MANAGEMENT CONTROLS

FEDERAL MANAGER'S FINANCIAL INTEGRITY ACT (FMFIA) OF 1982

During FY 2005, 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 our 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.

The efficiency of the Department's operations is continually evaluated using information obtained from reviews conducted by the Government Accountability Office (GAO), Office of Inspector General (OIG), and specifically requested studies. It is worth noting that the list of high-risk programs issued by GAO in January 2005 does not include any programs administered by the Department of Commerce. Also, on a yearly basis, operating units within the Department conduct self-assessments of their compliance with FMFIA.

Section 2 of the FMFIA, which deals with nonfinancial controls, 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 diverse reviews that took place during FY 2005 provide a high level of assurance that Commerce systems and management controls comply with standards established under FMFIA, with the exception of one material weakness. This weakness involves the need to validate that information technology (IT) security certification and accreditation (C&A) documentation and processes for the Department's national critical and mission critical systems are of adequate quality. As stated in the Secretary's introductory letter, the Department of Commerce has made important progress in resolving this material weakness by working closely with its operating units to address concerns and to improve the overall performance of the Department's IT security program.

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

Section 2 of FMFIA

NUMBER OF MATERIAL WEAKNESSES				
	NUMBER AT BEGINNING OF YEAR	NUMBER CORRECTED	NUMBER ADDED	NUMBER REMAINING END OF FISCAL YEAR
FY 2002	2	1	0	1
FY 2003	1	0	0	1
FY 2004	1	0	0	1
FY 2005	1	0	0	1

Strengthening Information Technology Security

During the year, the Department of Commerce significantly improved its IT security posture, focusing on completing corrective actions to address prior-year IT security concerns and improving the quality of C&A processes and documentation for national critical and mission critical systems. Improved C&A packages for all national critical systems and most mission critical systems have been completed. However, only a small number of improved C&A packages were available by the Inspector General's (IG) August 31 deadline for independent evaluation under the Federal Information Security Management Act (FISMA). The OIG's review of the available packages found that the risk assessments and security plans were much improved, but three of the five improved packages reviewed had not undergone adequate certification testing. In light of the limited number of packages available for review and the testing deficiencies found, OIG concluded that the C&A process had not yet improved to the point where authorizing officials throughout the Department have sufficient information about the vulnerabilities remaining in their systems when it is time to make the accreditation decision. Corrective action related to system testing is underway and all C&A packages are scheduled to have been improved by the end of FY 2006.

Additionally, in FY 2005, the IG's independent audit of the Department's FY 2004 financial statements included security reviews of the Department's financial management systems. The audit concluded that seven operating units had weaknesses in six key IT security areas —entity-wide security program planning and management, access controls, application software development and change control, system software management, segregation of duties, and service continuity.

The Office of the Chief Information Officer (OCIO) issued a *Plan for Eliminating the Basis for the Commerce FMFIA IT Security Material Weakness,* which contains a schedule and reporting plan developed collaboratively with Commerce operating units to improve C&A documentation and processes during FY 2005 and FY 2006. OCIO closely monitored efforts in FY 2005 by operating units to improve the quality of C&A documentation and processes. OCIO completed IT security compliance reviews that included inspecting improved system C&A packages for five of the Department's national critical and 21 of its mission critical systems. It also reviewed 50 IT contracts for inclusion of IT security clauses, and reviewed secure configuration management implementation status and procedures for compliance with federal guidance and Departmental policy. It monitored on a monthly basis the status of corrective actions taken by operating units in response to these and prior-year reviews, and provided quarterly status updates to OMB on planned corrective actions and IT security performance metrics as required by FISMA.

Additionally, at the end of FY 2004, OCIO identified the following planned actions for FY 2005:

- Continue quality inspections of C&A package documentation, expanding reviews to business essential systems within the Department.
- Continue monitoring the inclusion of IT security provisions and requirements in contracts, and inspecting contractor operations to ensure adequate implementation of Commerce requirements to protect IT resources.
- Update Departmental IT security policy to reflect recent government-wide guidance.
- Improve the Department's computer incident response capability and implement mechanisms necessary to facilitate a Department-wide information sharing capability.
- Improve the Department's configuration management practices to ensure secure system configurations are implemented and maintained for IT systems.

All of these actions were completed in FY 2005, and the accomplishments and efforts taken by Commerce to strengthen its Department-wide IT Security Program are summarized below:

- The Department updated its IT Security Program Policy to align with the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.* This major undertaking required Department-wide collaboration and extensive review.

- 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 Commerce operating units at Level 3 (implemented policies and procedures) or higher, and recognized 64 percent of the operating units as having achieved level 4 (tested and reviewed procedures and controls). 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, including review of business essential systems, 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 2005 compliance review included review of C&A packages for compliance with government-wide and Commerce requirements and to ensure that the quality of the documentation reflects sound security planning and processes. This year's compliance monitoring effort concluded that while all C&A packages inspected were complete, and efforts during FY 2005 to improve the quality of the documentation have resulted in raising the quality of C&A packages, still more work needs to be done.

- Direction was provided to all Commerce operating units to implement the secure system configuration management procedures recommended by NIST. By the end of FY 2005, operating units reported that more than 70 percent of all Commerce systems were under secure system configuration control.

- Through the IT security compliance review program, 60 IT contracts were reviewed for inclusion of IT security provisions and requirements, and several contractor-operated systems were reviewed.

- The Department renewed its agreement with the Office of Personnel Management (OPM) for access to online role-based IT security training. The courses include two levels of training in C&A skills for personnel involved in the C&A process, for senior managers serving as system Authorizing Officials, and for personnel participating on certification teams.

- The Department issued guidance for the development of operating procedures for Commerce computer incident response teams (CIRT). This guidance, and revitalization of communications processes and procedures for the Department's five CIRTs, has provided improved governance to ensure Department-wide consistency in handling IT security incidents.

In addition, the following activities were continued in order to maintain effective oversight of Department-wide IT security program implementation:

- The Department CIO provided input to the rating official (operating unit head or deputy head) on the performance of each operating unit CIO, a significant portion of which relates to IT security.

- The Department 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 Commerce IT Review Board, chaired by the Commerce 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 the program and project officials, as appropriate.

- The Department continued its IT security training program, leveraging capabilities available through other government agencies, especially through OPM's Government Online Learning Center. This provides cost-effective annual IT security refresher training for employees and contractors, and availability of specialized training for personnel with more intensive IT security roles and responsibilities.

Ongoing Effort to Strengthen IT Security will Continue in FY 2006

Notwithstanding these achievements during FY 2005 to resolve prior IT security issues and to maintain a strong IT security program, work still remains to ensure the implementation and management of secure system configurations and to sustain efforts to improve C&A practices and adequate quality of work products for managing system security. Specifically, actions planned for FY 2006 include:

- Completion of the use of secure system configurations to ensure 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 Department-wide will be reviewed.

- Confirming that C&A improvement efforts undertaken in FY 2005 have resulted in establishing lasting, repeatable, quality management practices for C&A documentation.

As the Department works to fully resolve this material weakness during FY 2006, the focus will be on ensuring that IT security practices are integrated throughout the Department, demonstrating further that sound, repeatable practices are implemented in a compliant and consistent manner.

Section 4 of FMFIA

NUMBER OF MATERIAL WEAKNESSES				
	NUMBER AT BEGINNING OF YEAR	NUMBER CORRECTED	NUMBER ADDED	NUMBER REMAINING END OF FISCAL YEAR
FY 2002	1	0	0	1
FY 2003	1	1	0	0
FY 2004	0	0	0	0
FY 2005	0	0	0	0

The Department has no material weaknesses relating 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 2005, 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, 2004, through May 31, 2005.

SUMMARY OF ACTIVITY ON AUDIT REPORTS
JUNE 1, 2004 - MAY 31, 2005

	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	49	$ 23,600,378	26	$ 43,206,760	28	103
New Reports	35	3,361,337	12	16,101,323	23	70
Total Reports	84	26,961,715	38	59,308,083	51	173
Reports Closed	(28)	(8,635,575)	(8)	(508,063)	(35)	(71)
Ending Balance	56	$ 18,326,140	30	$ 58,800,020	16	102

1. *Disallowed costs are questioned costs that management has sustained or agreed should not be charged to the government. The beginning balances for the number of reports and the dollar amount of disallowed costs have been corrected for duplication caused by more than one type of action having affected an audit report during the last reporting period.*
2. *"Funds to be put to better use" refers to any management action to implement recommendations that funds 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 fee programs biennially, with some bureaus conducting annual reviews. In the current review, the Department noted that all but one bureau adjusted their fees to be consistent with the program and with the program's purpose to maximize the recovery of goods or services provided to the public. ITA is currently implementing an OMB-approved compliance plan for Circular A-25, and plans to complete pricing for all of its products in FY 2006. The Department will keep OMB and Congress informed on its progress with the compliance plan.

IMPROPER PAYMENTS INFORMATION ACT (IPIA) OF 2002

Narrative Summary of Implementation Efforts for FY 2005

The Department has not identified any significant problems with erroneous payments; however, it recognizes the importance of maintaining adequate internal controls to ensure proper payments, and its 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 bureaus:

- Prepayment and post payment audit analyses are performed.
- Controlled/limited access to the 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 the financial system provides reasonable assurance against overpayment or erroneous payments.
- Edit reports 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 system—relating to payments are in place throughout the Department, and has reviewed all financial statement audit findings and results of other payment reviews for indications of a breach of those controls. None of these reviews or audits has uncovered any problems with erroneous payments or the internal controls that surround disbursements.

In FY 2005, the Department continued its reporting procedures that required quarterly reporting to the Department by its bureaus on any erroneous payments, identifying the nature and magnitude of the erroneous payment, along with any necessary control enhancements to prevent further occurrence of the type of erroneous payments identified. Our analysis of the data collected from the bureaus shows that Department-wide erroneous payments were below one tenth of one percent in FY 2005, as was the case in FY 2004. As a separate effort during FY 2005, the Office of Financial Management conducted a systematic sampling process to draw and review random samples of disbursements from the Department-wide universe of FY 2005 disbursements. Results of the test revealed no significant erroneous payments or internal control deficiencies. The same results were achieved following a similar test in FY 2004. Also, in FY 2005, the Department received the results of an Office of Inspector General's (OIG) audit involving a comprehensive review of disbursements for improper payments at the Department's largest payment office. Results of this audit revealed no significant erroneous payments or internal control deficiencies. Overall, our assessments demonstrate that the Department has strong internal controls over the disbursement process, the amounts of erroneous payments in the Department are immaterial, and the risk of erroneous payments is low.

During FY 2005, in compliance with Section 831 of the Defense Authorization Act of 2002 (P.L. 107-107, Title VIII, Subtitle D, Sec. 831; 31 USC 3561-3567), which requires federal agencies to identify and recover overpayments to contractors due to payment errors, the Department contracted with a private vendor to perform recovery auditing. The audit included thorough reviews of sample invoices from two of the Department's largest payment offices, and an independent confirmation of open items with key vendors. Results of the audit and confirmation efforts revealed no significant improper payments or internal control deficiencies.

For FY 2006 and beyond, the Department will continue its efforts to ensure the integrity of its programs' payments.