MANAGEMENT CONTROLS

The Department of Commerce's senior leaders are responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA). The Department is able to provide a qualified statement of assurance that the internal controls and financial management systems meet the objectives of FMFIA, with the exception of one material weakness as discussed below.

The Department conducted its assessment of the effectiveness of internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations in accordance with OMB Circular A-123, *Management's Responsibility for Internal Control*. Based on the results of this evaluation, as of September 30, 2007, the Department identified one material weakness in internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations. This material weakness involves information technology security issues and the need to improve the quality of certification and accreditation processes and documentation for information technology systems. Other than this exception, the internal controls were operating effectively, and no other material weakness was found.

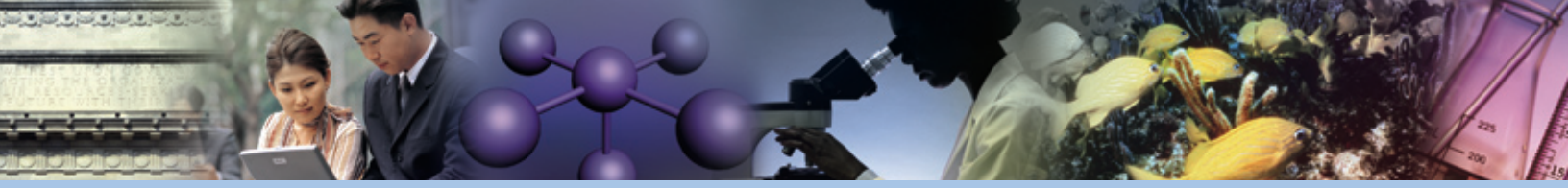
In addition, the Department conducted its assessment of the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with the requirements of Appendix A of OMB Circular A-123. Based on the results of this evaluation, the Department can provide reasonable assurance that its internal control over financial reporting as of June 30, 2007, was operating effectively and no material weaknesses were found in the design or operation of the internal control over financial reporting. Further, no material weaknesses related to internal control over financial reporting were identified between July 1, 2007 and September 30, 2007.

Carlos M. Gutierrez
Secretary of Commerce
November 15, 2007

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT (FMFIA) OF 1982

During FY 2007, the Department reviewed its management control system in accordance with the requirements of FMFIA, and Office of Management and Budget (OMB) and Departmental guidelines. The objective of the Department's management control system is to provide reasonable assurance that:

- obligations and costs are in compliance with applicable laws;
- assets are safeguarded against waste, loss, and unauthorized use of appropriations;
- revenues and expenditures applicable to Agency operations are properly recorded and accounted for, permitting accurate accounts, reliable financial reports, and full accountability for assets; and
- programs are efficiently and effectively carried out in accordance with applicable laws and management policy.



Section 2 of the FMFIA – Internal Management Controls

Section 2 of the FMFIA requires that federal agencies report, on the basis of annual assessments, any material weaknesses that have been identified in connection with their internal and administrative controls. The efficiency of the Department's operations is continually evaluated using information obtained from reviews conducted by the Government Accountability Office (GAO) and the Office of Inspector General (OIG), and specifically requested studies.

The diverse reviews that took place during FY 2007 relative to nonfinancial controls provide assurance that the Department's systems and management controls comply with standards established under FMFIA, with the exception of one material weakness. As discussed in detail below, this material weakness involves information technology (IT) security issues and the need to improve the quality of certification and accreditation (C&A) processes and documentation for IT systems. See Appendix D for summary of material weaknesses reported under Section 2 of FMFIA.

Department-wide Enhancements to IT Security Continue

Given the continuing significant focus across the federal government, in general, and the Department, specifically, on the need for effective cyber security and the protection of sensitive information, the Department continued working assiduously to enhance its IT security program during FY 2007.

In addition to other improvements made in recent years, the Department has adopted a comprehensive approach to IT security by utilizing enterprise architecture and governance to address security matters from the earliest stages of an IT investment's lifecycle. By fully considering IT security needs and building on the collective strength of its operating units, the Department has implemented an IT risk management model that combines centralized and decentralized processes in a way that ensures an appropriate level of standardization, but not at the expense of innovation. This cohesive and coordinated approach is critical to overcoming IT security deficiencies that have burdened the Department for the last several years.

Consistent and vocal support from senior leadership has enabled the Department and its bureaus to work as a team in addressing IT security issues. The Department's Chief Information Officers (CIO) Council has implemented controls to improve the integrity, availability, and confidentiality of IT systems throughout the Agency. Furthermore, the Department's CIO incorporated IT security in performance plans for operating unit CIOs, and instituted effective mechanisms that have allowed successful communication and collaboration across organizational boundaries.

The result, thus far, has been a stronger and highly visible IT security program that continuously weighs the risks of technology against operational necessity to bring about a security posture that facilitates mission accomplishment.

To ensure that the Department effectively manages ongoing IT security concerns, the Office of the CIO (OCIO) has adjusted its strategy to include reviewing and updating relevant policies and procedures as needed as well as exercising C&A compliance oversight based on Federal Information Security Management Act (FISMA) requirements, OMB policy, National Institute of Standards and Technology (NIST) standards and guidelines, and previous OIG recommendations. As a result of this year's Department-wide C&A improvement effort, 96 percent of the Department's 302 IT systems have been certified and accredited. OCIO determined that all of the C&A packages it reviewed follow the Department's IT security policy and NIST guidance on risk management framework. The highlights of the Department's IT security accomplishments are described below.

Personally Identifiable Information (PII): The Department aggressively pursues the OMB mandate for protecting and monitoring sensitive information. Since issuance of OMB Memorandum M-06-16, *Protection of Sensitive Agency Information,* in June 2006, the Department has developed and implemented the policies and standards needed to protect such information.

- To remain compliant with OMB Memoranda M-06-16 and M-06-19, the Department's Computer Incident Response Teams (CIRT) have taken the lead in reporting to the U.S. Computer Emergency Readiness Team (US-CERT) and to Departmental management the state and management of PII. The Department's executive management receives weekly reports.

- The Office of the Secretary has established an Identify Theft Task Force that coordinates with other Departmental offices to ensure that appropriate risk-based responses to data breaches are developed and implemented. In addition, the Identify Theft Task Force has been tasked with working closely with other federal agencies, offices, and teams which influence or oversee programmatic issues involved in particular breaches or losses.

- An OMB-mandated breach notification plan was prepared, vetted, and, shortly after the end of the reporting period, distributed throughout the Department. The plan identifies appropriate senior management officials within the Department to oversee the management of security breaches. The plan also specifies the responsibilities of the Identity Theft Task Force in providing advance planning, guidance, in-depth analysis, and recommended courses of action in response to data breaches.

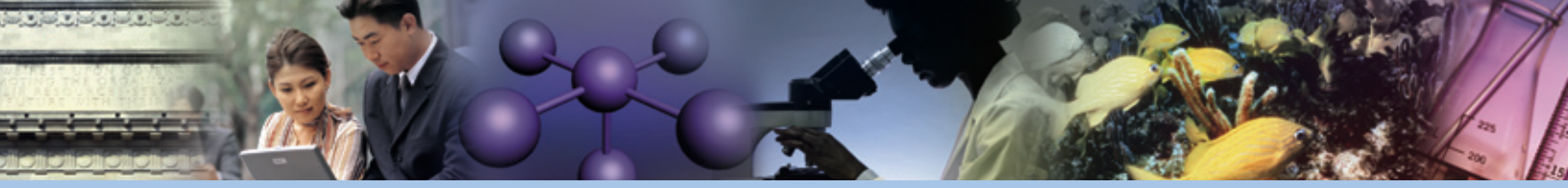
Encryption: The Department has taken assertive steps in safeguarding sensitive information such as encrypting any PII contained on mobile devices. The Department has successfully installed full-disk encryption on 100 percent of its laptop computers using Safeboot Federal Information Processing Standards (FIPS) 140-2-compliant software.

Two-Factor Authentication: A Department-wide standard for two-factor authentication was selected that will strengthen access control by substantially reducing the threat from reusable passwords.

IT Security Governance: OCIO has revitalized the IT Security Coordinating Committee (ITSCC) to improve the Department's IT security program's strategic alignment with Departmental policy. Regularly scheduled sessions were held to discuss pressing issues, to define and resolve technical IT security problems, and to make recommendations concerning IT security to the CIO Council.

IT Security Training: Targeted training was provided to the core group of personnel that are responsible for carrying out the C&A process as well as for interpreting and determining the acceptability of C&A results. OCIO has provided or has plans to provide role-based training to all stakeholders involved in the C&A process. Additionally, IT security training was provided for FISMA database automation, risk management process, management of plans of action and milestones (POA&M), and C&A quality improvement. Because of the significance of addressing IT security awareness at the Department, it has experienced an unprecedented participation in training efforts.

Certification and Accreditation (C&A) Quality and Process: The Department transformed C&A compliance reviews into a dynamic and collaborative process, interacting with stakeholders through an exhaustive review of past OIG findings as well as OMB and NIST guidance. Emphasis was placed on better documentation and risk acceptance awareness by authorizing officials. Subsequently, eight high quality packages were delivered to the OIG for its review. These CIO-conducted C&A reviews were generally received positively by the operating units and the results are being incorporated in their quality assurance processes. The CIO Council has selected for implementation in early FY 2008 a software solution—the Cyber Security Assessment and Management tool—to assist with FISMA reporting.



Internal Control Review: The Department conducted an internal control review for all 14 of its operating units that combined FISMA and FMFIA requirements. The review assessed the effectiveness of IT security controls, PII management, C&A, IT security training, contractor system oversight, and usage of a newly instituted Information Security Acquisitions Checklist. In addition to reviewing the operating units, two program level functions were reviewed—the IT security and the identity theft protection programs. OCIO found that the internal controls that were examined were generally effective.

Plans to Further Strengthen IT Security in FY 2008

Notwithstanding these achievements, the Department believes that further enhancements are possible in implementing and managing secure system configurations, and in sustaining improvements in the C&A process to ensure quality work products for managing system security. To ensure consistent and repeatable processes, the following activities will continue to foster effective oversight of Department-wide IT security program implementation:

- The Department CIO will continue to provide input to the rating official for each operating unit CIO on their performance, a significant portion of which will relate to IT security.
- The Department CIO will remain actively involved in the review of proposed IT budget initiatives to ensure that IT security is adequately addressed and funded, and to assure sufficient planning for continuity of operations (COOP).
- The Commerce IT Review Board, chaired by the Department CIO and co-chaired by the Department's Chief Financial Officer/ Assistant Secretary for Administration (CFO/ASA), will continue to evaluate proposed security plans for every IT project under consideration, including new initiatives and continuing IT projects. These reviews include examining the adequacy of IT security management and funding, and the involvement of IT project managers in spotlighting IT security concerns for their projects as a key part of their work.
- The Department CIO will continue conducting annual internal control reviews as needed to ensure FISMA and FMFIA compliance.

Automated FISMA Tool: The Department has developed an implementation plan for an automated FISMA tool, which will enhance its integrity in managing IT risks, corrective action plans (CAP), and OMB reporting.

Secure Configurations: Secure system configurations are an essential element in an IT security program and the Department has made it a critical element of its C&A quality improvement process. In the OIG's FY 2007 FISMA evaluation, four of the six C&A packages that were submitted for their review had inadequate secure configuration settings. As a result, secure configurations will be stressed and incorporated as a critical process in the Department's C&A Smart Spot-Checks. OCIO has also coordinated with the Department's Office of Acquisition Management to ensure that the appropriate security clause is used to obtain secure operating systems upon the purchase of any Microsoft Windows or Intel-based system. To support the operating units' schedules for the use of secure configurations in early FY 2008 for all Vista and XP devices, OCIO has begun to explore how it can assist with consistency and standardization across the Department. Selection is imminent of a lead operating unit to help guide this effort and reduce redundancy for the implementation of configurations for Windows, as well as other key operating systems and applications.

Perimeter Protection, Critical Infrastructure, and Continuity of Operations (COOP): The Department's IT infrastructure is comprised of a heterogeneous network of networks. To effectively manage its IT assets, the Department utilizes a Defense-in-Depth strategy, which involves people, process, and technology. The Department has implemented a baseline IT security policy and conducted oversight reviews to ensure sufficient security awareness training for employees and contractors with security responsibilities. From a technology perspective, the Department, through a federation of CIRTs, communicates and protects its network perimeters from malicious threats. The Department's CIRT uses state of the art technologies—including forensic analysis tools, intrusion detection and protection devices, incident alert software, and log analysis tools—to protect the Department's networks and users from cyber incidents. As incidents occur and are investigated, the Department's CIRT coordinates efforts with the Department of Homeland Security, US-CERT, OIG, and the Department federation of CIRTs. The Department responded to and reported 533 incidents in FY 2007.

The Department has selected an E-Team emergency management system to provide alert notification and task tracking capability throughout the organization. Several exercises have been conducted thus far with personnel trained on the use of the system. The Department also participated in the government-wide FY 2007 Pinnacle exercise in which OCIO responded to several incidents and tested communications capabilities between the normal operating location and alternate operating facilities. The Department conducts monthly COOP working group meetings to share information and to coordinate appropriate maintenance of COOP support plans. OCIO recently conducted situational awareness, and roles and responsibilities refresher training for all personnel in its organization. Personnel were updated on the tasks to be performed in the event of COOP activation, as well as the importance of personnel availability and sustainability to ensure the Department's essential functions continue regardless of the nature of any event.

Other Internal Control Enhancement Activities Continue

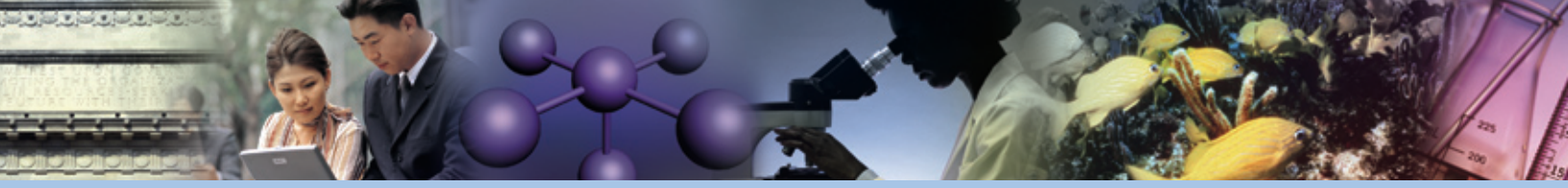
The Department's comprehensive effort to enhance management of internal controls under OMB Circular A-123 continued during FY 2007. Progress made in implementing Appendix A to OMB Circular A-123, which relates to financial internal controls, included the following:

- A three-year, risk-based rotational testing plan was developed based on the FY 2006 assessment of the key processes and results of previous audits. Under this approach, high-risk cycles will be tested annually and low to moderate-risk cycles will be tested every three years. Selected test procedures at certain locations or on certain sub-processes will be performed as often as needed based on specifically identified risks; and a limited controls review assessment survey will be utilized for cycles that are not tested in any given year.

- The Senior Management Council (SMC) continued to oversee, direct, and implement the assessment process, and the Senior Assessment Team (SAT) continued to develop planning documentation, administer internal control test plans, and monitor and review test work.

- Department-wide testing templates for selected key processes and sub-processes were updated, and the Departmental sampling plan was modified to ensure consistency, including the use of a statistical sample size generator.

- Department-wide testing results and work papers were reviewed and the structure, breadth, and depth of bureau-level documentation were assessed to ensure consistency and completeness.



The Department also continued its focus on management of nonfinancial internal controls under OMB Circular A-123. Through the SAT, the operating units were tasked with identifying and conducting assessments of programmatic and administrative activities meriting review in FY 2007. A wide range of programs and functions were assessed within individual operating units. Department-wide, principal focus was given to enhancing internal controls relating to the management of personal property.

Late in FY 2006, it became evident through press reports and Congressional inquiries that oversight of laptop computers and the data that they contain required evaluation across government. In addition to the overall efforts of OCIO in the area of IT security, the Office of the CFO/ASA undertook a comprehensive initiative to assess how the Department and its operating units manage not only laptop computers, but personal property, in general. The Department's multi-prong approach included:

- Conducting a complete inventory and reconciliation of personal property owned by the Department;
- Providing refresher training and certifying employees with direct property management responsibilities;
- Impaneling of Property Boards of Review to evaluate and resolve all incidents of missing property;
- Consolidating pre-existing personal property systems into one centralized automated system;
- Establishing bureau-specific procedures as necessary to ensure full employee accountability for property with which they are entrusted;
- Amending performance plans for property managers, custodians, and accountability officers to include a critical element relating to property management;
- Reviewing management practices involving mobile devices such as cell phones, removable memory storage devices, and personal digital assistants (PDA); and
- Conducting a Department-wide review of internal controls used for managing personal property.

This year-long initiative has provided assurance that adequate controls are in place across the Department, employees are properly trained and accountable for their responsibilities, and that any losses are appropriately identified and resolved, as necessary.

The Department's assessments reflect a system of nonfinancial and financial controls that is operating effectively. No material weaknesses relative to financial controls were identified for the period July 1, 2006 through June 30, 2007, the reporting period established by OMB Circular A-123. Further, with limited review and inquiries, no material weaknesses related to internal control over financial reporting were identified between July 1, 2007 and September 30, 2007. As a result of its FY 2007 activities, the Department identified only one material weakness in its internal controls, which, as described above, relates to IT security.

Section 4 of the FMFIA – Internal Controls over Financial Management Systems

Based on reviews conducted by the Department and its operating units for FY 2007, the financial systems in the Department are compliant with GAO principles and standards and requirements of the CFOs Act and OMB. The Department had no material weaknesses under Section 4 of FMFIA. See Appendix E for summary of material weaknesses reported under Section 4 of FMFIA.

FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT (FFMIA) OF 1996

Under the Federal Financial Management Improvement Act (FFMIA) of 1996, the Department is required to have financial management systems that comply with federal financial management system requirements, federal accounting standards, and the U.S. Government Standard General Ledger (USSGL) at the transaction level. In FY 2007, the Department remained in compliance with FFMIA.

REPORT ON AUDIT FOLLOW-UP

The Inspector General Act, as amended, requires that the Secretary report to Congress on the final action taken for Inspector General audits. This report covers Commerce Department audit follow-up activities for the period June 1, 2006, through May 31, 2007.

SUMMARY OF ACTIVITY ON AUDIT REPORTS
JUNE 1, 2006 THROUGH MAY 31, 2007

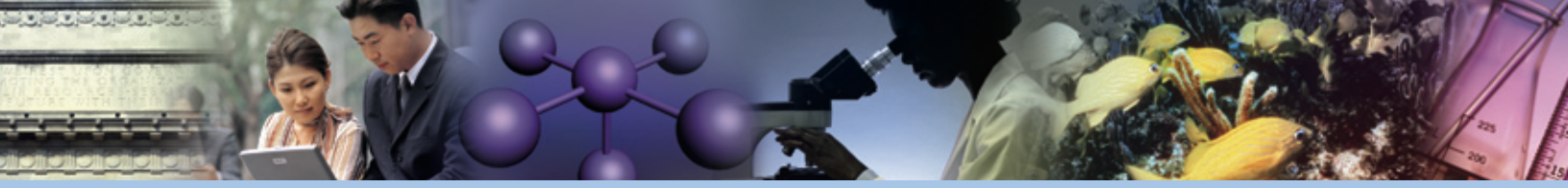
	DISALLOWED COSTS[1]		FUNDS TO BE PUT TO BETTER USE[2]		NONMONETARY REPORTS[3]	TOTAL
	NUMBER OF REPORTS	DOLLARS	NUMBER OF REPORTS	DOLLARS	NUMBER OF REPORTS	REPORTS
Beginning Balance	54	$ 13,359,832	19	$ 25,266,418	19	92
New Reports	30	2,145,069	19	4,215,765	15	64
Total Reports	84	15,504,901	38	29,482,183	34	156
Reports Closed	(29)	(6,712,154)	(19)	(19,095,372)	(23)	(71)
Ending Balance	55	$ 8,792,747	19	$ 10,386,811	11	85

1. Disallowed costs are questioned costs that management has sustained or agreed should not be charged to the government.
2. "Funds to be put to better use" refers to any management action to implement recommendations where funds should be applied to a more efficient use.
3. Includes management, contract, grant, loan, and financial statement audits with nonmonetary recommendations.

BIENNIAL REVIEW OF FEES

OMB Circular A-25, *User Charges*, requires the biennial review of agency programs to determine whether fees should be charged for government goods or services, and to ascertain that existing charges are adjusted to reflect unanticipated changes in costs or market values.

The Department conducts a review of its programs biennially, with some bureaus conducting annual reviews. In the current review, the Department noted that all bureaus, except for one bureau receiving an exemption from Circular A-25, adjusted their fees to meet the Circular A-25 requirement of full-cost recovery for user charges.



IMPROPER PAYMENTS INFORMATION ACT (IPIA) OF 2002

Narrative Summary of Departmental Efforts for FY 2007

IPIA was enacted to provide for estimates and reports of improper payments by federal agencies. The Act requires that federal agencies estimate improper payments and report on actions to reduce them. A review of all programs and activities that the Department administers is required annually to assist in identifying and reporting improper payments.

The Department has not identified any significant problems with improper payments, however, the Department recognizes the importance of maintaining adequate internal controls to ensure proper payments, and the Department's commitment to the continuous improvement in the overall disbursement management process remains very strong.

Each of the Department's payment offices has implemented procedures to detect and prevent improper payments. The following are some examples of the internal control procedures used by the payment offices:

- Prepayment and post-payment audit analyses are performed;
- Controlled/limited access to financial system screens, and approval authority for changes to information in the vendor table have been implemented to prevent unauthorized diversion of funds;
- Funds control in financial systems provides reasonable assurance against overpayments or improper payments;
- Edit reports in financial systems are programmed to identify potential items that may result in improper or duplicate payments;
- All documents submitted for payment are required to have previously gone through an approval process at several levels, including initial request, subsequent budget approval, voucher examination, and electronic certification system review.

The Department has ensured that internal controls, manual, as well as financial system, relating to payments are in place throughout the Department, and has reviewed all financial statement audit findings/comments and results of other payment reviews for indications of breaches of disbursement controls. None of these audit findings/comments or reviews have uncovered any significant problems with improper payments or the internal controls that surround disbursements.

The Department continued its reporting procedures that required quarterly reporting to the Department, by the payment offices, on any improper payments, identifying the nature and magnitude of the improper payments along with any necessary control enhancements to prevent further occurrences of the type of improper payments identified. The Department's analysis of the data collected from the payment offices shows that Department-wide improper payments were below one-tenth of one percent in FY 2007, as was the case in FY 2006. As a separate effort during FY 2007, the Department conducted a systematic sampling process to draw and review random samples of disbursements from the Department-wide universe, covering the period from October 1, 2006 through June 30, 2007. Results of the review revealed no significant improper payments or internal control deficiencies. The same results were achieved following a similar review in FY 2006. Overall, the Department's assessments demonstrate that the Department has strong internal controls over the disbursement processes, the amounts of improper payments by the Department are immaterial, and the risk of improper payments is low.

For FY 2008 and beyond, the Department will continue its efforts to ensure the integrity of its disbursements.