Department of Veterans Affairs
Washington, DC 20420

VA Directive 4900
Transmittal Sheet
June 28, 2004

INTERNAL CONTROLS FOR FINANCIAL AND FINANCIAL INTERFACING AUTOMATED INFORMATION SYSTEMS

1. REASON FOR ISSUE: This directive replaces the Department of Veterans Affairs (VA) Directive 4900, Management Control Over Financial Automated Information Systems, and rescinds VA Directive 4910, ADP Financial & Interfacing Systems Integrity.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive sets forth the policies and responsibilities for the management and oversight of internal controls for Office of Management (OM) automated information systems and their interfaces. OM systems include financial, procurement, budgetary, logistics and mixed systems.

a. This directive prescribes policy, responsibilities, references and definitions that VA program managers must follow to demonstrate the required internal controls over the development and maintenance of OM automated information systems within VA.

b. Requisite internal controls include General Controls and Application Controls.

c. This directive establishes the Systems Quality Assurance Service (SQAS) as the primary office for management and oversight of independent verification and validation (IV&V) activities and the internal control areas for OM systems developed, managed, maintained or contracted by OM and related system interfaces.

d. For OM systems and their interfaces that involve contracted IV&V services, SQAS will perform contract management services to include selection, establishment of commitments, oversight, tracking, and reviewing performance and results.

3. RESPONSIBLE OFFICE: The Office of Management, SQAS, is responsible for the material contained in this directive.

4. RELATED HANDBOOKS: Related handbooks will be issued in the near future.

5. RESCISSION: VA Directive 4900 dated July 8, 1994; and VA Directive 4910 dated July 8 1994.

CERTIFIED BY:

Robert N. McFarland
Assistant Secretary for
Information & Technology

BY DIRECTION OF THE
SECRETARY OF VETERANS AFFAIRS:

William H. Campbell
Assistant Secretary
for Management

Distribution: RPC
FD

INTERNAL CONTROLS FOR FINANCIAL AND FINANCIAL INTERFACING AUTOMATED INFORMATION SYSTEMS

1. PURPOSE

a. This directive sets forth policy and responsibilities for required internal controls for financial systems and other automated information systems. Internal controls form the core of the Federal Government's financial management standards. The Federal Managers' Financial Integrity Act of 1982 requires that VA systems and their interfaces comply with quality assurance processes that support functional, technical and internal controls (also referred to as management controls) requirements. VA internal controls include but are not limited to the following types:

(1) General Controls. Program Planning; Access Controls; Application Software Development and Change Controls; System Software; Segregation of Duties; and Service Continuity.

(2) Application Controls. Input Controls; Output Controls; Processing Controls; Security Controls; Documentation Controls; Storage Controls; and Communication Controls.

b. This directive applies to all Office of Management (OM) program managers and their organizations responsible for the management of federal funds. This directive addresses internal control policies used by management to support their assertions that the financial statements and reports for their program(s) are fairly presented, and represents the results of financial activities in accordance with governing legal requirements.

c. This directive establishes the Systems Quality Assurance Service (SQAS) as the office that manages and oversees independent verification and validation (IV&V) of internal controls for OM automated information systems (AISs) and their interfaces. Additionally, for OM systems and their interfaces that involve contracted IV&V services, SQAS will perform contract management services to include selection, establishment of commitments, oversight, tracking, and reviewing performance and results.

2. POLICY

a. All OM automated information systems and their interfaces shall execute internal controls, satisfy owner-specified requirements, and meet VA's security requirements as defined in the governing directives cited in paragraph 4 (References) of this directive. Program managers shall agree to institutionalize these internal controls into their program plan and schedule to cover the system development life cycle for their systems and applications.

b. Documentation of the internal controls and application security requirements shall reflect that requisite controls exist and application security requirements are satisfied as well as give reasonable assurance that the financial reports produced by the system present fairly the results of operations for each program.

c. All OM systems will follow a system development life cycle (SDLC). SDLC is the period of time that begins when a software product is conceived, and ends when the software is no longer available for use. According to the *IEEE-STD-1074*, a life cycle typically includes the following phases:

concept, requirements, design, implementation, test, installation and checkout, operation and maintenance, and sometimes a retirement phase. OM is currently operating under an approved SDLC that includes the following phases: Planning, Requirements, Design, Code & Unit Test, System & Integration Test, and Implementation.

d. All OM systems and their interfaces will have an assigned system criticality category and associated integrity level. System criticality is a description of the intended use and application of a system. System criticality descriptions denote a range of system integrity levels. System integrity levels and risk assessments are used to determine the appropriate level of IV&V activities.

e. To ensure overall systems integrity, the verification and validation of each OM system and ultimate certification of the appropriateness of internal controls will be accomplished organizationally independent from the elements that acquire, design, develop or maintain the OM system. In order to provide reasonable assurance that OM systems and associated interfacing systems and program processes are properly documented, efficient, reliable, available, and secure, SQAS will perform the following IV&V activities to assess and determine the effectiveness of internal controls:

(1) Systems Quality Assurance. The IV&V activity that provides for the systematic prevention of defects, identification of nonconformance to regulations and standards (includes application security compliance regarding the confidentiality, integrity and availability of data), identification of unsatisfactory trends and conditions, and correction of factors that may contribute to defective work processes or products.

(2) Systems Testing. The IV&V activity that conducts and/or oversees system engineering processes (testing includes black box/system, integration, regression, application security, load/stress, user/acceptance, etc.). It is focused on determining whether the product built satisfies the customers' requirements based on functional, performance and design specifications.

(3) Financial Systems Review. The IV&V activity that oversees compliance with Office of Management and Budget (OMB) Circular A-127. This circular prescribes policies and standards for executive departments and agencies to follow in operating, evaluating, and reporting on financial systems. The policies in OMB Circular A-127 are applicable to all VA financial systems.

3. RESPONSIBILITIES

a. Assistant Secretary for Management. The Chief Financial Officers (CFO) Act of 1990 and the Office of Federal Procurement Policy Regulations (title 41, chapter 7) mandate improved financial management (in part, by assigning clearer responsibility for leadership to senior officials and by requiring the establishment of CFO organizations in each agency), enhanced financial systems, audited financial statements and performance measurement reporting. Improving federal financial, budgetary, logistics, and mixed systems requires increased accountability for program managers to provide necessary information for better decision-making, and to improve the efficiency and effectiveness of services provided by the federal government. The Assistant Secretary for Management, as VA's Chief Financial Officer and Senior Procurement Executive, will develop policies and procedures to implement the provisions of the CFO Act of 1990 and the Office of Federal Procurement Policy Regulations (title 41, chapter 7) for improving management, enhancing systems, providing audited financial statements and reporting on performance measurement.

b. Under Secretaries, Assistant Secretaries, and Other Key Officials. Under Secretaries, Assistant Secretaries, and other key officials are responsible for:

(1) Ensuring that new OM AISs and their interfaces as well as major system modifications to existing AISs and their interfaces contain required internal controls and security measures in accordance with regulations, policies, and procedures;

(2) Reviewing and documenting current operational, undocumented systems for adequacy of internal controls;

(3) Ensuring documentation of internal controls in application software reflects compliance with established government directives, standards, and procedures;

(4) Ensuring certification of OM AISs and their interfaces are in conformance with the policies described by this directive;

(5) Establishing supplemental policies or guidelines, as necessary, to help ensure the integrity of OM AISs and their interfaces; and

(6) Monitoring compliance with the above-stated requirements on a regular basis.

c. OM Deputy Assistant Secretaries, Associate Deputy Assistant Secretaries, and Program Managers. OM Deputy Assistant Secretaries, Associate Deputy Assistant Secretaries, and program managers are responsible for:

(1) Ensuring that internal controls are an integral part of each program's entire cycle of planning, budgeting, program delivery or operations, accounting, and auditing processes;

(2) Ensuring that clear documentation for transactions, internal controls and other significant events is readily available for examination by SQAS;

(3) Assessing on a continuous basis the risks and external factors that may impair program delivery and operations;

(4) Periodically assessing, commensurate with the level of risk, the adequacy of internal controls for their respective programs and operations and documenting results;

(5) Identifying weaknesses in internal controls and developing corrective action plans for deficiencies;

(6) Disclosing internal control weaknesses to the next higher level of management;

(7) Ensuring that all deficiencies identified by SQAS are closed in a timely manner;

(8) Ensuring that all managers and employees are aware of the importance of internal controls as well as control objectives, program risks, and performance measures;

(9) Ensuring that OM systems are properly documented and in compliance with OMB and other government directives, standards and procedures (see paragraph 4);

(10) Ensuring supplemental policies or guidelines are established as necessary to ensure the integrity of OM systems and their interfaces; and

(11) Ensuring that testing of OM systems that interface with VA financial systems is coordinated with SQAS.

d. SQAS. SQAS will, at a minimum:

(1) Review OM AISs and their interfaces for compliance with applicable governing directives and VA policies;

(2) Perform IV&V of internal control areas for OM AISs and their interfaces that are developed, managed, maintained or contracted by OM;

(3) Conduct detailed financial system reviews of OM AISs and their interfaces, pursuant to OMB Circular A-127 "Financial Management Systems";

(4) Issue reports that reflect the status of program internal controls;

(5) Establish system quality assurance processes (e.g., conduct product reviews and phase audits, identify risks, defects and deviations);

(6) Identify, document and communicate system anomalies and defects (defects, deviations and recommendations are tracked to closure);

(7) Review program, project and system documentation and determine compliance with applicable governing directives and policies (conduct an ongoing review of programs and/or projects to ascertain compliance with required laws, directives and policies);

(8) With system owner approval, verify documentation related to application security for compliance with applicable policies, rules and regulations. Application security documentation includes but is not limited to the following: Threat Assessments, Risk Assessments, Security Requirements Traceability Matrices, Application Security Plans, Security Features User Guides;

(9) Participate as a non-voting member on all Change Control Boards for OM systems;

(10) Develop tests and/or perform integration, regression, and application access testing; and

(11) Certify systems are ready for production.

4. REFERENCES. This directive is issued pursuant to the governing requirements published by federal oversight agencies. Over the past decade, the General Accounting Office (GAO), OMB, and other federal entities, both internal and external to VA, have issued numerous directives that provide

guidance and requirements for the implementation of controls over federal AISs. The following list includes key references applicable to this directive:

a. General

(1) ADP Systems Integrity Guidelines published by the Office of Financial Management and ADP Systems Integrity, May 1993.

(2) Chief Financial Officers Act of 1990.

(3) Office of Federal Procurement Policy Regulations (title 41, chapter 7).

(4) Federal Managers' Financial Integrity Act of 1982.

(5) Framework for Federal Financial Management Systems, a Joint Financial Management Improvement Program (JFMIP) directive, FFMSR-0, January 1995.

(6) GAO/AIMD-00-21.2.3, Human Resources and Payroll Systems Requirements, Checklist for Reviewing Systems Under the Federal Financial Management Improvement Act of 1996, A GAO Exposure Draft, October 1999.

(7) GAO AIMD-12-19-6, Federal Information Systems Controls Audit Manual (FISCAM).

(8) GAO Policy and Procedures Manual for Guidance of Federal Agencies.

(9) JFMIP-SR-02-01, Core Financial System Requirements, a JFMIP directive, November 2001.

(10) JFMIP-SR-99-05, Human Resources & Payroll Systems Requirements, a JFMIP directive, April 1999.

(11) OMB Circular A-123, Internal Control Systems.

(12) OMB Circular A-127, Financial Management Systems.

(13) OMB Circular A-130, Management of Federal Information Systems Resources.

(14) Privacy Act of 1974.

b. IV&V

(1) IEEE Standard 1012-1998, Software Verification and Validation.

(2) IEEE Standard 1074-1995, Software Life Cycle Processes.

c. Security Compliance

(1) OMB A-130, Appendix III.

(2) Computer Security Act of 1987.

(3) The Federal Information Security Management Act of 2002 (FISMA).

(4) National Institute of Standards and Technology (NIST), Special Publications Computer Security Resource Center, 800 Series (http://csrc.nist.gov/publications/nistpubs/index.html).

d. VA Directives. Implementation of the policies stated in this directive are congruous with policies stated in the following VA directives.

(1) VA Directive 0070, Management Accountability and Control Program.

(2) VA Directive 4510, Financial Management Systems.

(3) VA Directive 6000, VA Information Resources Management (IRM) Framework.

(4) VA Directive 6212, Security of External Electronic Connections.

(5) VA Directive 6214, Information Technology Security Certification and Accreditation Program (ITSCAP).

(6) VA Directive 6500, Information Security Program.

5. DEFINITIONS

a. Independent Verification & Validation (IV&V). System verification and validation performed independently of the program office and development team for an automated information system. The purpose of IV&V is to help the program and development organizations to build quality into system software during the system development life cycle. IV&V activities determine whether development products conform to the requirements and whether the system software satisfies the intended use and specified needs of the user. IV&V is an extension of both program management and system engineering functions. Through assessment, analysis, evaluation, review, inspection and testing of software products, IV&V identifies objective data and conclusions about software quality, performance, application security, and schedule compliance for the program and development organizations. These results allow the program to modify the software products in a timely fashion and reduce project costs and schedule delays. This proactive approach of employing IV&V in parallel with the system development life cycle, enables programs to address anomalies and defects earlier throughout the life cycle rather than delaying discovery until the time of implementation, which results in greater program cost and schedule delays.

b. Internal controls. A set of controls that provides for checks and balances that guard against inefficient or ineffective practices. These controls are designed to provide reasonable assurance that:

(1) Operations, including the use of agency resources, are effective and efficient;

(2) Financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, is reliable; and

(3) Applicable laws and regulations are followed.

Internal controls also include the safeguarding of agency assets against unauthorized acquisition, use or disposition.

c. Management controls. Policies and procedures used to provide reasonable assurance that:

(1) Programs achieve their intended results;

(2) Resources are used consistent with the organization's mission;

(3) Programs and resources are protected from waste, fraud, and mismanagement;

(4) Laws and regulations are followed; and

(5) Reliable and timely information is obtained, maintained, reported and used for decision-making.

The term "management controls" is interchangeable with the term "internal controls."

d. Project Planning. Project planning is the activity that provides reasonable estimates regarding resources, costs and schedules. Planning activities include establishing the scope and objectives of the project; identifying and defining required staffing, roles and responsibilities; scheduling, estimating, tracking and monitoring; and using appropriate tools and techniques to accomplish project objectives.

e. Reasonable Assurance. This term refers to a concept used to judge the effectiveness and efficiency of management controls developed by management to achieve program objectives.

f. Software Quality Assurance. Software quality assurance consists of a planned and systematic set of activities that provide adequate confidence that products and services satisfy technical, functional, application security and internal controls specifications. Software quality assurance activities include reviewing, testing, developing standards and metrics, and generating reports for monitoring the software.

g. Systems and Data Integrity. Systems and data integrity provides the assurance that each system employs adequate control over data received, processed, retrieved, reported and stored. Additionally, that such data is complete, secure and free from internal and external contamination from improper processing or breach of security, with proper reporting capabilities of all data and system activities.

h. Validation. Validation is the determination of the correctness of the final program or software produced from a development project with respect to customer needs and requirements. Examples of validation activities include integration, system, application security and regression testing.

i. Verification. Verification is the demonstration of consistency, completeness and correctness at each stage of the system development life cycle. Examples of verification activities include walk-throughs, reconciliations, and technical, product and managerial reviews.