

## MANAGEMENT CONTROLS

The Department of Commerce's management is 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, the Department identified one material weakness in internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 2006. 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, 2006, 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, 2006 and September 30, 2006.

Carlos M. Gutierrez
Secretary of Commerce

## FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT (FMFIA) OF 1982

During FY 2006, 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
- 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 U.S. Government Accountability Office (GAO) and the Office of the Inspector General (OIG), and specifically requested studies. It is worth noting that GAO's list of high-risk programs, which was last issued in January 2005 at the beginning of the new Congress, does not include any programs administered by the Department. Also, on a yearly basis, operating units within the Department conduct self-assessments of their compliance with FMFIA.

The diverse reviews that took place during FY 2006 relative to nonfinancial controls provide assurance that Department 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 all IT systems.

The following table reflects the number of material weaknesses reported under Section 2 of FMFIA in recent years by the Department.

| NUMBER OF MATERIAL WEAKNESSES | | | | |
|---|---|---|---|---|
| | NUMBER AT BEGINNING OF FISCAL YEAR | NUMBER CORRECTED | NUMBER ADDED | NUMBER REMAINING AT END OF FISCAL YEAR |
| FY 2003 | 1 | 0 | 0 | 1 |
| FY 2004 | 1 | 0 | 0 | 1 |
| FY 2005 | 1 | 0 | 0 | 1 |
| FY 2006 | 1 | 0 | 0 | 1 |

### *IT Security Requires Further Improvement*

As stated in the Secretary's introductory letter, the Department made significant strides again this year in addressing this concern while acknowledging that further improvements are needed.

There are 229 moderate and high impact systems in the Department's information systems inventory. Twenty-two improved C&A packages for high and moderate-impact systems were received by the Office of the Chief Information Officer (OCIO) in time for review by OIG under the Federal Information Security Management Act (FISMA). OCIO reviewed the 22 packages and determined 12 to be of sufficient quality to forward to OIG. OIG evaluated 11 of these packages, which were for Department-owned systems, as well as four additional packages for contractor systems. OIG found that the quality of risk assessments and system security plans for Department-owned systems overall had significantly improved, but that certification testing and related documentation for many of the systems still needed improvement. OIG concluded that five of the 11 Department-owned systems and none of the four contractor systems met the C&A criteria established by the Department's IT security policy, OMB's policy, and the National Institute of Standards and Technology's (NIST) standards and guidelines. Further improvement of system testing is underway and improvement of all C&A packages will be monitored throughout FY 2007.



During FY 2006, OIG's independent audit of the Department's FY 2005 financial statements included security reviews of the Department's financial management systems. The audit concluded that seven operating units had weaknesses in five out of six key IT security areas: entity-wide security program planning and management, access controls, application software development and change control, system software management, and service continuity. The Department notes that the number of auditor findings has been decreasing—from 46 in FY 2005 to 25 in FY 2006—and that the severity of the findings has lessened, indicating significant improvement.

In February 2005, OCIO issued a *Plan for Eliminating the Basis for the Commerce FMFIA IT Security Material Weakness*, which set forth a schedule and reporting plan developed collaboratively with Department operating units to improve C&A documentation during FY 2005 and FY 2006. On a monthly basis, OCIO monitored the status of the operating units' corrective actions in response to this plan and prior-year reviews, and provided quarterly status updates of these and other planned corrective actions, as well as the status of IT security performance metrics, to OMB in accordance with FISMA requirements.

In its FY 2005 FMFIA report, the Department highlighted the following planned actions for FY 2006:

- Complete the use of secure system configurations to ensure that software parameters are set in a standard way to make each system adequately secure, and review the extent to which such secure system configurations have been implemented Department-wide.

- Confirm that C&A improvement efforts undertaken in FY 2005 have resulted in establishing lasting, repeatable, quality management practices for C&A documentation. In FY 2006, the focus was on ensuring that IT security practices were integrated throughout the Department, demonstrating further that sound, repeatable practices are implemented in a compliant and consistent manner.

These actions were addressed in FY 2006 for selected high and moderate-impact systems, yet work will continue into FY 2007 for all systems Department-wide. The Department's efforts and accomplishments during FY 2006 to strengthen its Department-wide IT security program are summarized below.

- The Department's IT security program maturity, as measured using the federal CIO Council's 5-level IT security maturity scale, maintained 100 percent of the Department operating units at level 3—implemented policies and procedures—or higher. This level of accomplishment in improving the maturity of IT security management reflects the hard work of many dedicated IT security professionals within the Department to institutionalize IT security practices and develop repeatable processes.

- The Department continued its IT security compliance review program, in which OCIO has arranged for a contractor to assess the extent to which IT security policy and guidance are implemented within the operating units and to assess the adequacy of agency-level IT security programs. The FY 2006 compliance review included looking at C&A packages for compliance with government-wide and Department requirements, and to ensure that the quality of the documentation reflects sound security planning. This year's compliance monitoring effort concluded that while all C&A packages inspected were complete, and FY 2006 efforts have resulted in raising the quality of C&A packages, additional work needs to be done.

- The Department enhanced its role-based IT security training program by procuring formal, instructor-led education seminars. The seminars include education in general IT security concepts as well as the C&A methodology recommended by NIST. This education will improve the skills of personnel involved in the C&A process, including senior managers serving as system Authorizing Officials and personnel participating on certification teams.



In order to maintain effective oversight of Department-wide IT security program implementation, the following activities continued.

- The Department's CIO provided input to rating officials, i.e., either the head of the operating unit or their deputy, on the performance of each operating unit CIO, a significant portion of which relates to IT security.

- The Department's CIO and OCIO IT security staff have been 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.

- The Department IT Review Board, chaired by the Department's CIO, considers and evaluates the proposed IT security approach for every IT project it reviews, including new initiatives as well as continuing IT projects. This review includes examination of the adequacy of the IT security management and funding, as well as the involvement of IT project managers in leading IT security for their project as a key part of their work. Corrective actions are identified and required of program and project officials, as appropriate.

Additionally, efforts to fully resolve this material weakness are being monitored by the Department's senior management. The Deputy Secretary is routinely kept apprised of progress that is being made, and the status of activities being undertaken at the Departmental and operating unit levels is formally discussed as part of the quarterly performance reviews. Further, the Deputy Secretary has requested that the IG and CIO regularly brief the Secretary and the heads of the operating units during Executive Management Team meetings.

Notwithstanding these achievements, work still remains to ensure the implementation and management of secure system configurations and to improve the C&A process as needed to guarantee the necessary quality of work products for managing system security. Specifically, actions planned for FY 2007 include:

- Enhanced training of personnel with significant IT security roles and responsibilities. The Department will focus efforts on educating Authorizing Officials and System Owners regarding their roles and responsibilities for IT security, especially for their role in the C&A process.

- Increased monitoring to validate that secure system configurations have been implemented, thereby ensuring that software parameters are set in a standard way to make each system adequately secure. The extent to which such secure system configurations have been implemented for selected systems and operating system platforms Department-wide will be validated.

- Continue efforts to confirm that C&A improvement efforts undertaken in FY 2006 have resulted in establishing lasting, repeatable, quality management practices for C&A documentation.

In FY 2007, the focus will be on ensuring that secure system configurations are being implemented for all operating system platforms throughout the Department, that personnel with significant IT security roles are properly trained, and that a sound, repeatable C&A process has been implemented in a compliant and consistent manner. Involved Departmental officials will continue to work closely with operating unit personnel to address these issues, and progress will continue to be monitored through quarterly performance reviews with the Deputy Secretary.



### *Strengthening Internal Controls over Financial Reporting*

In December 2004, OMB issued a complete revision to Circular A-123, *Management's Responsibility for Internal Control*, which focused on strengthening requirements for assessing internal controls over financial reporting. In FY 2006, the first year for which the revised circular was effective, the Department and its operating units undertook a comprehensive and coordinated approach to conducting an assessment of the effectiveness of internal control over financial reporting in accordance with the new requirements of Circular A-123.

- A Senior Management Council was established to implement, direct, and oversee the assessment process, and a Senior Assessment Team was established to develop and conduct the assessment.
- The scope of the assessment was determined by identifying financial and budgetary reports that have significant effects on spending, budgetary, and other financial decisions.
- The overall control environment was evaluated, and 12 key process cycles and approximately 630 key controls were identified for evaluation across the Department. The 12 key processes included Budget Execution; Inventory; Purchasing; Revenues; Payroll and Employee Benefits; Property, Plant and Equipment Spending, and Maintenance; Financial Reporting; Treasury Management; Risk Management; Information Systems; Grants Management; and Loans.
- A Department-wide testing approach and plan were developed.
- The Senior Management Council and Senior Assessment Team reviewed testing results and determined the significance of any deficiencies, i.e., whether they constituted an internal control deficiency, reportable condition, or material weakness.
- A communication plan was developed for use in raising the awareness of Department employees to the importance of internal controls in carrying out their responsibilities.

The Department's assessment reflects a system of financial controls that is operating effectively. No material weaknesses were identified for the period October 1, 2005 through June 30, 2006, the reporting period specified by OMB Circular A-123. Further, no material weaknesses related to internal control over financial reporting were identified between July 1, 2006 and September 30, 2006.

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

| NUMBER OF MATERIAL WEAKNESSES | | | | |
|---|---|---|---|---|
| | NUMBER AT BEGINNING OF FISCAL YEAR | NUMBER CORRECTED | NUMBER ADDED | NUMBER REMAINING AT END OF FISCAL YEAR |
| FY 2003 | 1 | 1 | 0 | 0 |
| FY 2004 | 0 | 0 | 0 | 0 |
| FY 2005 | 0 | 0 | 0 | 0 |
| FY 2006 | 0 | 0 | 0 | 0 |

Based on reviews conducted by the Department and its operating units for FY 2006, the financial systems in the Department are compliant with GAO principles and standards, the requirements of the Chief Financial Officers (CFO) Act, and OMB requirements. The Department had no material weaknesses 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 (SGL) at the transaction level. In FY 2006, 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, 2005, through May 31, 2006.

**SUMMARY OF ACTIVITY ON AUDIT REPORTS**
**JUNE 1, 2005 THROUGH MAY 31, 2006**

| | 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 | 57 | $ 18,329,344 | 30 | $ 58,800,020 | 16 | 103 |
| New Reports | 24 | 1,488,685 | 6 | 948,555 | 29 | 59 |
| Total Reports | 81 | 19,818,029 | 36 | 59,748,575 | 45 | 162 |
| Reports Closed | (27) | (6,458,197) | (17) | (34,482,157) | (26) | (70) |
| Ending Balance | 54 | $ 13,359,832 | 19 | $ 25,266,418 | 19 | 92 |

1. *Disallowed costs are questioned costs that management has sustained or agreed should not be charged to the government. The beginning balance (reports and dollars) of disallowed costs reflects an adjustment since the last reporting period.*
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 2006*

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; and
- 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 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 2006, as was the case in FY 2005. As a separate effort during FY 2006, the Department conducted a systematic sampling process to draw and review random samples of disbursements from the Department-wide universe of FY 2006 disbursements, covering the period from October 1, 2005 through June 30, 2006. Results of the test revealed no significant improper payments or internal control deficiencies. The same results were achieved following a similar test in FY 2005. Overall, the Department's assessments demonstrate that the Department has strong internal controls over the disbursement processes, the amounts of improper payments in the Department are immaterial, and the risk of improper payments is low.

For FY 2007 and beyond, the Department will continue its efforts to ensure the integrity of its disbursements.