

### **SECTION 3**

#### **CHAPTER 1**

#### **OVERVIEW**

In accordance with 340 DM §1.5.F, this section of the Internal Control and Audit Follow-up Handbook is designed to provide guidance and establish policy and process procedures for the information technology and information security community, within the Department of the Interior, for conducting the necessary Internal Control Reviews (ICRs) for information systems and Information Technology (IT) programs.

As identified in the Federal Regulations and OMB circulars, referenced in Addendum B, the Department of the Interior is required to conduct an ongoing review of internal controls and report annually on the adequacy of the department's program and operation internal control systems.

A major part of the ongoing review process of internal controls includes agency program management, financial management, and the supporting information systems and networks. All information systems (otherwise known as Major Applications and General Support Systems) shall undergo an ICR annually to comply with the regulation(s) and OMB directives identified herein. The ICR of information systems and IT programs directly supports and substantiates the annual assurance statement signed by the Secretary of the Interior.

It is paramount that bureaus and offices streamline their ICRs with their system and reporting requirements to facilitate more efficient reporting and use of their financial and human resources. Internal review processes and reporting requirements shall be evaluated to identify overlap and to facilitate eliminating or streamlining of those reviews that can satisfy multiple requirements.

This section provides detailed guidance for conducting ICRs of information systems. This section also details roles and responsibilities and fiscal year activity dates.

For the purposes of this section, the following acronyms and terms are defined for use.

- I. OCIO – Office of the Chief Information Officer, an organization under the Office of the Secretary.
- II. CSD – Cyber Security Division, an organization under the Office of the Chief Information Officer.
- III. OCIO ICR Coordinator – A designated “ICR” official in the Cyber Security Division of the OCIO.

**SECTION 3**  
**CHAPTER 2**  
**ROLES AND RESPONSIBILITIES POLICY**

Bureau and Office Directors have the overall responsibility to monitor bureau progress associated with the mitigation of material weaknesses, non-compliance issues, and other problem areas identified in OIG, GAO, Departmental, and independent reviews. To facilitate the correction of the identified problem areas, an "early warning system" shall be developed for the internal control and audit follow-up program to ensure that Departmental Management is advised of impending problems and recommended solutions that shall ensure that the bureau can complete remedial actions planned for the current fiscal year. This system shall include the Plan of Actions and Milestones (POA&M) process.

The following roles and responsibilities are defined for the ICRs of information systems and IT programs:

- A. Departmental Chief Information Officer - Responsible for the overall ICR program of information systems and IT programs for the department. Provides the department level assurance statement to the Secretary of the Interior.
- B. OCIO ICR Coordinator - Responsible for the annual guidance, support, compliance, and Department level reporting relating to ICRs of information systems and IT programs for the Department. This position is designated to a member of the Cyber Security Division in the Office of the Chief Information Officer.
- C. Bureau and Office Chief Information Officers - Responsible for the overall ICRs of information systems and IT programs within their respective bureau or office.
- D. Bureau and Office IT Security Managers - Responsible for the integrity and quality of ICRs of information systems and IT programs within their respective bureau or office. Responsible for ensuring that weaknesses are tracked and managed in accordance with regulation, policy, and the POA&M process.
- E. System Owners - Responsible for certifying the results of ICRs for their assigned information systems and IT programs.
- F. System Managers - Responsible for approving the results of ICRs for their assigned information systems and IT programs.
- G. System Security Officers - Responsible for planning and conducting ICRs of their assigned information systems and IT programs.

**SECTION 3**  
**CHAPTER 3**  
**EXECUTING INTERNAL CONTROL REVIEWS FOR INFORMATION SYSTEMS & IT PROGRAMS**

1. Policy: Internal Control Reviews (ICRs) of all information systems and Information Technology (IT) programs shall be conducted on an annual basis in accordance with and in support of Federal Managers' Financial Integrity Act of 1982, OMB Circular A-123, Federal Information Security Management Act of 2002, OMB Circular A-130, NIST Special Publications 800-26, 800-37, and 800-53.
2. Scope: All Department information systems and IT programs.
3. Definitions:
  - 3.1. The term “information system” refers to either a major application or general support system with a defined security accreditation boundary as described in the NIST “Certification and Accreditation Guide” (NIST Special Publication 800-37).
    - 3.1.1. The term “major application” means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other application should be provided by security of the system in which they operate (either a major application or general support system). Source: OMB A-130 Appendix III
    - 3.1.2. The term “general support system” or “system” means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). Source: OMB A-130 Appendix III
    - 3.1.3. The process of uniquely assigning information resources (“information resources” consist of information and related resources, such as personnel, equipment, funds, and information technology) to an information system defines the “security accreditation boundary” for that system. Source: NIST Special Publication 800-37
    - 3.1.4. Material Weakness – A reportable condition, or combination of

reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. (IC-8)

3.1.5. Non-conformance – A condition in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially relate (or mixed) systems. The OIG often terms this as a NONCompliance issue. (IC-8)

3.1.6. Nonmaterial weaknesses – Control problems that can be corrected at the bureau/office level without the approval or attention of the next higher level or management. (IC-8)

4. Policy & Process:

\* Note: If the dates provided in the policy and process do not fall on a business day, the next business day should be used.

4.1. The OCIO ICR Coordinator shall distribute the revised assessment template and guidance document for completing the template; and shall issue a complete listing of information systems to all bureaus and offices for reconciling and baselining the information systems to be reviewed. This shall be completed during the month of January.

4.1.1. Any discrepancies between the distributed list and bureau and office lists shall be immediately resolved, and any necessary updates completed.

4.2. The Bureau and Office Chief Information Officers shall immediately begin formalizing and executing plans to review all of the information systems and IT program(s) under their responsibility. Plans shall be submitted by each Bureau and Office Chief Information Officer to the OCIO ICR Coordinator by March 1<sup>st</sup>.

4.2.1. The plans shall include all information systems and IT program(s) for the bureau or office.

4.2.2. The plans shall include a reasonable schedule with defined dates and the appropriate designated resources for each of the major functions of the ICR.

4.2.3. The plans shall demonstrate a schedule that meets the date requirements for delivery of the reports to the department.

4.3. ICRs for all Information Systems and IT programs shall be completed and submitted to the OCIO ICR Coordinator by June 1<sup>st</sup>.

4.3.1. The ICR of each Information System shall include:

4.3.2. a completed NIST Special Publication 800-26, or a revised 800-26 self assessment questionnaire;

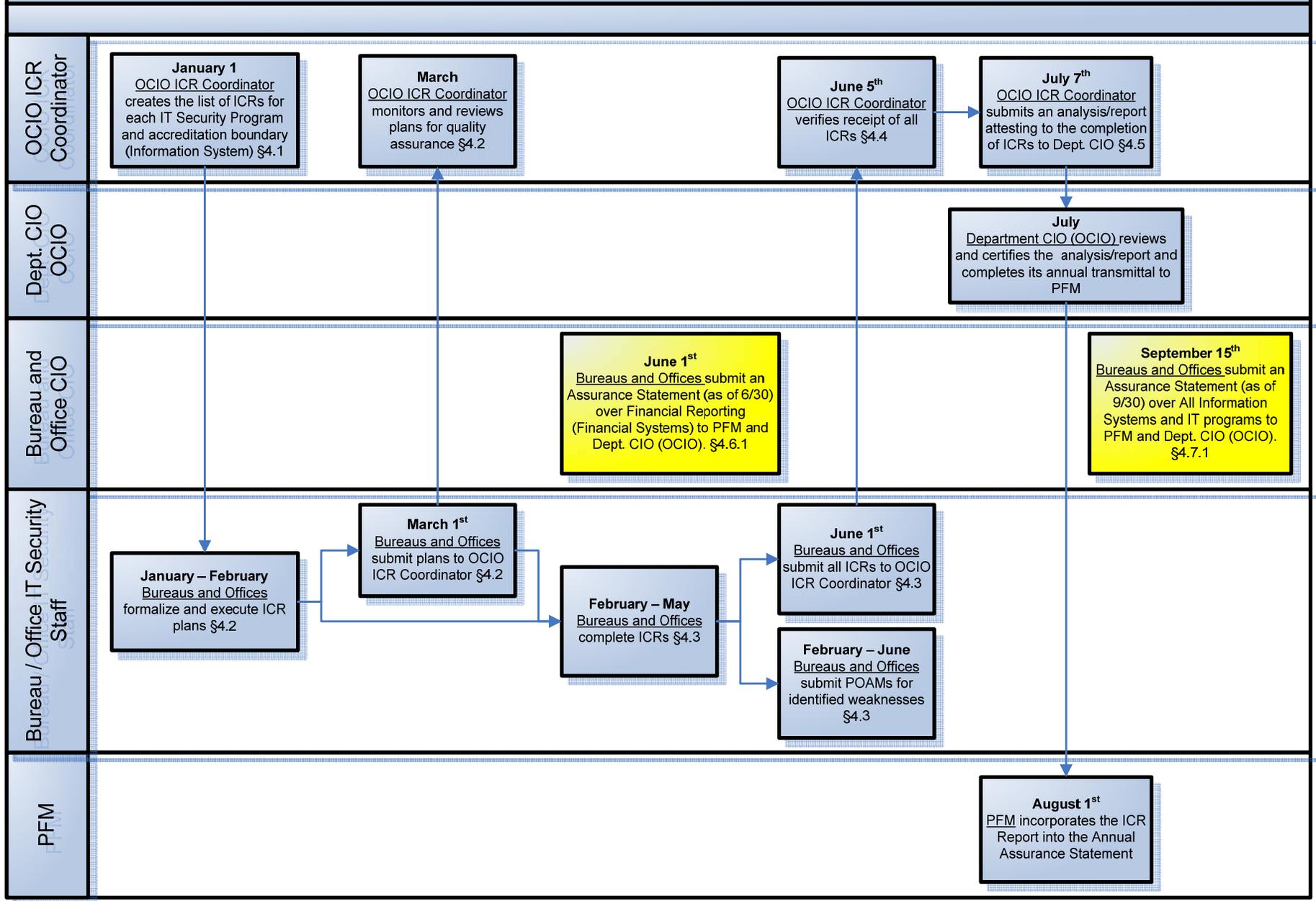
- 4.3.2.1. The guidance and instructions in NIST Special Publication shall be followed to ascertain and conclude the maturity level of the program and information systems for each control area.
- 4.3.3. A statement letter of “No Weaknesses” or “Weaknesses Found.” Statement letters shall be addressed to the Departmental CIO and OCIO ICR Coordinator. A separate statement letter shall be completed for each individual Information System and IT program.
  - 4.3.3.1. All Material Weaknesses, Non-conformance, and Nonmaterial Weaknesses found shall be recorded in the statement letter and recorded in the respective Information System or IT program Plan of Actions and Milestone (POA&M) report.
    - 4.3.3.1.1. A POA&M is used to identify, prioritize, and manage corrective efforts associated with the mitigation of security weaknesses identified in a system or program. It is also used to report the status of security weakness remediation efforts to OMB and Congress.
    - 4.3.3.1.2. A POA&M entry shall be made for each weakness and shall include the related corrective actions, the scheduled completion date for correcting each weakness, and the status for correcting each weakness.
- 4.4. The OCIO ICR Coordinator shall validate that ICRs have been submitted for each system identified in the list completed in §4.1. This shall be completed by June 5<sup>th</sup>. Any missing ICRs shall be announced to the respective Bureau or Office IT Security Manager and Bureau or Office Chief Information Officer.
- 4.5. The OCIO ICR Coordinator shall assess all ICRs for quality and completeness with the respective System Security Officers, System Managers, Systems Owners, and Bureau and Office IT Security Managers. This quality review shall be completed by July 1<sup>st</sup>. Within 7 business days, a letter from the OCIO ICR Coordinator, addressed to the Departmental Chief Information Officer, shall attest that all ICRs have been completed for information systems and IT programs, and all ICRs shall be included in the transmittal.

#### Bureau and Office Assurance Statements

- 4.6. All bureau and office ICRs over financial reporting shall be completed on or before June 1<sup>st</sup>. This includes required reviews for financial information systems. Bureaus’ and offices’ assurance statements over financial reporting as of June 30<sup>th</sup> must be submitted to PFM on or before June 1. The assurance statement must address compliance with FFMIA for financial Information Systems. (PFM Guidance)

- 4.6.1. POLICY: On or before June 1<sup>st</sup>, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for financial information systems.
- 4.7. All reviews of non-financial programs or operations planned shall be completed on or before August 31<sup>st</sup>. Bureaus' and offices' annual assurance statement over all programs and operations, including Information Systems, as of September 30<sup>th</sup>, must be submitted to PFM on or before September 15<sup>th</sup>. This statement should include an update to the June 30<sup>th</sup> assurance statement over financial reporting which verifies that key financial reporting controls either have no reportable changes between June 30<sup>th</sup>, and September 30<sup>th</sup>, or reportable material weaknesses have been corrected. (PFM Guidance)
- 4.7.1. POLICY: On or before September 15<sup>th</sup>, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for all Information Systems and IT programs reviewed, and any updates from the June 30<sup>th</sup> assurance statement.

# Internal Control Reviews for Information Systems and IT Programs – November 10<sup>th</sup>, 2005 Rev 2.1



**SECTION 3**  
**Addendum B -**  
**Statutory and OMB Requirements Outline**

Federal Regulations

**1. FISMA (Federal Information Security Management Act of 2002)**

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include:

- **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
- **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- **A process for planning, implementing, evaluating, and documenting** remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;
- **Procedures for detecting, reporting, and responding** to security incidents; and
- **Plans and procedures to ensure continuity of operations** for information systems that support the operations and assets of the agency.

44 U.S.C. §§ 3541, 3544

§ 3541 Purpose

The purpose of FISMA is to:

- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

§ 3544 Federal agency responsibilities

The head of each agency shall

- (a)(1) be responsible for

- (A) providing information security protections;
- (B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
- (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

- (2) ensure that senior agency officials provide information security for the information and information systems that support the operations assets under their control, including through;

- (A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;
- (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards for information security classifications;
- (C) implementing policies and procedures to reduce risks to an acceptable level; and
- (D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

- (3) delegate to the agency CIO the authority to ensure compliance with the requirements imposed on the agency, including:

- (A) **CISO** - designating a senior agency information security officer;
- (B) **Security Program** - developing and maintaining an agencywide information security program;
- (C) **Policies** - developing and maintaining information security policies, procedures, and control techniques;
- (D) **Training** - training and overseeing personnel with significant responsibilities; and
- (E) assisting senior agency officials concerning their responsibilities.

- (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements

- (5) ensure **CIO reports annually** to the agency head on the effectiveness of the agency information security program

- (b) implement information security program that includes

- (1) **Risk Assessment** - periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency

- (6) **POA&M** - a process for planning, implementing, evaluating, and documenting

- remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency
- (7) **Incident Response** - procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued
- (c) **Agency Reporting** - each agency shall
- (1) report annually on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements
  - (2) address the adequacy and effectiveness of information security policies, procedures, and practices
  - (3) report any significant deficiency in a policy, procedure, or practice identified
- (d) **Performance Plan**
- (1) each agency shall include a description of (A) the time periods, and (B) the resources, including budget, staffing, and training, that are necessary to implement the program.
  - (2) The description shall be based on the risk assessment.

## 2. OMB Circular A-130

OMB A-130 establishes “security guidance” for Federal systems, issued in response to the Paperwork Reduction Act of 1980 (P.L. 104-13 and 44 U.S.C. Chapter 35, which established “a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner”).

- a. A minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123
- b. Authorization of a system to process information. By authorizing a system, a manager accepts the risk association with it. Management authorization is based on an assessment of management, operational, and technical controls

### OMB Circular A-130 Appendix III

#### A. Requirements

1. Purpose – establishes a minimum set of controls to be included in Federal automated information security programs
2. Definitions
3. Automated Information Security Programs. Implement policies, standards and procedures. At a minimum, agency programs shall include the following controls in their general support systems and major applications:
  - a. General Support Systems
    - 1) Assign Responsibility for Security.
    - 2) System Security Plan. Shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35). Security plans shall include:

a) Rules of the System.	b) Training.
c) Personnel Controls.	d) Incident Response Capability.
e) Continuity of Support.	f) Technical Security.
g) System Interconnection.	

- 3) Review of Security Controls. When significant modifications are made to the system, but at least every three years.
- 4) Authorize Processing. Use of the system shall be re-authorized at least every three years.

b. Major Applications

- 1) Assign Responsibility for Security.
- 2) Application Security Plan. Shall be incorporated into the strategic IRM plan required by the PRA. Application security plans shall include:

a) Application Rules.	b) Specialized Training.
c) Personnel Security.	d) Contingency Planning.
e) Technical Controls.	f) Information Sharing.
g) Public Access Controls.	

- 3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years.
- 4) Authorize Processing.

4. Assignment of Responsibilities.

5. Correction of Deficiencies and Reports

- a. Agencies shall correct deficiencies which are identified through the reviews.
- b. **Reports on Deficiencies.** In accordance with OMB Circular A-123, material deficiencies shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the agency level.
- c. **Summaries of Security Plans.** Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act.

**3. GISRA (Government Information Security Reform Act of 2000)**

FISMA replaced GISRA.

**4. CSA (Computer Security Act of 1987)**

FISMA repealed CSA.

**5. ITMRA (Information Technology Management Reform Act of 1996) / CCA (Clinger-Cohen Act)**

ITMRA/CCA assigns the head of each agency the responsibility to assess Information Technology (IT) resources and makes him/her responsible for effectively managing the risks of IT investments. Recent amendments to this CCA included in the Intelligence Reform and Terrorism Prevention Act of 2004 have created mandatory security responsibilities for the agencies and their CIO.

- a. Requires an inventory of all computer equipment under agency's control; and maintenance of an inventory of any such equipment that is excess or surplus property.
- b. Includes security as a requirement for systems planning and acquisition by agencies.
- c. Provides OMB greater authority in guiding agencies on information security issues, with some specific exemptions.
- d. Codifies the Chief Information Officer responsibility for the security of the information technology architecture.

#### **6. OMB Circular A-11, Preparation, Submission, and Execution of the Budget**

OMB A-11 provides guidance to agencies on how to prepare annual budget submissions. Part 1 provides an overview of the budget process. Part 2 covers development of the President's Budget and describes how to prepare and submit materials required for OMB and Presidential review of agency requests and for formulation of the FY 2007 Budget, including development and submission of performance budgets for FY 2007. The performance budget replaces the annual performance plan required by the Government Performance and Results Act.

- a. Submit a Report on Information Technology to OMB (OMB Circular A-11, Exhibit 53). Per Exhibit 53, agencies are required to have major IT investments within 10% of cost, schedule, and performance objectives.
- b. Submit an OMB Circular A-11 Exhibit 300 for each major IT system. Exhibit 300 requires information on plans and justifications for major acquisitions as identified in OMB Circular A-11, Section 300: Any information technology system reported as a major system in Exhibit 53 (Parts 1, 2, 3, and 4) must also be reported on Exhibit 300;
- c. Ensure information and systems are secure and that security is part of the management of the process from initial concept and throughout the entire life cycle of the investment. Agencies must also protect privacy in a manner consistent with relevant laws and OMB policies, including privacy impact assessments where appropriate.

#### **7. FMFIA (Federal Managers Financial Integrity Act of 1982) (31 U.S.C. 3512 et seq.)**

FMFIA requires agencies to establish and maintain internal control. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations.

Evaluate and report annually on the control and security of financial systems contained within each agency.

Amendment to the Accounting and Auditing Act to require ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control.

(d)(2) OMB shall establish guidelines for the evaluation by agencies of their systems of internal accounting and administrative control to determine such systems' compliance with requirements.

(3) By December 31 of each year, 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; or

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

(4) ...include a report in which any material weaknesses in the agency's systems of internal accounting and administrative control are identified and the plans and schedule for correcting any such weakness are described.

### **8. OMB Circular A-123, Management's Responsibility for Internal Control**

OMB Circular A-123 provides guidance to agencies and Federal Managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control to meet the requirements of the Federal Managers' Financial Integrity Act (FMFIA) of 1982, OMB revised internal controls in Section II to better align with current standards.

- a. Identifies security as a necessary component to all internal controls. Specifically, "the safeguarding of assets is a subset of all of those objectives." Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of assets;
- b. Requires a separate section (Section III) and a listing of statutes for agencies to consider when assessing internal control; and
- c. Introduces a new assurance statement on the effectiveness of internal control over financial reporting, which will be a subset of the overall FMFIA assurance statement.

### **9. OMB Circular A-127, Financial Management Systems**

OMB A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.

### **10. FFMIA (Federal Financial Management Improvement Act of 1996) (31 U.S.C. 3512)**

FFMIA requires agencies to have financial management systems that substantially comply with the Federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (SGL) at the transaction level. Financial management systems shall have general

and application controls in place in order to support management decisions by providing timely and reliable data.

- a. Develop and implement general and application controls compliant with guidance provided by FASAB and SGL;
- b. Make a determination annually about whether the agency's financial management systems substantially comply with FFMIA; and
- c. Develop a remediation plan if systems are found to be non-compliant with FFMIA, and determine whether the deficiencies must be reported pursuant to FFMIA.

### **11. PRA (Paperwork Reduction Act)**

Amended by GPEA.

### **12. GPEA (Government Paperwork Elimination Act)**

GPEA enacted to make government service delivery more efficient while ensuring baseline standards for electronic signatures across federal agencies.

Perform business case analysis, cost/benefit analyses, technology assessments, and risk assessments to determine which technologies, systems, and procedures best support compliance with GPEA.

### **13. GPRA (Government Performance and Results Act)**

GPRA requires strategic plans and goals to be integrated into: (i) the budget process; (ii) the operational management of agencies and programs; and (iii) accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. The primary purpose is to assess program effectiveness and improve program performance.

Develop strategic plans, set performance goals, and report annually on actual performance compared to the goals relating to agency budget, operational management, and reporting to the public on performance results

## National Institute of Standards and Technology

14. **800-16** Information Technology Security Training Requirements: A Role and Performance-Based Model
15. **800-18** Guide for Developing Security Plans for Information Technology Systems
16. **800-23** Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
17. **800-26** Self-Assessment Guide for Information Technology Systems
18. **800-30** Risk Management Guide for Information Technology Systems

19. **800-34** Contingency Planning Guide for Information Technology Systems
20. **800-37** Guide for the Security Certification and Accreditation of Federal Information Systems
21. **800-47** Security Guide for Interconnecting Information Technology Systems
22. **800-50** Building an Information Technology Security Awareness and Training Program
23. **800-53** Recommended Security Controls for Federal Information Systems
24. **800-55** Security Metrics Guide for Information Technology Systems
25. **800-60** Guide for Mapping Types of Information and Information Systems to Security Categories
26. **800-61** Computer Security Incident Handling Guide
27. **800-64** Security Considerations in the Information System Development Life Cycle
28. **800-65** Integrating Security into the Capital Planning and Investment Control Process

**S E C T I O N 3**  
**Addendum C - REPORTING REQUIREMENTS**

**1. FISMA**

- a. What: Annual reporting defined in OMB memorandum (2005: M-05-15)
- b. Who: OMB M-05-15
  - section A – no reporting
  - section B – Agency CIO (delegated to CSD, OCIO)
  - section C – IG
  - section D – Privacy Officer
- c. When: Annually at the end of the fiscal year (2005: October 7, 2005)
- d. How: Using the OMB Guidance and Excel template, completed and transmitted (hard copy and electronic). Tools used to gather inputs for section B include DEAR, Command Center C&A module, DOI CIRC, Department policy, online training reports, and data calls using various office automation tools include Word and Excel.

**2. OMB A-130 Appendix III**

- a. What: No extra reporting requirements.
- b. Who: N/A
- c. When: N/A
- d. How: N/A

**5. ITMRA/CCA**

- a. What: No extra agency reports required.
- b. Who: N/A
- c. When: N/A
- d. How: N/A

**6. OMB A-11**

- a. What:
  - 1) Report on resources for financial management activities (Exhibit 52).
  - 2) Submit a Report on Information Technology to OMB (Exhibit 53).
  - 3) Submit an Exhibit 300 for each major IT system. Any information technology system reported as a major system in Exhibit 53 (Parts 1, 2, 3, and 4) must also be reported on Exhibit 300.
- b. Who:
  - 1)
  - 2)
  - 3)
- c. When: 1)

- 2)
- 3) 2005: August 30, 2005 [?]

- d. How: 1)  
2)  
3)

#### **7. FMFIA**

- a. What: Statement that the agency's systems of internal accounting and administrative control fully comply with requirements
- b. Who: Department Secretary
- c. When: Annually, September 30
- d. How: The Assistant Secretaries provide a statement to PMB for each Bureau

#### **8. A-123**

- a. What: Assurance statement of internal control along with a report on identified material weaknesses and corrective actions.
  - 1) Bureaus/Offices submit material weakness corrective action progress and OIG and GAO audit recommendation implementation status reports
- b. Who: Department Secretary
  - 1) Bureau/Office management director and/or Assistant Secretary if appropriate.
- c. When: Appendix A is due to OMB June 30  
September 30 weaknesses are updated
  - 1) monthly for audited financial statement material weakness and noncompliance issues
  - 1) Quarterly ( January, April, July, and September) for non financial statement weaknesses
- d. How: The assurance statement is submitted in PAR
  - 1) Bureaus/Offices submit quarterly status reports to PFM

#### **9. A-127**

- a. What: No specific reporting requirements.
- b. Who: N/A
- c. When: N/A
- d. How: N/A

#### **10. FFMIA**

- a. What: Report to the Congress regarding implementation of FFMIA
  - b. Who: (a) Agency Director  
(b) Inspector General  
(c) Comptroller General
  - c. When: (a) Annually, by March 311  
(b) [?]
-

(c) Annually, by October 1

d. How: [?]

# Statutory and OMB Requirements Traceability Matrix

Replaced /Notes	Applies to all Federal Systems				Repealed by FISMA	Internal Control Reviews	FMFIA Guidance	Pursuant to FMFIA / Financial Mgmt Systems	External Audits	Amends to PRA	12. GPEA	13. GPRA
	1. FISMA	2. A-130	3. GISRA	4. CSA								
1. FISMA												
2. OMB A-130				REQ	REQ	REF	REF	REF		REQ	REQ	REQ
2e. M-05-15	REQ	REF			REF			REF				
5. ITMRA/CCA												
6. A-11	REF	REF			REQ					REF	REF	REF
7. FMFIA												
8. A-123							REQ					
9. A-127		REF					REQ					
10. FFMIA												
14. 800-16		REQ		REQ								
15. 800-18		REQ		REQ								
16. 800-23		REQ		REQ								
17. 800-26	REQ	REQ	REQ	REQ	REC	REQ	MCR					
18. 800-30	REQ	REQ	REQ	REQ	REQ							
19. 800-34		REQ		REQ	REQ							
20. 800-37	REQ	REQ			REF					REF		
21. 800-47		REQ		REQ	REQ							
22. 800-50	REQ	REQ										
23. 800-53	REQ	REQ										
24. 800-55	REQ	REQ	REQ		REQ	REQ	MCR				REQ	REQ
25. 800-60	REQ	REQ										
26. 800-61	REQ	REQ										
27. 800-64	REQ	REQ			REF							
28. 800-65	REQ	REQ			REF	REC						

REQ	Required by LAW
REQ	Required
REC	Recommended
REF	Referenced
PREREQ	Prerequisite to X
OPT	Optional;

# NIST Requirements Traceability Matrix – Continued

	800-16	800-18	800-23	800-26	800-30	800-34	800-37	800-47	800-50	800-53	800-55	800-60	800-61
14. 800-16													
15. 800-18													
16. 800-23													
17. 800-26		PREREQ		REF									
18. 800-30		REF											
19. 800-34					REF								
20. 800-37		REF				REF		REF	REF				REF
21. 800-47		REF							REF				
22. 800-50	REF												
23. 800-53		REF		REF	REF		REF					REF	
24. 800-55				REF									
25. 800-60		PREREQ		PREREQ	PREREQ		PREREQ			PREREQ			
26. 800-61					REF								
27. 800-64					REF								
28. 800-65				REF	REF					REF	REF		

	800-64	800-65	800-70	FIPS	FIPS 87	FIPS 199	FIPS 200	FIPS 201	FPC 65	PDD	PDD 67	PDD 63	FEMA/ FRP
14. 800-16													
15. 800-18													
16. 800-23													
17. 800-26													
18. 800-30				REF									
19. 800-34					OPT				OPT		OPT	OPT	OPT
20. 800-37			REF					REF					
21. 800-47													
22. 800-50													
23. 800-53						REF	REF						
24. 800-55				REF						REF			
25. 800-60						REF	REF					OPT	
26. 800-61													
27. 800-64													
28. 800-65													

REQ	Required by LAW
REQ	Required
REC	Recommended
REF	Referenced
PREREQ	Prerequisite to X
OPT	Optional;