the general support systems from unauthorized access or misuse, to facilitate detection of security violations, and to support security requirements for associated applications.

a. User Identification and Authentication - Controls used to verify the

identity of a station, originator, or individual prior to allowing access to the system, or specific categories of information within the system. . . .

b. Authorization/Access Controls - Hardware or software features used to detect and/or permit only authorized access to or within the system (e.g., the use of access lists). Includes controls to restrict access to the operating system, limits on access to programming resources, and controls to support security policies of associated applications.

c. Integrity Controls - Controls used to protect the operating system, applications and information in the system from accidental or malicious alteration or destruction, and provide assurance to users that data has not been altered (e.g., message authentication). . . .

d. Audit Trail Mechanisms . . .

e. Confidentiality Controls . . .

A.10.1 Cross-References and Comments

TABLE A-21. OMB Bulletin No. 90-08-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

App.A(I)(C)

X

App.A(II)(A-B)

X

App.A(III)(E)(1-5)

X

X

X

X

X

X

X

App.A(III)(F)(1-5)

X

X

X

X

X

X

X

App.A(I)(C)

[Security Policy] In general, any particular AIS may provide (partial or total) automation of a major application while at the same time serving as a general support system. For example, a logistics DBMS [data base management system] might be considered to be a major application, and hence represents the automation of a major service provided by a component. At the same time, the AIS(s) on which the DBMS resides may provide various applications which support the functioning of that component itself, such as a payroll or other management system. At a minimum, the operation system of AIS can be considered as providing general support. Thus, such an AIS would be called upon to support (possibly) diverse protection policies. The Security Policy must represent an integration of protection policies associated with both the major applications and the general support systems provided by the AIS.

App.A

(II)(A-B)

[Security Policy] The general scope of the type of information to be protected under system security policies is defined. The availability are explicitly included. Other control objectives are affected by these concerns. Notably, fault tolerance and assurance for safety-critical systems are implied.

App.A

(III)(E)(1-5)

[Security Policy, MAC, DAC, Marking, Accountability, Assurance, Fault Tolerance] This section outlines a variety of computer security controls (e.g., management, development, operational, and technical) which apply to major application subsystems. In general, control systems extend beyond the boundaries of automated systems. However, in many cases, support for or enforcement of necessary controls can be generalized and integrated into an AIS via automated mechanisms. Significantly, these controls are analogous to those traditionally associated with, and provided by, operating systems-yet control requirements may be unique on an application-by-application basis. This may imply an increased functionality over current AIS security kernel designs to allow for the enforcement of multiple, independent security policies. All control objectives are affected.

App.A

(III)(F)(1-5)

[Security Policy, MAC, DAC, Marking, Accountability, Assurance, Fault Tolerance] This section outlines a variety of computer security controls which are associated with the traditional notion of a system. These controls essentially apply to the enforcement of a system-wide security policy. However, under the Computer Security Act of 1987, sensitive information must now be taken into account. Also, the requirements associated with major applications must also be incorporated. Hence, all control objectives are affected.

A.11 [OMB] Internal Control Guidelines

The Federal Managers' Financial Integrity Act requires sets forth requirements for internal accounting and administrative controls within Executive agencies, and requires that OMB establish-in consultation with the Comptroller General of the United States-guidelines for the evaluation of these controls. This document embodies the guidelines required to be developed by OMB under this Act.

The following table contains selected sections of the Guidelines. The cross-reference table and comments appear in the next section. Some of the numbering below does not occur in the original source text-it is included to aid in the clarity of cross-referenced comments. Because of the comprehensive nature of these guidelines, only brief examples related to AIS security will be highlighted and commented upon. The Guidelines should be consulted for required details.

TABLE A-22. [OMB] Internal Control Guidelines-Selected Source Text

Chapter IV - Vulnerability Assessments

Analysis of General Control Environment

Several factors determine the general control environment, including the following . . . :

· ADP [Automated Data Processing] Consideration - When utilized, an awareness of the strengths and exposures inherent in a system that uses ADP and the existence of appropriate controls. . . .

Chapter V - Internal Control Reviews

Identification of the Event Cycles

Event cycles are the processes used to initiate and perform related activities, create the necessary documentation, and gather and report related data. In other words, an event cycle is a series of steps taken to get something done. Each program and administrative function performed within an agency or agency component contains one or more event cycles. For example, an entitlement program could contain the following event cycles: information gathering and verification, eligibility determination, information processing and record keeping, payment, and monitoring. The event cycles for an administrative function could include payroll, procurement of supplies and materials, correspondence handling, etc. (Appendices B and B-1 present event cycles commonly found in Federal Government agencies. The General Accounting Office, professional associations, and private organizations also publish lists of common event cycles). . . .

Evaluation of the Internal Controls within the Event Cycle

. . . The manner in which this is done is to:

· Ascertain the control objective for the event cycle. . .

· Examine the documentation and ascertain whether appropriate internal control techniques are in place to enable the control objective to be met in an efficient and effective manner. Internal control techniques are the processes or documents that enable the control objective to be achieved. . . .

· Identify whether there are any internal control techniques that are excessive, . . .

Glossary

Assessable Unit - A program or administrative function or subdivision thereof which is to be the subject of a vulnerability assessment.

Control Objective - A desired goal or condition for a specific event cycle that reflects the application of the overall objectives of internal control to that specific cycle.

Event Cycle - The processes used to initiate and perform related activities, create the necessary documentation, and gather and report related data.

Inherent Risk - The inherent potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself.

Internal Control - The steps that an agency takes to provide reasonable assurance that obligations and costs are in compliance with applicable law; funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

Internal Control System - The sum of the organization's methods and measures used to achieve the objectives of internal control.

Internal Control Technique - A process or document that is being relied on to efficiently and effectively accomplish a control objective and thus help safeguard an activity from waste, loss, unauthorized use, or misappropriation.

Appendix B - Common Event Cycles and Suggested Control Objectives in Federal Agencies

This appendix presents a list of event cycles commonly found in Federal agencies and agency components. Also included are certain types of assets that are highly susceptible to loss and for which controls are vital, e.g., cash, materials and supplies. Finally, the list provides suggested control objectives for each event cycle/type of asset. . . .

[In addition to the AIS-specific event cycle examples listed below, other common event cycles address such areas as Operations, Internal Management and Administration, and Assets and Liabilities. We have included source text dealing with Information Processing and Reporting because these event cycles are directly related to all aspects of automated processing. However, in general, many of the other common event cycles and suggested control objectives cited in this section will need to be considered in formulating AIS Security Policy.]

III. Information Processing and Reporting Cycles

A. Information Collection

The primary internal control objectives normally associated with information collection are the following:

(1) Information collected is meaningful and useful.

(2) Information collected is reliable.

(3) Information is arranged in an orderly fashion.

(4) Information is maintained on a current basis.

B. Records Maintenance

The primary internal control objectives normally associated with records maintenance are the following:

(1) Records are readily available.

(2) Records are adequately protected.

(3) Only necessary records are retained.

C. Automatic Data Processing

The primary internal control objectives normally associated with automatic data processing are the following:

(1) Proper authorization of transaction inputs, adequate edit checks, and necessary safeguards of sensitive input forms to insure accurate, proper, complete and timely entry of information.

(2) Data is safeguarded to prevent unauthorized access, improper changes, or loss.

(3) Appropriate controls exist to detect unauthorized use of the system.

(4) Outputs produced accurately, completely and timely.

A.11.1 Cross-References and Comments

TABLE A-23. [OMB] Internal Control Guidelines-Cross-References

Section

Security
Policy

MAC

DAC

Marking

Accountability

Assurance

Fault
Tolerance

Chapter V

X

App.B(III)(A)(1-4)

X

X

App.B(III)(B)(1-3)

X

X

X

App.B(III)(C)(1-4)

X

Chapter V

[Security Policy] The protection requirements of each event cycle in the internal control environment shall be specified, and such specifications shall be generally reflected in the overall Security Policy.

App.B

(III)(A)(1-4)

[Accountability] Collected information must be maintained on a current basis and arranged in an orderly fashion. [Assurance] Collected information must be meaningful, useful, and reliable.

App.B

(III)(B)(1-3)

[Security Policy] Only necessary records can be retained. Records must be available and adequately protected. [Accountability] Each Agency shall establish responsibilities for record administration. The accountable individuals shall ensure that records acquisition, maintenance, and disposition conform to applicable laws and policy. [Assurance] Periodic review of records administration shall be conducted.

App.B(III)(C)

[Security Policy] An outline of internal control objectives normally associated with automated systems is presented. These internal control objectives should be reflected in each Agency and should be enforceable through Security Policy implementation mechanisms.

A.12 GAO Policy and Procedures Manual for Guidance of Federal Agencies-Title 2 - Accounting

The Federal Managers' Financial Integrity Act requires sets forth requirements for internal accounting and administrative controls within Executive agencies, and requires that OMB establish-in consultation with the Comptroller General of the GAO-guidelines for the evaluation of these controls. This document embodies the GAO guidelines and standards required under this Act.

The following table contains selected sections of the Manual. The cross-reference table and comments appear in the next section. Some of the numbering below does not occur in the original source text-it is included to aid in the clarity of cross-referenced comments. Because of the comprehensive nature of these guidelines, only brief examples related to AIS security will be highlighted and commented upon. The Manual should be consulted for required details.

TABLE A-24. GAO Policy and Procedures Manual, Title 2 - Accounting-Selected Source

Text

Appendix II-[Comptroller General's] Standards for Internal Control in the Federal Government

The internal control standards define the minimum level of quality acceptable for internal control systems in operation and constitute the criteria against which systems are to be evaluated. These internal control standards apply to all operations and administrative functions but are not intended to limit or interfere with duly granted authority related to development of legislation, rule-making, or other discretionary policy-making in an agency.

A. General Standards

1. Reasonable Assurance. Internal control systems are to provide reasonable assurance that the objectives of the systems will be accomplished.

2. Supportive Attitude. Managers and employees are to maintain and demonstrate a positive and supportive attitude toward internal controls at all times.

3. Competent Personnel. Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

4. Control Objectives. Internal controls objectives are to be identified or developed for each agency activity and are to be logical, applicable, and reasonably complete.

5. Control Techniques.

Internal control techniques are to be effective and efficient in accomplishing their internal control objectives.

B. Specific Standards

1. Documentation. Internal control systems and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.

2. Recording of Transactions and Events. Transactions and other significant events are to be promptly recorded and properly classified.

3. Execution of Transactions and Events. Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.

4. Separation of Duties. Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

5. Supervision. Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

6. Access to and Accountability for Resources. Access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. Periodic comparison shall be made of the resources with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

C. Audit Resolution Standard

Prompt Resolution of Audit Findings.

Managers are to (1) promptly evaluate findings and recommendations reported by auditors, (2) determine proper actions in response to audit findings and recommendations, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

D. Explanation of General Standards

4. Control Objectives

This standard requires that objectives be tailored to an agency's operations. All operations of an agency can generally be grouped into one or more categories called cycles. Cycles comprise all specific activities (such as identifying, classifying, recording, and reporting information) required to process a particular transaction or event. . . . Agency management cycles cover the overall policy and planning, organization, data processing, and audit functions. . . .

5. Control Techniques

Internal control techniques are the mechanisms by which control objectives are achieved. Techniques include, but are not limited to, such things as specific policies, procedures, plans of organization (including separation of duties), and physical arrangements (such as locks and fire alarms). This standard requires that internal control techniques continually provide a high degree of assurance that the internal control objectives are being achieved. . . .

E. Explanation of Specific Standards

1. Documentation

This standard requires written evidence of (1) an agency's internal control objectives and techniques and accountability systems and (2) all pertinent aspects of transactions and other significant events of an agency. Also, the documentation must be available as well as easily accessible for examination. . .

2. Recording of Transactions and Events

Transactions must be promptly recorded if pertinent information is to maintain its relevance and value to management in controlling operations and

making decisions. This standard applies to (1) the entire process or life cycle of a transaction or event and includes the initiation and authorization, (2) all aspects of the transaction while in process, and (3) its final classification in summary records. Proper classification of transactions and events is the organization and format of information on summary records from which reports are statements are prepared.

3. Execution of Transactions and Events

This standard deals with management's decision to exchange, transfer, use, or commit resources for specified purpose under specific conditions. It is the principal means of assuring that only valid transactions and other events are entered into. Authorization should be clearly communicated to managers and employees and should include the specific conditions and terms under which authorizations are to be made. Conforming to the terms of an authorization means that employees are carrying out their assigned duties in accordance with directives and within the limitations established by management.

4. Separation of Duties

To reduce the risk of error, waste, or wrongful acts or to reduce the risk of them going undetected, no one individual should control all key aspects of a transaction or event. Rather, duties and responsibilities should be assigned systematically to a number of individuals to ensure that effective checks and balances exits. Key duties include authorizing, approving, and recording transactions; issuing and receiving assets; making payments; and reviewing or auditing transactions. Collusion, however, can reduce or destroy the effectiveness of this internal control standard.

5. Supervision

This standard requires supervisors to continuously review and approve the assigned work of their staff. . . .

6. Access To and Accountability For Resources The basic concept behind restricting access to resources is to help reduce the risk of unauthorized use, loss to the Government, and to help achieve the directives of management. However, restricting access to resources depends upon the vulnerability of the resource and the perceived risk of loss, both of which should be periodically assessed. . . .

Appendix III-Accounting System Standards

A. Introduction

. . . The standards contained in this appendix apply to all manual and/or automated systems of accounting and related internal controls that are operating or are under development or major revision, in all departments, agencies, or instrumentalities in the executive branch . . .

B. Accounting System Structure and Operation

. . . Within each department or agency, the account structure (general ledger and subsidiary accounts), definitions, and data elements must be standardized to ensure consistency, uniformity, and efficiency in accounting treatment, classification, and reporting. Furthermore, the procedures for capturing, classifying, communicating, processing, and storing data and transactions must be uniform (or translatable among the various subsystems or segments of the system, as necessary). . . . Department or agency accounting systems must include reasonable safeguards and controls to ensure data integrity and to protect against the loss of the system's ability to function. . . . Agencies must periodically review their accounting systems to ensure that the system, along with its controls and security features, continues to perform as intended, meet user needs, and conform to applicable laws and accounting standards. . . .

1. Structure of the Accounting System.

. . . the systems must be structured in a way that ensures the proper gathering, recording, storing, processing, communicating, and consistent reporting [of information] . . .

Accounting information is most useful when organized by project or program, responsibility center, activity, object class of expenditure, organizational unit, appropriation, etc. Systems should be capable of responding to requirements for information along these various dimensions. . . .

2. Accounting Processing and Procedures

a. Support for Transactions

A fundamental requirement for any viable accounting system is that the financial transactions for which the system must account be adequately supported with pertinent documents and source records. These transactions, and any subsequent adjustments, should be authorized and executed in accordance with management criteria by personnel acting within the scope of their authority. . . . These transactions should be recorded in the accounts promptly and accurately . . . Thus, information should be captured in the accounting records simultaneously with or immediately following the event that gave rise to the transaction.

All transactions, including those which are computer-generated and computer-processed, must be referenced to individual source records. Referencing must be done in a manner that enables tracing or replicating a transaction from its source to the resulting record or report, and from the resulting record or report to the source, or by tracing indirectly . . .

In the case of computer-generated transactions, verification of amounts recorded or reported requires (a) reviews of systems documentation, such as edit routines and decision criteria in program listings, to gain an understanding of the events which generate transactions, and (b) ref-

erence to master files, data base records, detailed listings of computer media work files, or input transactions which trigger the computer-generated transactions.

b. Reconciliation

General ledger balances must be reconciled with subsidiary accounts and records, either manually or by the computer, in a timely manner. Regularly scheduled reconciliation . . . helps to substantiate and maintain the accuracy of account postings and balances . . .

c. Transaction Processing/Production Control

Agency accounting systems, whether automated or manual, must contain internal controls which operate to prevent, detect, and correct errors and irregularities which may occur anywhere in the chain of events from transaction authorization to issuance of reports. The controls can be generally thought of as covering the functions of transaction authorization and approval, data preparation and validation, input, communications, processing, storage, output, error resolution and re-entry of data, and file or data base quality maintenance. . . .

In automated systems, controls are usually classified as ``general'' or ``application-specific'' controls. General controls are those that affect the agency's data processing operations across-the-board . . . Application-specific controls are those related to a particular activity or subsystem, such as requirements that payroll transactions can be entered only at certain terminals. Typically, application controls are considered in terms of input, processing, and output.

Input controls should detect unauthorized, incomplete, duplicate, or otherwise erroneous transactions and ensure they are controlled until corrected. Processing controls should provide reasonable assurance that all transactions have been processed and that the application processing was correct, using correct file data, operator procedures, and processing logic. Output controls provide reasonable assurance that the output is complete, correct, and distributed only to authorized users.

Closely related to controls over input, processing, and output are controls over data communication and data storage and retrieval. Data communication controls help ensure that the integrity and confidentiality of messages (data) transmitted by communication lines . . . are maintained. In addition, data storage and retrieval controls help to ensure that the files are protected from loss, destruction, and unauthorized changes, and that only the correct and latest version of data and program files are used during processing. . . .

While the particular procedures and records used to effect these controls are left to each agency, agency systems (whether automated or manual) should include internal controls, where appropriate, that pre-

vent or detect the following kinds of situation:

-- failure to record a transaction,

-- incorrect or incomplete recording of a transaction,

-- duplicate recording of a transaction,

-- loss of a transaction document in handling,

-- incorrect entry of data at a terminal,

-- processing of unauthorized or incorrect data,

-- directly changing account/master file/data base records without an authorized transaction,

-- use of a superseded or test version of a program rather that the current production version,

-- use of a wrong file or record in processing,

-- unauthorized file maintenance transactions (which have a financial impact),

-- use of an incorrect value in internal tables,

-- incorrect default value,

-- input of incorrect program parameters,

-- unauthorized use of programs which bypass normal program controls and edits,

-- incorrect or incomplete processing logic,

-- abnormal interruption of the application processing run,

-- destruction of part or all of a file during processing,

-- data base errors,

-- out-of-balance conditions, and

-- data errors caused during data transfer between interfacing systems.

Since most transactions . . . can be heavily automated . . . initial and periodic testing of the adequacy and accuracy of the transaction processing software is necessary . . .

d. Error Handling

Systems must provide procedures for control over errors to ensure that, once errors are detected, (1) corrections are made in a timely manner and re-entered into the appropriate processing cycle, (2) corrections are made only once, and (3) the correction itself is validated.

The disposition of erroneous transactions depends on the type of transaction, the data item in error, or other control considerations. The possibilities include (1) the entire transaction is rejected and returned to its originator for correction and re-submission, or (2) the transaction is held in a suspense file . . . Procedures should be established for periodically analyzing reasons for errors and rejected transactions by type and source so that management may ensure that appropriate corrective action is taken.

e. Control Over Output

Output distribution should be controlled to ensure that only properly authorized personnel receive reports or other output. Prior to distribution, output should be checked for such things as completeness, agreement of control totals, proper labeling, and appropriate number of copies. If feasible, a cross-check with output from related programs should be done. . . .

f. Verifying File Data

The correctness or integrity of file data depends on the quality of the original file and the quality of subsequent processing affecting that file. Since data quality can deteriorate over time, systems should provide maintenance procedures to help ensure the continuing quality of files. Methods for maintaining file quality include the scanning of file contents by a computer program which reviews data items against criteria similar to those used during validation of input data. . . .

g. System Security and Integrity

To help ensure continued and authorized processing and protection of information, systems must include procedures and controls which protect hardware, software, data, and documentation from physical damage . . . and from unauthorized access whether inadvertent or deliberate. . . .

The integrity and confidentiality of the system's data and software must also be protected from accidental or malicious modification, destruction, or unauthorized disclosure. . . . Therefore, controls over personnel selection, placement, job rotation, and vacation requirements for critical or sensitive positions are important. In addition, the agency must ensure continuing availability of information processing by providing backup, recovery, and retention procedures encompassing hardware, personnel, supplies, software, data, and vital documentation. . . .

3. Accounting System Maintenance

Agency accounting systems are dynamic. They are subject to changing requirements throughout their useful lives due to changes in related technology, agency programs, funding, personnel, etc. Reaction to changing requirements as well as the activities which carry out day-to-day operations can be termed system maintenance. Management should have sufficient involvement to ensure that despite such changes, the system's stability is maintained. Stability of the system, in one context, exists when the computer software has been debugged and performs as intended. In a second context, it is maintained when successful application of management policies and procedures for control of changes in application software, improved compilers, changes in hardware, and training . . . operate to protect against communication problems, data entry failures, and user negligence. . . .

Procedures for controlling changes should require rigorous analysis of requested changes. Formally approved and documented change procedures help to protect against fraudulent or otherwise unauthorized changes . . .

4. Accounting System Reviews and Evaluations

Another consequence of the dynamic nature of accounting systems is the need for periodic reviews and tests of their operations. These are critical to ensure that the system and its controls and security features continue to meet user needs, perform as intended, and conform with applicable accounting standards. . . .

Tests should be designed to disclose whether valid transactions are processed properly and whether the system rejects invalid transactions. The tests should cover the entire flow of transactions from initial authorization through processing, posting to the accounts, and reporting. . . .

Agencies will need to exercise judgment in determining which tests would be appropriate for their systems. Also, agencies may adopt evaluation policies which provide for more comprehensive evaluations on some cyclical basis. . . .

A.12.1 Cross-References and Comments

TABLE A-25. GAO Policy and Procedures Manual, Title 2 - Accounting-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

II-A(1-5)

X

X

X

X

X

II-B(1-6)

X

X

X

X

X

X

II-C

X

II-D(4-5)

X

X

X

X

X

II-E(1)

X

II-E(2)

X

II-E(3)

X

X

X

X

II-E(4)

X

X

X

X

II-E(5)

X

II-E(6)

X

X

X

X

X

X

III-B

X

X

X

X

X

III-B(1)

X

III-B(2)(a)

X

X

X

III-B(2)(b)

X

X

III-B(2)(c)

X

X

X

III-B(2)(d)

X

X

X

III-B(2)(e)

X

X

X

III-B(2)(f)

X

X

X

III-B(2)(g)

X

X

X

X

III-B(3)

X

III-B(4)

X

II-A(1-5)

[Security Policy] These general standards for internal control should be reflected in the security policy. In particular, specific control objectives are to be identified and enforcing control techniques are to be applied. Logical, applicable, and reasonably complete control objectives must be identified or developed. Internal control techniques are to be effective and efficient. [MAC, DAC, Marking] A key aspect of these standards is the requirement for competence in performing assigned duties. Personnel should be identified with levels of competence that reflect the expectations one has for their performance and accountability. This implies that system support must exist to provide separation of levels of competency. Implementation of the abstractions of ``roles'' and ``duties'' may suffice in providing such support. [Assurance] Internal controls are designed to provide assurance for the proper operations of the system. Reasonable assurance should be defined in terms of cost effectiveness.

II-B(1-6)

[Security Policy] These specific standards for internal control should be reflected in the security policy. In particular (a) the requirements for transaction or event-execution authorization, (b) controls to ensure that individuals are only acting within the scope of their authority, (c) separation of duties and responsibilities among individuals, and (d) the requirement for qualified and continuous supervision-should be incorporated into the security policy. [MAC, DAC, Marking] In order to separate the key duties and responsibilities of individuals, those duties must be identified and bound to objects upon which transactions can be authorized, processed, recorded, or reviewed. These identifying markings should be sufficient to ensure the intent of separation is enforced. The implementation of ``roles'' and ``duties'' via typing mechanisms may suffice in providing such support. [Accountability] The recording of specified actions for which individuals are to be held accountable should be accomplished on a continuous basis. The recorded account shall be periodically reconciled and shall be compared to the external entities that the account represents. The periodicity of such comparison shall be a function of the vulnerability of the external entities. [Assurance] Documentation of sensitive events is required to provide assurance that all such events have been identified, and to assure that proper controls exist and can be properly applied before, during, and/or after the execution of such events.

II-C

[Accountability] The need to evaluate audit data and act on the evaluation findings promptly is specified and the requirement to set time bounds on resolving audit issues is established.

II-D(4-5) [Security Policy, MAC, DAC, Marking] An agency must be able to (a) identify and group related activities into specific categories, and (b) specify control objectives for the (event) cycles characterized by those categories. Control techniques must be implemented to realize the control objectives. Implementation of the abstractions of ``roles" and ``duties" enable a system to group related activities and resources, and also provide support for policy enforcement. [Assurance] A high degree of assurance that control objectives are being met is required.

II-E(1)

[Assurance] The existence of sensitive information or sensitive applications must be determined and documented. Documentation is to be readily available.

II-E(2)

[Accountability] Transactions and other significant events must be promptly recorded and classified.

II-E(3)

[Security Policy, MAC, DAC, Marking] It is implied that system support must exist to provide separation of areas of authority. Implementation of the abstractions of ``roles" and ``duties" provides such support.

II-E(4)

[Security Policy, MAC, DAC, Marking] Key duties and responsibilities must be separated among individuals. The systematic assignment of duties and responsibilities is required. The implementation of the abstractions of ``roles" and ``duties" provides support for separating mechanisms for authorizing, processing, recording, and reviewing of transactions in a systematic manner.

II-E(5)

[Assurance] Qualified and continuous supervision is to be provided.

II-E(6)

[Security Policy, MAC, DAC, Marking] Access to resources is to be limited to authorized individuals. Implementation of the abstractions of ``roles" and ``duties" provides support for constraining authorization as well as constraining access. [Accountability] Accountability for the custody and use of resources is to be assigned and maintained. [Assurance] Periodic verification of recorded accountability with reality must be made.

III-B

[Security Policy, MAC, DAC, Marking] Standardization of definitions and data elements

is required. Implementation of the abstractions of ``roles'' and ``duties'' provides standardization capabilities. Control procedures must be uniform. [Assurance] Reasonable safeguards and periodic reviews are required.

III-B(1)

[Assurance] Structure of the system must ensure proper and consistent controls are possible. Implementation of the abstractions of ``roles'' and ``duties'' provides one approach to such structuring.

III-B(2)(a)

[Security Policy] Transactions should be authorized and executed in accordance with management criteria. Transactions should be recorded promptly and accurately. [Accountability, Assurance] Referencing and tracing requirements are outlined. These requirements imply that where automated transactions replace the source documents or ``safety paper,'' concepts such as digital signatures, non-repudiation, assured service, fault tolerance, error control, etc., must be considered. Verification of recorded values is required.

III-B(2)(b)

[Accountability, Assurance] Balances must be reconciled with subsidiary accounts and records. Accuracy must be substantiated and maintained.

III-B(2)(c)

[Security Policy] The requirement to address application-specific security policy concerns is cited. A large number of representative situations in which controls are required are cited. Preventive and/or detective controls are required for these situations. [Assurance, Fault Tolerance] Controls to ensure fault detection and/or fault tolerant input, processing, and output are required. Reasonable assurance that input, processing, and output events are adequately controlled is required. Reliable communication and reliable file storage are required.

III-B(2)(d)

[Security Policy] The security policy must address how transaction errors are to be handled. In particular, it must address whether errors abort the transaction completely or whether fault detective and/or fault tolerant mechanisms can or should be employed. Errors should be detected as close as possible or practicable to their injection into the system, and must be resolved in a timely manner. [Assurance, Fault Tolerance] Error correction must take place only once and the correction itself must be validated.

III-B(2)(e)

[Security Policy] Output should be distributed only to authorized personnel. [Marking] Output media should be properly labeled to reflect sensitivity, distribution restrictions, copy numbers, etc. [Assurance] Verification of output is required, if feasible.

III-B(2)(f)

[Security Policy] Appropriate standards of quality must be specified against which quality attributes of data can be assessed. Timing aspects with respect to data quality must be addressed in the security policy. For example, the frequency of updates, allowable lag time from input to processing, and the serialization of data and events must be addressed. [Marking] Time sensitivities must be represented in the system as an attribute of data objects. [Assurance] Maintenance procedures to help ensure the continuing quality of files is required. Conformance to quality standards must be ensured. This implies verification of internal values and attributes with external facts via periodic reviews and reconciliation.

III-B(2)(g)

[Security Policy, MAC, DAC, Marking] A system's data and software must be protected from accidental or malicious modification, destruction, and unauthorized disclosure. Controls over personnel and job assignment are required. Issues such as rotation of duties, authorization overrides, and temporary authorization must be considered. Implementation of the abstractions of ``roles'' and ``duties'' provides support for such features.

III-B(3)

[Assurance] A well-disciplined configuration management and version control system is required. Procedures for controlling changes to systems require rigorous analysis and documented and formally-approved change procedures.

III-B(4)

[Assurance] Periodic reviews are required. These reviews are directed towards determining whether a system and its controls and security features meet user needs, perform as intended, and conforms to standards. Functional testing of control features must extend to application subsystems. Control objective testability is implied.

A.13 DoD Directive 5010.38-Internal Management Control Program

This directive establishes the DoD program for Internal Management Control (IMC), incorporating guidance under 31 U.S.C. 3512 (also referred to as PL 97-255, Federal Managers' Financial Integrity Act of 1982); OMB Circular A-123 (Internal Control System); OMB Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government; and GAO Standards for Internal Control in the Federal Government. This Directive provides policy, prescribes procedures, and assigns responsibilities.

DoD internal management control (IMC) is ``the plan of organization, methods, and procedures adopted by management to provide reasonable assurance that the objectives of [FMFIA 1982] are met'' [DoD 5010.38-D, Encl.2(7)]. IMC is intended to safeguard resources, assure the accuracy and reliability of information, assure adherence to applicable laws, regulations, and policies, and promote operational economy and efficiency. IMC systems are not separate from, but are integral to, systems used to operate programs and functions. As such, IMC within the DoD is equivalent to the more prevalent term ``internal controls.''

The following table contains selected sections of DoD Directive 5010.38. The cross-reference table and comments appear in the next section.

TABLE A-26. DoD Directive 5010.38-Selected Source Text

A. Re-issuance and Purpose

1. This Directive reissues [DoD 5010.38-D of July 16, 1984] to:

a. Establish the DoD program for Internal Management Control (IMC).

b. Incorporate guidance under references [FMFIA 1982], [OMB A-123], . . . , and [GAO 1983].

c. Provide policy, prescribe procedures, and assign responsibilities.

D. Policy

1. Each DoD Component shall implement a comprehensive system for IMC that provides reasonable assurance that:

a. Obligations and costs comply with applicable law.

b. Assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

c. Revenues and expenditures applicable to DoD operations are recorded and accounted for properly to permit the preparation of accounts and reliable financial and statistical reports, and to maintain accountability over the assets.

d. Programs and administrative functions are efficiently and effectively carried out in accordance with applicable law and management policy.

e. IMC systems emphasize prevention of waste, fraud mismanagement, and timely correction of specific weakness.

Enclosure 2. Definitions

5. Event Cycle. A series of steps taken to get something done. Any program or function performed within an organization contains such processes used to start and perform related activities, create necessary documentation, and gather and report related data.

15. Material Weakness. Specific instances of noncompliance with the FMFIA of sufficient importance to be reported to the next higher level of management. Such weakness significantly impairs the fulfillment of a DoD Component's mission; deprives the public of needed services; violates statutory of regulatory requirements; significantly weakens safeguards against fraud, waste, or mismanagement of funds, property. or other assets; or results in a conflict or interest. (See enclosure 4 for further information.)

Enclosure 4. Guidance in Applying the Definition of Material Weakness

B. Discussion of Material Weakness Definition . . .

1. A material weakness in DoD's system of internal management controls may be due to lack of an applicable control, or more frequently, inadequate compliance with existing controls. These controls deal with all program and administrative functions; they are not limited to financial or accounting matters. . . .

2. In addition to the basic characteristics of a material weakness described in sections A. and B., above, the final determination to categorize an internal control weakness as material results from management judgment about the relative impact of the weakness. For example, scoring each of the following considerations as ``significant'' or ``insignificant'' might help a manager in determining whether the absence of or noncompliance with a control is a material weakness.

a. Actual or potential loss or resources.

b. Sensitivity of the resources involved.

c. Magnitude of funds, property, or other resources involved.

d. Frequency of actual and/or potential loss.

e. Current or probable media interest (adverse publicity).

f. Current or probable Congressional interest (adverse publicity).

g. Unreliable information causing unsound management decisions.

h. Diminished credibility or reputation of management.

i. Impaired fulfillment of essential mission.

j. Violation of statutory or regulatory requirements.

k. Impact on information security.

l. Deprived the public of needed Government services.

A.13.1 Cross-References and Comments

TABLE A-27. DoD Directive 5010.38-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

D(1)(a-e)

X

Encl.4(B)(1)

X

Encl.4(B)(2)(a-l)

X

D(1)(a-e)

[Security Policy] Policies and guidance stipulated under [FMFIA 1982], [OMB A-123], and [GAO 1983, GAO Title 2, App.II] are promulgated to DoD components.

Encl.4(B)(1)

[Security Policy] This broadens the scope of controls to include all programs and administrative functions.

Encl.4(B)(2)(a-l)

[Security Policy] All of these categories have some effect on the degree of integrity which needs to be provided by information systems which are directly involved with primary functions, or support those functions. Some of these include ways in which the ``value'' of information can be determined in non-monetary ways. Material weakness, such as those cited, provide specific effects of system failure or non-compliance with policy. The controls implementing a policy should be examined for specific weaknesses that might be presented should a control failure occur in an event cycle. ``Material weakness'' was previously defined in Encl.2(15) of the Selected Source Text.

A.14 DoD Directive 5200.28-Security Requirements for Automated Information Systems

This Directive establishes uniform policy for protecting classified data that is stored, processed, used, communicated, displayed, or disseminated via AISs. In addition, this Directive provides for the application of access and distribution controls for classified data beyond those required by security classification. A stated objective of this Directive is to establish that the reliability, integrity, and operation of AISs are enhanced by the

imposition of controls which satisfy classification requirements. Significantly, this Directive states that increased AIS reliability and integrity features are necessary for (a) the dependable enforcement of confidentiality policy for classified information, and (b) the prevention of unauthorized manipulation of computers and peripherals.

The following table contains selected sections of DoD Directive 5200.28. The cross-reference table and comments appear in the next section.

TABLE A-28. DoD Directive 5200.28-Selected Source Text

D. Policy

It is DoD policy that:

1. Classified information and sensitive unclassified information shall be safeguarded at all times while in AISs. Safeguards shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required. When classified information is involved, the information security requirements in [DoD 5200.1-R] shall be met.

2. Unclassified information while in AISs shall be safeguarded against tampering, loss, and destruction and shall be available when needed. . . . Suggested safeguards for unclassified information are in OMB Circular No. A-130, and include applicable . . . controls.

3. The safeguarding of information and AIS resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards . . . .

4. The mix of safeguards selected . . . shall ensure the AIS meets the minimum requirements as set forth in enclosure 3 [see below]. . . .

5. Computer security features of commercially produced products and Government-developed or -derived products shall be evaluated (as requested) for designation as trusted computer products for inclusion on the Evaluated Products List (EPL). Evaluated products shall be designated as meeting security criteria maintained by the National Computer Security Center (NCSC) . . . described in DoD 5200.28-STD [TCSEC 1985].

Enclosure 3. Minimum Security Requirements

A. Minimum Security Requirements. The following minimum requirements shall be met through automated or manual means in a cost-effective manner and integrated fashion:

1. Accountability.There shall be in place safeguards to ensure each person having access to an AIS may be held accountable for his or her actions on the AIS. There shall be an audit trail providing a documented history of AIS use. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur. To fulfill

this requirement, the manual and/or automated audit trail shall document the following:

a. The identity of each person and device having access to the AIS.

b. The time of the access.

c. User activity sufficient to ensure user actions are controlled and open to scrutiny.

d. Activities that might modify, bypass, or negate safeguards controlled by the AIS.

e. Security relevant actions associated with periods processing or the changing of security levels or categories of information.

DAAs [Designated Approval Authorities] shall cause a review to be made of audit trails associated with the AIS(s) over which the DAAs have cognizance to determine an adequate retention period for the audit information. The decision to require an audit trail of user access to a stand-alone, single-user AIS (e.g., personal computer (PC), memory typewriter, drafting machine) should be left to the discretion of the DAA.

2. Access. There shall be in place and access control policy for each AIS. It shall include features and/or procedures to enforce the access control policy of the information within the AIS. The identity of each user authorized access to the AIS shall be established positively before authorizing access.

3. Security Awareness and Training. There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS. The program shall ensure that all persons responsible for the AIS and/or information, therein, and all persons who access the AIS are aware of proper operational and security-related procedures and risks.

4. Physical Controls. AIS hardware, software, and documentation, and all classified and sensitive unclassified data handled by the AIS shall be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification (i.e., data integrity shall be maintained). The level of control and protection shall be commensurate with the maximum sensitivity of the information and shall provide the most restrictive control measures required by the data to be handled. This includes having personnel, physical, administrative, and configuration controls. Additionally, protection against denial of service of AIS resources (e.g., hardware, software, firmware, and information) shall be consistent with the sensitivity of the information handled by the AIS. Unclassified hardware, software, or documentation of an AIS shall be protected if access to such hardware, software, or documentation reveals classified information, or access provides information that may be used to eliminate, circumvent, or otherwise render ineffective the security safeguards for classified information. Software development and related activities (e.g., systems analysis) shall be controlled by physical controls (e.g., two-person control) and protected when it is determined that the software shall be used for

handling classified or sensitive unclassified data.

5. Marking. Classified and sensitive unclassified output shall be marked to accurately reflect the sensitivity of the information. Requirements for security classification and applicable marking for classified information are set forth in [DoD 5200.1-R]. The marking may be automated (i.e., the AIS has a feature that produces the markings) or may be done manually. Automated markings on output must not be relied on to be accurate, unless the security features and assurances of the AIS meet the requirements for a minimum security class B1 as specified in DoD 5200.28-STD [TCSEC 1985]. If B1 is not met, but automated controls are used, all output shall be protected at the highest classification level of the information handled by the AIS until manually reviewed by an authorized person to ensure that the output was marked accurately with the classification and caveats. All media (and containers) shall be marked and protected commensurate with the requirements for the highest security classification level and most restrictive category of the information ever stored until the media are declassified (e.g., degaussed or erased) using a DoD-approved methodology set forth in the DoD AIS Security Manual [DoD 5200.28-M], on unless the information is declassified or downgraded in accordance with [DoD 5200.1-R].

6. Least Privilege. The AIS shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but to no more. In the case of ``need-to-know'' for classified information, access must be essential for accomplishment of lawful and authorized Government purposes.

7. Data Continuity. Each file or data collection in the AIS shall have an identifiable source throughout its life cycle. Its accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know.

8. Data Integrity. There shall be safeguards in place to detect and minimize inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.

9. Contingency Planning. Contingency plans shall be developed and tested in accordance with OMB Circular No. A-130 [OMB A-130] to ensure that AIS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data is modified or destroyed, procedures must be in place to recover.

10. Accreditation. Each AIS shall be accredited to operate in accordance with a DAA-approved set of security safeguards.

11. Risk Management. There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.

A.14.1 Cross-References and Comments

TABLE A-29. DoD Directive 5200.28-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

D(1)

X

X

D(2)

X

X

X

D(3)

X

X

X

D(4)

X

X

X

X

X

D(5)

X

Encl.3(A)(1-11)

X

D(1)

[Security Policy] Classified information must only be used for its intended purpose and must retain its content integrity. Hence, arbitrary operations outside the scope of an individual's authority on instances of classified data should not be allowed. [Marking] This further implies that the information must be identified in terms of state attributes which allow judgement to be made as to the retention of content integrity.

D(2)

[Security Policy] In general, unclassified information is to be considered an asset and should be protected from tampering, loss, and destruction. [Assurance, Fault Tolerance] Information shall be available when needed.

D(3)

[Security Policy] AIS resources, including classified and unclassified systems and information, must be protected from unauthorized modifications. The prevention of fraud implies that controls shall exist to limit actions of authorized users. [Assurance, Fault Tolerance] Protection of systems and information must be continuous.

D(4)

[Security Policy] The minimum requirements for data integrity includes safeguards to detect and minimize erroneous modifications, and to detect and prevent malicious modifications. A risk reduction policy is called for in minimizing possible damage. [MAC, DAC, Marking] Prevention of malicious modifications implies controls on authorization. [Accountability] The detection of erroneous and malicious modifications is called for.

D(5)

[Assurance] Trusted systems shall be used in the protection of information.

Encl.3(A)(1-11)

[Security Policy] The minimum security requirements for AISs are specified.

A.15 DoD Directive 7740.1-DoD Information Resources Management Program

This Directive implements the policies stated in Public Law 96-511, Paperwork Reduction Act of 1980 and establishes the DoD Information Resources Management (IRM) Program. IRM is defined as ``the policy, action, or procedure concerning information (both automated and non-automated) that management establishes to serve the overall current and future needs of the organization. IRM policy and procedures

address such areas as availability, timeliness, accuracy, integrity, privacy, security, auditability, ownership, use, and cost-effectiveness of information" [DoD 7740.1-D, Encl.2(3)]. A list of DoD policy issuances related to these functions is included in DoD Directive 7740.1 [Encl.1]. However, because this Directive was issued in 1983, some of these policy issuances are either dated or have been superseded. This Directive applies to DoD information management activities including such areas as information technology, data elements, information collection, privacy of records, information security, statistical activities, forms, reports, and records.

The following table contains selected sections of DoD Directive 7740.1, used for cross-referencing the source material and the affected control objectives. The cross-reference table and comments appear in the next section.

TABLE A-30. DoD Directive 7740.1-Selected Source Text

A. Purpose

This Directive:

1. Establishes the DoD Information Resources Management (IRM) Program to promote coordinated and integrated information management functions and implements [PRA 1980].

B. Applicability and Scope

2. Its provisions cover the information management activities of information technology, data elements, information collection, privacy of records, information security, statistical activities, forms, reports, and records. . . .

3. Its provisions cover the management of information within the Department of Defense, as well as information provided to and received from government agencies and information received from the public.

D. Policy

It is the policy of the Department of Defense to implement IRM aggressively in ways that enhance mission performance through the effective, economic acquisition and use of information.

E. Procedures

In achieving the above policy, it is necessary that efforts be directed toward procedures that are designed to:

1. Support DoD operations and decision making with information that sufficiently meets the need in terms of availability, accuracy, timeliness, and general quality.

2. Provide for the economic and effective acquisition of information resources emphasizing maximum practicable competition and lowest total overall cost consistent with mission requirements.

3. Structure information systems in ways that encourage horizontal, as well as vertical, sharing of information within the Department of Defense, with other government agencies, and with allied nations, consistent with security and privacy requirements.

4. Ensure that information planning becomes an integral part of the management process at all levels.

5. Require user responsibility and accountability in the development of effective information systems.

6. Manage information, information technology, and information systems using a disciplined approach from inception through acquisition and use until discontinuance.

7. Use regular reviews and evaluations to identify opportunities for improvement, to increase the usefulness of information, to reduce the cost of information activities, and, in general, to further DoD IRM Program goals and objectives.

8. Create a broad awareness of IRM concepts and practices and provide necessary training.

9. Organize and integrate information management functions to accomplish mission goals.

10. Collect information that is non-duplicative and that supports essential needs in a cost-effective manner.

11. Establish and maintain effective working relationships within the Department of Defense and with Congress and the federal central management agencies, such as the Office of Management and Budget (OMB), the General Services Administration (GSA), and the General Accounting Office, with respect to IRM matters.

12. Encourage users and information managers to plan effectively for the sustainability and readiness of information resources in both peacetime and wartime conditions.

A.15.1 Cross-References and Comments

TABLE A-31. DoD Directive 7740.1-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

D

X

E(1)

X

X

X

X

E(3)

X

X

X

X

X

E(5)

X

X

E(6)

X

X

E(7)

X

X

E(8)

X

X

E(10)

X

X

E(12)

X

X

D

[Security Policy] Information acquisition and use must be effective, economic, and must serve to enhance mission performance.

E(1)

[Security Policy] Operations and decision making must be supported by information systems. Requirements for information accuracy, timeliness, and quality imply the need to implement system features that control these attributes in accordance with specified policy. [Marking] The control of these attributes may require marking of data objects to support implementation. [Assurance] The effectiveness of the control features in maintaining these attributes within specifications shall be assessed. [Fault Tolerance] The requirement for information availability implies fault tolerant features.

E(3)

[Security Policy] The Security Policy must address the horizontal and vertical sharing of information. [MAC, DAC] The requirement for both vertical and horizontal sharing of information implies the need for access control features. The simultaneous sharing of information between vertical and horizontal DoD components may require a more rigorous specification of authorization, as is represented by the abstractions of ``roles'' and ``duties.'' [Marking] The establishment of information sharing agreements must include confirmation that the receiving DoD component can mark and protect the shared information as required by the providing component. If such protection is not possible, then the providing component must determine the need to desensitize the information to the degree commensurate with the maximum protection capabilities of the receiving component prior to actual sharing. [Accountability] The receiving component should be accountable for the protection of any shared information it receives. The providing component is accountable for the sharing of sensitive information for which the receiving component does not have the capabilities to protect.

E(5)

[Security Policy] Information systems which are developed by DoD components must be effective relative to specific mission requirements. [Accountability] Individuals in-

volved in the development (and maintenance) of information systems are to be held accountable for the effectiveness of those systems.

E(6)

[Security Policy] Systems, information technology, and information must be managed with discipline throughout their respective life cycles. [Assurance] Measures must be implemented to assure that proper controls exist throughout the life cycle of all information resources.

E(7)

[Security Policy, Assurance] Continuous improvement in information life cycle management is required. Review and evaluation processes must be integrated into life cycle management to enable the identification of improvement opportunities. Review and evaluation processes are essential to ensure that overall goals and objectives associated with information systems are being met.

E(8)

[Security Policy] Security training must be integrated into information life cycle management. [Assurance] Training is an essential assurance measure.

E(10)

[Security Policy] Specific component policies regarding information sharing and elimination of duplication should be established. [Assurance] Cost effectiveness can only be determined by weighing the benefits of sharing data against the associated risks and the costs incurred in countering those risks. This implies that a thorough risk analysis must be performed.

E(12)

[Security Policy] Plans for the sustainability and readiness of information resources are required. [Assurance] Contingencies should not only be planned for but also routinely exercised whenever practicable.

A.16 DoD 7740.1-G-DoD ADP Internal Control Guideline

This Guideline incorporates the provisions of the Federal Managers' Financial Integrity Act and OMB Circulars A-123, A-127, and A-130, and provides guidance on implementing DoD Directives 5010.38, 7740.1, and 5200.28. It incorporates the ``Model Framework for Management Control over Automated Information Systems," developed by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency. This document provides guidance for implementing an AIS internal control program and is issued under the authority of DoD Directive 7740.1, DoD Information Resources Management Program. The Guideline [DoD 7740.1-G, p. 1-4] provides the following definition of AIS internal control for the Department of Defense:

The steps taken within each DoD program and administrative function consisting of the plan of organization and all of the methods and techniques used to safeguard AIS re-

sources and provide reasonable assurance of the accuracy and reliability of computer-based input, processing and output; ensure the adherence to applicable laws, regulations and policies; and promote the effectiveness, efficiency and economy of AIS operations and systems.

The Guideline provides general guidance which can be tailored to meet the specific requirements under the Internal Management Control Program, a mandatory program for all DoD Components. However, compliance to the program under this Guideline must be comprehensive, addressing all relevant sections. This document is intended to (1) assist managers, users, and developers in conducting risk assessments, (2) provide a framework for management control efforts, and (3) serve as a reference for AIS control techniques. Table 3.1 of the Guideline contains a set of 55 system control requirements cross-referenced with the most important of the policy documents. This table is reproduced in Appendix B of this document.

The following table contains selected sections of the Guideline. Because of its comprehensive nature, only a small portion of the Guideline is included. The Guideline should be consulted for required details. The cross-reference table and comments appear in the next section.

TABLE A-32. DoD Guideline 7740.1-G-Selected Source Text

Chapter 1 Introduction

A. Background

1. The Department of Defense (DoD) depends increasingly on automated information systems (AISs). . . . These systems are vulnerable to fraud, waste, and abuse. A few examples include:

· unauthorized access and disclosure of classified, privacy, and proprietary records and/or data,

· diversion of payments to unauthorized parties,

· use of computers for personal matters, and

· disruption and loss of computerized records and/or transactions.

D. Objectives of the Guideline

There are six (6) basic objectives:

1. Assist AIS managers and users in understanding their responsibilities and requirements to develop AIS internal management controls as required by OMB Circular A-123 and by the current DoD Directive 5010.38, DoD Directive 7740.1, and DoD Directive 5200.28 . . .

2. Provide a vehicle for the education and training of managers so they may have a working understanding of AIS internal management controls.

3. Notify components of a requirement for a 5-year Management Control Plan (MCP) to be developed annually.

4. Delineate responsibilities for managers in either monitoring large AIS systems and assets or conducting internal control reviews and alternative review, such as internal audits, inspections, investigations, studies, and computer security reviews.

5. Help to ensure that internal controls receive appropriate attention, emphasis, and resources in the automated information system life cycle, to include development, modification, operation and records management concerns.

6. Show managers how to protect their operations by providing AIS internal control techniques and procedures for conducting risk assessments.

Chapter 2 - System Controls Conceptual Framework

A. Introduction

1. This chapter presents a conceptual framework for instituting and maintaining information system controls. The control framework consists of three elements:

a. Control requirements - the terms used to explain why controls are needed and/or what their implementation is expected to achieve.

b. Selection and use of control techniques - the definition, selection, and use of control techniques to satisfy the requirements specified.

c. Areas of control - the terms used to describe how and where control techniques are applied to satisfy basic control requirements.

3. Most control-related activities have traditionally centered on internal control reviews, risk assessments, and audits of existing automated systems and processes. While these types of review are needed, they do not necessarily ensure that adequate management controls are built into current and future systems. . . .

4. Fundamentally, automated information systems are developed to support managers to effectively fulfill their responsibilities. In the Federal Government, automated information systems perform a wide range of functions that include: making benefit payments; collecting receivables; and recording and accounting for obligations, costs, revenues, and expenses. In many cases, these kinds of functions are almost completely dependent on automated information systems, thereby creating many new concerns and risks for management. . . .

5. To address these concerns, managers who operate or use ADP systems should take actions to eliminate or at least reduce the risks to acceptable levels. All such actions taken to reduce risks are referred to as ``control techniques'' or, more commonly, ``controls.'' The underlying requirement of control over an automated information system is to provide reasonable assurance that the information processed by the system is reliable and properly safeguarded.

6. Management oversees and effects the development, implementation, and use of automated information systems through a variety of mechanisms, including standards, budget and procurement review and authorization, and personnel hiring practices. While existing mechanisms have worked with varying success to ensure that systems support an organization's mission, they have not always provided reasonable assurance that a system is safe. Systems may improve accuracy, increase productivity, or speed service but at the same time be subject to fraud, waste, and abuse.

B. System Control Requirements

1. Control requirements are established to address a known vulnerability or promote reliability or security of a system. They can be based on management experience, vulnerability assessments, other reviews, and/or common sense. Regardless of why established, control requirements should be as specific as possible and stated in clear, understandable terms.

2. Four categories of control requirements surfaced in an analysis of the provisions of the system control directives . . . These are application controls, general controls, administrative controls, and required system functions. While the ongoing discussion deals with these four categories of control requirements, it should be recognized here that the operational implementation of a controls program will involve a refining of these requirements into sub-requirements or control objectives. [See Appendix B of this document].

3. The first category, application controls, are those that help assure that information processed is authorized, valid, complete, accurate, and timely. It also contains requirements that ensure that the system is secure and that an audit trail exists.

4. Compliance with the requirements for application controls has proved the most elusive for management to meet. Requirement terminology varies among the many directives, but the intent is the same in all.

5. Three principles are important to note:

a. How information should be handled, once its sensitivity and/or classification has been determined, is fairly well established by the regulating agency.

b. The determination of the classification levels for systems and data is a management responsibility of the sponsoring agency.

c. Once the classification levels are determined by management, the determinations should be systematically applied, and management should be aware of any exceptions.

6. What the third principle means is that sensitive data in a computer data base should have the same classification as they are given in a hard copy publication. Most processes (accounting or otherwise) consist of both manual and automated portions. Reviews of the process should assess the totality of the process compo-

nents affected, not just a portion of the affected components. Further, management must be aware that increases in security are almost always accompanied by increases in cost, although some security measures can be implemented with little effort. Management must be aware of situations when resources are insufficient to provide the level of protection required, because it is management that must accept the risk of loss and/or disclosure. Because of the terminology and technical complexities of automated processes, the evidence suggests that managers often delegate these critical decisions to their program and/or technical staff. It is of paramount importance that managers fully understand the need for controls, the resource implications of controls, and the risks associated with inadequate controls. These are management's responsibilities and cannot be delegated.

7. The second category, general controls such as cost-benefit analysis and certification, are quantifiable and require a product to be created for management review and/or acceptance. These tools are essential to good management in the development and operation of systems by facility managers, users, systems analysts, and computer programmers. Another essential tool which should be applied by all managers and users is agency record and disposition schedules.

8. The third category, administrative controls such as supportive attitudes or competent personnel, are generally difficult to quantify and have not resulted in the past in tangible work products within automated information systems.

9. Many of the requirements have become standard operation procedures in some Federal Agencies, with considerable guidance provided on how they should be met.

10. The last category of control requirements, required systems functions, consists of mandated features that must be designed and built into a system, such as a particular access capability.

C. Selection and Use of Control Techniques

1. Control techniques are procedures used to meet control requirements. Control techniques employed might be preventive, detective, corrective, or a combination of the three . . .

2. The selection of a control technique should, in most cases, be a group decision to ensure that it is feasible for the entire system, is understood by all affected, and comprehensively meets the organization's control requirements. . . .

3. Further, the control selected must be cost-effective. . . . Controls that require manpower, such as integrity reviews of transactions, can be costly and require a cost-benefits analysis. This analysis becomes part of the controls documentation. Decisions on some controls may also require detailed knowledge of controls already in place. This is especially true of routine controls, such as access controls. The composition of current access controls may greatly affect the design of any additional access controls being contemplated for a particular system.

4. The installation of controls must be accompanied by an effort to provide assurance that the control operates as initially intended. Testing is needed before the

control is implemented, as well as later, to be sure it still fulfills the control requirement. Ongoing reviews might be a part of a management initiative. . . .

5. The controls selected and implemented must have certain characteristics to ensure that they are effective. They must be:

a. Clear in purpose - If not understood, controls may not be used and if they do not have a clear purpose or address a known vulnerability, they are of little or no value.

b. Coordinated - Developed in partnership by personnel knowledgeable about the application, process, computer systems, and control techniques. It is unlikely that effective, feasible controls can be selected and implemented unilaterally by, for example, a user, a system analyst, a programmer, or an auditor.

c. Cost-effective - The cost of the control should not, in general, exceed the expected benefits. Stated another way, there should be reasonable assurance that the system is protected from a known risk. If total assurance of control were possible, it would probably be prohibitively expensive. . . .

d. Documented - The documentation process should be simple, understandable, clearly link risks to controls, and provide management with assurance that all reasonable controls are in place. Without some form of documentation, there is no assurance that all known vulnerabilities are addressed or that controls are in place.

e. Tested and reviewed - There must be assurance that the controls function as originally intended. This assurance is needed when the systems first becomes operational and also during ongoing operation. Initial controls testing should normally be done when all other aspects of the system are tested. Ongoing testing and review might be done as part of a general system review, and internal control review, an audit, or other management initiative.

f. Manageable - Management must have the means to change, delete, evaluate cost, upgrade, or review the system of controls under its purview.

D. Areas of Control

1. Automated information systems typically encompass data files, computer programs, and equipment, all of which may affect controls in some way. Part of the problem in dealing with controls is the wide variability in how systems are defined. If there was uniformity in definitions, then control techniques could be applied, evaluated, and cataloged more easily.

2. The five control areas listed below are the basic control requirements. . . .

a. Input - includes the records (also referred to as either manual data or transactions) to be processed by the system, and the associated processes from origination to the computer.

b. Output - includes the records and reports produced by the system, and the associated manual processes from the computer to the user.

c. Processing - includes all computer processing to receive the input and store and/or otherwise manipulate the input to produce output.

d. Storage - includes all computer program code and/or instructions and data files.

e. Communications - includes the transmission of data and/or information either between sites or between peripherals at a site.

3. Viewing a system in its pieces makes it easier to set specific control requirements and select control techniques. It is important to retain a system's perspective, to avoid over-control, and to deal with system-wide issues. The following system-wide control issues need to be considered:

a. Control techniques in one control area may lessen the need for controls in another control area; for instance, tight controls over data files may negate the need for some communication controls.

b. Some aspects of a system may require special system-wide attention; e.g., a highly sensitive sub-file may require tight controls during inputting, storage, or outputting.

4. This perspective should be the responsibility of individuals or a group that is involved in all aspects of the system. A user group or a controls specialist assigned to the project might be assigned controls responsibility.

5. In general, the framework proposes that control techniques be applied to defined control areas to fulfill control requirements . . .

A.16.1 Cross-References and Comments

TABLE A-33. DoD Guideline 7740.1-G-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

Chap.2(B)(1)

X

Chap.2(B)(2)

X

Chap.2(B)(3)

X

X

X

X

X

Chap.2(B)(5)

X

X

Chap.2(B)(5)(c)

X

X

Chap.2(B)(6)

X

X

X

Chap.2(B)(8)

X

X

X

X

Chap.2(B)(9)

X

Chap.2(B)(10)

X

X

X

Chap.2(C)(1)

X

Chap.2(C)(2)

X

Chap.2(C)(3)

X

Chap.2(C)(4)

X

Chap.2(C)(5)(a-f)

X

Chap.2(D)(1)

X

Chap.2(D)(2)(a-e)

X

Chap.2(D)(3)(a-b)

X

Chap.2(D)(4)

X

Chap.2(B)(1)

[Security Policy] A security policy serves as the set of basic requirement statements which must address vulnerabilities and promote security, reliability, and safety. Specific control requirements must be developed for each appropriate facet (i.e., security, reliability, safety, and known vulnerabilities) and must be clearly stated.

Chap.2(B)(2)

[Security Policy] Control requirements must address each of the four cited categories. Of these, application controls and required systems functions are of paramount concern in terms of (a) specification of intent, (b) specification of explicit constraints, and (c) specification of control area.

Chap.2(B)(3) [Security Policy] Application-specific control requirements must address the authorization, validity, completeness, accuracy, and timeliness of information processing. [MAC, DAC, Marking] Requirements for authorization imply access control features. [Accountability] Auditing of access controls for accountability is required by authorization requirements.

Chap.2(B)(5)

[Security Policy] The protection of information may have mandatory control components imposed by law, an external regulatory agency, and/or a higher authority within an organization. The security policy must reflect this imposed requirement. [MAC] The application of the security policy must ensure that the mandatory access control component is consistent with the specification in the policy requirement.

Chap.2(B)(5)(c)

[Accountability] Audit and/or other accountability features are required to keep management aware of exceptions to established policies. [Assurance] Systematic application of controls implies that the totality of controls, including those resident in AISs, must be considered in determining the scope of protection. Assurance techniques can be used to make management aware of any exceptions in the systematic application of controls.

Chap.2(B)(6)

[Security Policy] Management must be aware of the cost-benefit tradeoffs in providing protection and control features. This implies a thorough and comprehensive risk assessment process. [Marking] Information within AISs must be marked with attributes which reflect the same categorization (and implying the same controls) as those associated with external hard copies of that information. [Assurance] Reviews must consider the totality of process components.

Chap.2(B)(8)

[Security Policy] The issue of identifying competency of personnel, albeit difficult, is one that is significant for integrity. In identifying competency levels, the initial procedure should be to objectively separate specific duties into roles, to which individuals can be assigned. Thus, role and duty specifications form an objective basis of competency, while actual assignment of roles can be based on management's subjective opinion. [MAC, DAC] The mandatory and discretionary aspects of the use of roles and duties, coupled with data object attributes, serve as a basis for object access or process execution, enabling enforcement of competency-related policies. [Marking] Attributes of both subjects and objects must be available either through system-enforced marking or as an inherent part of a subject or object to enable such controls.

Chap.2(B)(9)

[Security Policy] Many standard operating procedures that contain acceptable controls in manual environments will not necessarily be acceptable in an automated environment. As more functionality becomes integrated into computer systems, new controls for standard automated operating procedures will be required. This will result in a much richer set of security policy and ensuing controls the those conceived for confidentiality.

Chap.2(B)(10)

[Security Policy, Assurance, Fault Tolerance] Required systems functions must be considered in formulating the security policy. This implies assurance and fault tolerance features for some applications. The mandatory aspects of a security policy which must be enforced by system-provided mechanisms must be identified and determined to be a consistent (i.e., non-conflicting) set of requirements. Where conflicts arise, alternatives to system-provided mechanisms must be employed until the conflicts are resolved. In employing these alternative controls, the intent of the initial requirements set must be met.

Chap.2(C)(1)

[Security Policy] Prevention, detection, and correction are all valid techniques for addressing threats to protected resources. An appropriate choice of mechanisms employing a particular type of technique, or a combination of techniques, must be made for protected resources.

Chap.2(C)(2)

[Assurance] The feasibility, understandability, and comprehensiveness of selected control techniques must be considered. This implies ``economy of mechanism'' to enforce overlapping aspects of controls.

Chap.2(C)(3)

[Assurance] Risk assessments, the notion of ``due care,'' the notion of ``economy of mechanism,'' and engineering trade-offs are implied by the requirement for cost-effectiveness.

Chap.2(C)(4)

[Assurance] An effort (e.g., testing) must be made to ensure selected control techniques operate as intended. The degree of effort should reflect the sensitivity of the information or application in which the controls are intended to protect. Facility management procedures for installing and maintaining controls will be required.

Chap.2

(C)(5)(a-f)

[Assurance] A variety of Assurance features are listed to ensure the effectiveness of selected control techniques.

Chap.2(D)(1)

[Security Policy] The security policy must address, in clear and precise terms, the scope of resources which are applicable. Uniform terms should be used where possible.

Chap.2

(D)(2)(a-e)

[Security Policy] The Security Policy must address each of the five control areas which are applicable (input, output, processing, storage, and communications).

Chap.2

(D)(3)(a-b)

[Assurance] Assurance issues are raised by the integration of different controls and the dependence of controls upon other controls. System design should address these issues.

Chap.2(D)(4)

[Assurance] Responsibility should be assigned to address system-wide controls.

A.17 DoD Directive 7750.5-Management and Control of Information Requirements

This Directive implements the policies stated in DoD Directive 7740.1, DOD Information Resources Management Program and Public Law 96-511, Paperwork Reduction Act of 1980. Specifically, this Directive specifies administrative policies related to information requirements. This Directive applies to all internal, interagency, and public reporting DoD information requirements. All information systems and techniques for collecting, recording, maintaining, and disseminating information are included under its provision unless exempted under Public Law 96-511.

The following table contains selected sections of DoD Directive 7750.5. The cross-reference table and comments appear in the next section.

TABLE A-34. DoD Directive 7750.5-Selected Source Text

A. Purpose

1. This Directive prescribes policies for the management and control of information requirements. It also implements those policies in [DoD 7740.1-D] and [PRA 1980] concerning the licensing of reporting requirements internal and external to the Department of Defense and the development of an Information Collection Budget. . . .

D. Policy

1. Ensuring that sufficient information is available to achieve military effectiveness and management efficiency is a basic command and management responsibili-

ty. As a fundamental policy, however, the burden associated with the collection and reporting of this information must be controlled and minimized. The management of reports internally prescribed by the DoD component must include provisions for setting annual goals, consistent with critical mission needs, to reduce the number or frequency or reports.

2. The central ingredient in information management is the user's responsibility and accountability for assuring that information requirements are valid, accurate, and essential to the mission of the user's organization.

a. These requirements should be examined to avoid both duplication and unnecessary generation of data. Because the creation or collection of information requires the allocation of scarce resources, the user must first ascertain that the required data are not already available from other sources.

b. Statistical sampling techniques and information technology should be emphasized as approaches for minimizing reporting workloads.

c. In the development and operational life cycle of an automated information system, care shall be taken to assure that information needs are clearly identified and that reports to be generated by the automated system represent cost effective use of resources, as required by DoD Directive 7920.1 [Life Cycle Management of Automated Information Systems]

A.17.1 Cross-References and Comments

TABLE A-35. DoD Directive 7750.5-Cross-References

Section

Security Policy

MAC

DAC

Marking

Accountability

Assurance

Fault Tolerance

D(1)

X

D(2)

X

X

D(2)(a)

X

X

D(2)(b)

X

D(2)(c)

X

X

D(1)

[Security Policy] The sufficiency of information resources to achieve military effectiveness and management efficiency must be addressed. In addition to the concept of sufficiency, the burden associated with collecting and reporting information must be controlled and minimized.

D(2)

[Security Policy, Accountability] This policy statement supports the position that individuals are ultimately responsible for the information processing resources under their administration. Information processing resources and activities must be valid, accurate, and essential to the mission needs of the DoD component. This implies similar quality attributes for the operational aspects (e.g., data and processing properties) of the information resources which are used to fulfill component information requirements.

D(2)(a)

[Security Policy] The control of duplication and unnecessary generation of data is required. [Accountability] The user must ascertain that required information is not available by other means.

D(2)(b)

[Accountability] The minimization of reporting workload is required. The use of information technology to achieve this goal is explicitly mentioned.

D(2)(c)

[Security Policy, Accountability] The information needs of the DoD component must be identified and supporting AISs must be capable of meeting those needs. Reports generated by AISs must be cost effective.

APPENDIX B

B. POLICY CROSS-REFERENCE

The table appearing in this Appendix is a reproduction of Table 3.1 from the Department of Defense ADP Internal Control Guideline [DoD 7740.1-G]. This table ``provides a listing of 55 control requirements cross-referenced to the major control objectives . . ." [DoD 7740.1-G, p. 3-6]. Although this table does not provide cross-references for all of the policy statements used in this document, it does include the following:

· OMB Circular No. A-123, Internal Control Systems [OMB A-123];

· Internal Control Guidelines [OMB ICG];

· OMB Circular No. A-127, Financial Management Systems [OMB A-127];

· OMB Circular No. A-130, Management of Federal Information Resources [OMB A-130];

· GAO Policy and Procedures Manual for Guidance of Federal Agencies-Title 2 - Accounting [GAO Title II];

· Privacy Act of 1974 [PA 1974];

· Federal Managers' Financial Integrity Act of 1982 [FMFIA 1982];

· DoD Directive 5010.38, Internal Management Control Program [DoD 5010.38-D];

· DoD Directive 7740.1, DoD Information Resources Management Program [DoD 7740.1-D].

A set of 55 control requirements applying to the internal control of DoD components were derived from these seven documents. The table cross-references each control objective with the particular document(s) from which it was derived. The table contains a brief statement of each control requirement, while the full wording appears in a list following the table (also reproduced from [DoD 7740.1-G]). Four categories of requirements are cited: Application Controls, General Controls, Administrative Controls, and Required Systems Functions. Especially significant when considering integrity in AISs are those requirements listed under Application Controls and Required Systems Functions.

TABLE B-36. Summary of Control Requirements [DoD 7740.1-G]

Summary table of control objectives cross-referenced to the major control directives.

Line No.- Requirements

A-123

OMB IC

A-127

A-130

GAO Title II

FMFIA

Privacy Act

DoD IMCP

DoD IRMP

APPLICATION CONTROLS

1. Transactions are authorized

X

X

X

X

X

2. Transactions are valid

X

X

X

X

X

3. Information is complete

X

X

X

X

X

X

X

4. Information is accurate

X

X

X

X

X

X

X

X

5. Information is timely

X

X

X

X

X

X

X

6. System and data are secure

X

X

X

X

7. System is auditable

X

X

GENERAL CONTROLS

8. System controls exist

X

X

9. 5-yr. system plan developed

X

X

X

X

10. Contingency/disaster plan

X

X

X

11. Vulnerability assessment

X

X

X

X

12. Cost/benefit analysis

X

X

13. Reasonable assurance

X

X

X

X

X

X

X

14. Control objectives defined

X

X

X

X

15. Control techniques selected

X

X

X

X

16. Security reqs. adequacy

X

17. Security specs. exist

X

X

X

18. Security specs. adequacy

X

19. System design approved

X

X

20. Controls documented

X

X

X

21. System documentation exists

X

22. System contingency plan

X

X

23. Controls tested

X

X

24. System test conducted

X

25. Test results documented

X

X

26. System certified

X

27. Controls review performed

X

X

X

X

X

28. Periodic reviews

X

X

X

X

X

29. Periodic risk assessments

X

X

X

30. Corrective action/ audit

X

X

X

X

31. Internal controls report

X

X

X

X

32. Accounting systems report

X

X

X

33. Annual report to President

X

X

X

X

X

X

ADMIN. CONTROLS

34. Org. responsibility fixed

X

X

X

35. Separation of duty exists

X

X

X

X

36. Supervision is provided

X

X

X

X

37. Supportive attitude exists

X

X

X

X

38. Personnel are competent

X

X

X

X

39. Security training program

X

X

40. Written policies/ procedures

X

X

X

X

X

41. Personnel security policies

X

X

42. Ind. responsibilities fixed

X

X

X

X

X

X

43. Accountability assigned

X

X

X

X

X

X

X

44. Record retention procedures

X

X

45. Release of information

X

X

X

REQ. SYSTEM FUNCTIONS

46. System is efficient

X

X

X

47. System operation economical

X

	X			
48. System is effective				
	X			
	X			
	X			
49. System supports management				
	X			
	X			
	X			
50. System supports budget				
	X			
	X			
	X			
51. Comparability/ consistency				
	X			
	X			
52. Information useful/ relevant				
	X			
	X			
	X			
	X			
	X			
53. System provides disclosure				
	X			

X

X

54. Individual access
allowed

X

X

X

55. Network compatibility

X

B.1 Requirements List

The following list of requirements correspond with the summaries appearing in the first column of the preceding table.

Application Controls

1. Transactions are authorized - the information entered into the system must be authorized by management for entry.

2. Transactions are valid - the information system must process only data that represent legitimate events.

3. Information is complete - all valid data, and only those data, are to be processed by the information system.

4. Information is accurate - data must be free from error during all phases of processing, within defined levels of tolerance.

5. Information is timely - data must reflect the correct cycle, version, or period for the processing being performed. Financial management data shall be recorded as soon as practical after the occurrence of the event, and relevant preliminary data shall be made available promptly to managers after the end of the reporting period.

6. System and data are secure - the data files, computer program, and equipment must be secure from unauthorized and accidental changes, unauthorized disclosure and use, and physical destruction. Detective and corrective controls may also apply depending on the sensitivity and/or classification of the data.

7. System is auditable - an information trail must exist that establishes individual accountability for transactions and permits an analysis of breakdowns in the system and other anomalies.

General Controls

8. System controls exist - for each information system, the controls system should ensure that appropriate safeguards are incorporated into the systems, tested before implementation, and tested periodically after implementation.

9. Five-year system plan developed - a plan featuring specific milestones with obligation and outlay estimates for every system of the agency (both current and under development).

10. Contingency plan and/or disaster recovery plan exists - agencies shall develop, maintain, and test disaster recovery and continuity of operations plans for their data center(s). The plan's objective is to provide reasonable continuity of data processing support if normal operations are prevented.

11. Vulnerability assessment conducted - a review of the susceptibility of a program or function to waste, loss, unauthorized use, or misappropriation. Includes both vulnerability assessments or their equivalents, such as an audit.

12. Cost-benefit analysis exists - a review to determine and compare the benefits of the proposed system against the cost of developing and operating the current system. Only those proposals where the expected benefits exceed the estimated costs by 10 percent should be considered for development, unless otherwise specifically required by statute.

13. Reasonable assurance applied - reasonable assurance equates to a satisfactory level of confidence, based on management's judgment of the cost-benefits of the controls versus the recognized risks. (Practically, it is recognized that it is not cost-effective to attain 100 percent assurance.)

14. Control objectives defined - goals established to address a known vulnerability or promote reliability or security of a system.

15. Control techniques selected - methods to satisfy one or more control objectives by preventing, detecting, and/or correcting undesired events. More commonly referred to as "controls."

16. Adequacy of security requirements determined - agencies administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of facilities, equipment, or software.

17. Security specifications exist - internal control and security objectives must be stated as design specifications and approved by management before development (programming) of the application system can begin.

18. Adequacy of security specifications determined - proof that the design specifications satisfy control objectives must be presented to management to authorize computer program development and/or modification (programming).

19. System design approved - before development (programming) of the system is authorized, management must be assured that the system design satisfies the user's requirements and incorporates the control requirements. The design review must be documented and be available for examination.

20. Controls documented - internal control systems, including all transactions and significant events, are to be clearly documented and be readily available for examination.

21. System documentation exists - documentation that must reflect the current state of the system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

22. System contingency plan exists - plans must be developed, documented, and tested to ensure that users of the system can continue to perform essential functions in the event their information technology support is interrupted. The plan should also be consistent with the agency-wide disaster recovery plan.

23. Controls tested - before a new or modified system is placed into production status, the controls should be tested to prove that the controls operate as intended. The test results should be documented and sent to management for approval to implement the system.

24. System test conducted - before implementation of the system is authorized, evidence that the system operates as intended must be presented to management. This evidence must also include the results of controls testing. The test results must be documented and available for examination.

25. Test results documented - the documentation should demonstrate that the control and functionality requirements operate as intended.

26. System certified prior to implementation - before a system can be implemented, an agency official shall certify that the system meets all applicable Federal policies, regulations, and standards, as well as state that test results demonstrate that installed controls are adequate for examination.

27. Controls review performed - periodically, the controls of each system must be tested to determine if the controls still function as intended. The results of these tests must be documented and available for examination.

28. Periodic reviews and re-certifications are conducted at least every 3 years, agencies shall review applications and re-certify the adequacy of the safeguards. The re-certifications shall be documented and be available for review.

29. Periodic risk assessments are conducted - agencies shall conduct periodic risk assessments at each data center to provide a measure of the relative vulnerabilities and threats to the data center so that security resources can be effectively distributed to minimize potential loss.

30. Corrective action taken; audit findings resolved promptly - managers are to promptly evaluate audit findings and recommendations, determine proper corrective actions, and complete those actions.

31. Annual report on internal controls prepared - yearly, each agency must determine proper if its systems of internal controls are in compliance with the Comptroller General's standards.

32. Annual report on accounting systems prepared - yearly, each agency must determine if its accounting systems are in compliance with the Comptroller General's standards.

33. Annual reports to President sent - the head of each agency must sign both annual reports and transmit them to both the President and Congress.

Administrative Controls

34. Organizational responsibility is affixed - the assignment of responsibilities for planning, directing and controlling the controls evaluation process for the agency and/or segment is specified. The programs and functions conducted in each of the components have also been specified. The programs and functions conducted in each of the components have also been specified.

35. Separation of duties exists - key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

36. Supervision is provided - qualified and continuous supervision is to be provided to ensure that control requirements are met.

37. Supportive attitudes exist - managers and employees are to maintain and demonstrate a positive and supportive attitude toward controls at all times.

38. Personnel are competent - manager and employees are to have personnel and professional integrity and are to maintain a level of competence that allow them to accomplish their assigned duties, as well as understand the importance of developing and implementing good controls.

39. Security training program exists - agencies shall establish a security awareness and training program so that agency and contractor personnel involved with information systems are aware of their security responsibilities and know how to fulfill them.

40. Written policies and procedures exist - each agency shall establish administrative procedures to enforce the intended functioning of controls, including provisions that performance appraisals reflect execution of control-related responsibilities.

41. Personnel security policies exist - each agency should establish and manage personnel security procedures, including requirements for screening agency and contractor personnel designing, developing, operating, maintaining, or using the system. The level of screening depends on the sensitivity and/or classification of the system data.

42. Individual responsibilities are affixed - assignments or responsibility should be made for internal controls, accounting systems, and data center security on an 43. Custody and/or accountability assigned - the official whose function is supported by an information system is responsible and accountable for the products of the information system is responsible and accountable for the products of the information system.

44. Record disposition procedures exist - each agency must establish approved records disposition schedules which identify permanent data files and ensure their transfer to the National Archives and Record Administration.

45. Release of information provided for - each agency must have procedures in place so that information can be extracted from systems to meet requests made under the Privacy Act and Freedom of Information Act.

Required System Functions

46. An analysis of the ratio of outputs to inputs evaluated against an acceptable standard.

47. System operation is economical - uneconomical systems must be identified and phased out.

48. System is effective - periodically, each system should be reviewed to determine if the system still meets organizational needs.

49. System supports management - data shall be recorded and reported in a manner to facilitate carrying out the responsibilities of both program and administrative managers.

50. System supports budget - financial management data shall be recorded, stored, and reported to facilitate budget preparation, analysis, and execution.

51. Comparability and/or consistency provided for - financial management data shall be recorded and reported in the same manner throughout the agency, using uniform definitions that are synchronized with budgeting and used consistently for each reporting period.

52. Information is useful and/or relevant - data capture and reports shall be tailored to specific user needs, and if usage does not justify costs, data or reports shall be terminated.

53. System provides full disclosure - data shall be recorded and reported to provide users of the data with complete information about the subject of the report per OMB, Treasury, and Privacy Act standards.

54. Individual access allowed - systems must be able to extract any data contained in the data base about individuals to meet requests to see the data by that individual or his/her representative when required by the Privacy Act.

55. Network compatibility exists - any systems developed or acquired must be interoperable with any existing system that will be linked to the new system.

▲Top of Page