MANAGEMENT CONTROLS

Fiscal Year 2004 Secretary of Commerce Statement of Management and Financial Controls

For the programs, organizations, and functions covered by the Federal Managers' Financial Integrity Act (FMFIA), I am pleased to report that, with the exception of one material weakness identified below, the Department of Commerce's systems of management controls, taken as a whole, provide reasonable assurance that the objectives of the FMFIA have been achieved.

Donald L. Evans
Secretary of Commerce

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

During FY 2004, the Department reviewed its management control system in accordance with FMFIA requirements 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 preparation of accounts and 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 2003 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. These diverse reviews provide a high level of assurance that Department systems and management controls comply with standards established under FMFIA, except for the IT Security weakness summarized on the following page.

Section 2 of FMFIA

NUMBER OF MATERIAL WEAKNESSES				
	NUMBER AT BEGINNING OF YEAR	NUMBER CORRECTED	NUMBER ADDED	NUMBER REMAINING END OF FISCAL YEAR
FY 2001	0	0	2	2
FY 2002	2	1	0	1
FY 2003	1	0	0	1
FY 2004	1	0	0	1

In FY 2004, the Department of Commerce made major strides toward eventual resolution of one outstanding material weakness as identified under Section 2 of FMFIA – inadequate information technology (IT) security controls – by focusing on the completion of corrective actions needed to address previously identified concerns and improving the measurable performance of the Department's IT security program.

Working to Strengthen Inadequate IT Security Controls

At the end of FY 2003, the Department identified several steps to resolve the material weakness relating to its IT security controls, which included:

- achieving a higher level of maturity in the management of IT security across the Department, as verified through a formal maturity measurement process;

- continuing the compliance review program goal of assessing the extent to which IT security implementation is consistent with Department IT security policy; and

- ensuring the certification and accreditation (C&A) of all operational IT systems.

A summary of the Department's efforts in these areas during FY 2004 follows.

- The Department continued its IT security compliance review program, and hired a contractor to assess the extent to which policy and guidance are implemented by the bureaus and to assess the adequacy of bureau-level IT security programs. The compliance review included follow-up on FY 2002 OIG IT security inspection findings and recommendations at NIST and USPTO, as well as review of system C&A documentation for all national critical systems and a sample of mission critical systems.

- The review, which included testing of system controls in accordance with the GAO Federal Information System Controls Audit Manual (FISCAM), confirmed that the FY 2002 audit recommendations had been implemented at all involved bureaus and identified no new significant weaknesses, although less significant deficiencies in the quality of documentation were noted. The review of C&A packages, which included tests for compliance with federal and Departmental requirements as well as the quality of the documentation to reflect sound security planning throughout the system's life cycle, concluded that, while all C&A packages reviewed were complete, a broad range of work to improve the quality of the documentation remains.

- The Department's IT security maturity, measured using the federal Chief Information Officers (CIO) Council's five-level maturity scale, increased from 79 percent to 100 percent at Level 3 or higher, which involves having implemented policies and procedures; and from 7 percent to 36 percent at Level 4, which relates to having tested and reviewed procedures and controls. This improvement reflects hard work on the part of many IT security professionals within the Department to implement new standards and correct long-standing deficiencies.

- Migration of Commerce operating units in the Herbert C. Hoover Building to the new digital infrastructure that supports both voice and data requirements of the Herbert C. Hoover Building progressed during FY 2004. This centralization of network controls improves security by providing a defense-in-depth posture and reducing the external points through which an attacker might compromise security. The OIG, using the FISCAM as well as limited technical network and system security testing, examined the ability of this environment to protect EDA's financial systems and data and did not report any deficiencies with the controls tested.

- Formal instructor-led training was provided to improve the technical skills possessed by personnel involved in the C&A process. The training included a four-day workshop on the activities involved in the C&A process and a half-day seminar on the responsibilities of senior managers serving as system Authorizing Officials.

Additionally, ongoing activities intended to help maintain effective oversight for the Department's IT security program and continued during FY 2004 include:

- Annually, the Departmental CIO provides input to the rating official, i.e., the head of the operating unit or their deputy, on the performance of each bureau CIO, a significant portion of which relates to IT security.

- The Departmental CIO is 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 considers and evaluates the proposed IT security approach for every IT project it reviews, including new initiatives and continuing IT projects. This review includes examination of the adequacy of the IT security management and funding, and the involvement of the project managers in IT security 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, such as the Office of Personnel Management's Government Online Learning Center. This provides cost-effective annual IT security refresher training for both employees and contractors as well as specialized training for personnel with significant IT security roles and responsibilities.

During FY 2004, the Office of the CIO completed IT security compliance reviews of three Commerce operating units and reviewed system C&A packages for all 17 of the Department's national critical systems and 33 out of 254 mission critical systems. It also reviewed 80 IT contracts for inclusion of IT security clauses, and reviewed incident response and patch management procedures for compliance with federal guidance and Departmental policy. In addition, it monitored on a monthly basis the status of operating unit corrective actions in response to these and prior-year reviews and provided quarterly status updates of these and other planned corrective actions, along with status of IT security performance metrics, to OMB under the requirements of the Federal Information Security Management Act (FISMA).

In FY 2004, GAO issued a government-wide report on system C&A practices. In this report, GAO noted that Commerce was one of seven federal agencies to have met OMB's IT security performance goals for C&A. In addition, GAO noted that Commerce had identified and resolved numerous challenges in meeting these goals, and had instituted an effective compliance review program for continuous monitoring of IT security practices.

The OIG's independent audit of the Department's FY 2004 financial statements included security reviews of the Department's financial management systems. The auditors found that substantial progress was made during FY 2004 in IT security associated with financial management systems, reflecting the level of effort made by the Department to strengthen IT security, but IT security control deficiencies continue to be a reportable condition.

The OIG reviewed the documentation for a sample of the Department's national-critical and mission-critical systems reported as certified and accredited. Although the OIG observed some improvements compared to the results of a similar review last year, the OIG found serious shortcomings in their risk assessments, security plans, contingency plans, and testing of security controls. The OIG also issued reports for IT security reviews it conducted within the Department, which focused on IT security controls, computer incident response capabilities, and, specifically, the IT security program at the Bureau of the Census. The OIG's review of computer incident response reported on the absence of a centralized entity to promote information sharing and consistency in response processes, inadequate incident response procedures, incomplete and inconsistent incident reporting by the operating units, and the need for better intrusion detection approaches and specialized tools and training. The OIG review of Census's IT security program found significant deficiencies in its certification and accreditation processes and documentation. The OIG also issued a report on IT security in IT service contracts recommending that Commerce take steps to ensure that its service contracts contain the new security clause that the Department issued in November 2003, and that appropriate contract oversight occurs.

Work Remains to Strengthen IT Security

Notwithstanding these efforts to resolve prior IT security issues and to maintain a strong IT security program, work remains to ensure the implementation of consistent C&A practices and adequate quality of work products for managing system security. As discussed earlier, the Department's C&A documentation for national critical and mission critical systems is not yet fully compliant with Departmental IT security policy and associated guidance. It is crucial that C&A processes and work packages be validated, ensuring that they are capable of adequately protecting Commerce systems. In order to ensure that continued high priority is given to improving C&A practices for all operational IT systems, the Department of Commerce continues to consider IT security as a material weakness.

Both the Department's and the OIG's FISMA reports submitted recently highlighted the need to improve the C&A packages so they are fully compliant with Department policy and guidance, and both reports list this area as a significant deficiency.

In FY 2005, the focus will be on ensuring that compliant and consistent IT security practices are implemented meeting a high level of quality. During the coming year, the Department will:

- 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/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 implementing mechanisms necessary to facilitate Department-wide information sharing capability; and
- improve the Department's configuration management practices to ensure secure system configurations are implemented and maintained for IT systems.

Section 4 of FMFIA

NUMBER OF MATERIAL WEAKNESSES				
	NUMBER AT BEGINNING OF YEAR	NUMBER CORRECTED	NUMBER ADDED	NUMBER REMAINING END OF FISCAL YEAR
FY 2001	1	0	0	1
FY 2002	1	0	0	1
FY 2003	1	1	0	0
FY 2004	0	0	0	0

The Department has no material weaknesses relating to 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 2004, 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 August 1, 2003, through May 31, 2004. As with last year's report, an accelerated reporting cycle has resulted in a ten-month reporting period.

Audit Follow-up Activities Within the Department

In July 2004, a contract was awarded to upgrade the 15 year-old automated system used to track OIG audits and prepare this report. This system upgrade and user training are expected to be completed prior to the preparation of next year's report on audit follow-up.

The bureaus are continuing their efforts to implement audit recommendations that are more than a year old. At the end of the reporting period, recommendations included in a total of 59 audits were reported as having been unimplemented for more than one year. Although some audits share reasons for recommendations not having been fully implemented, the reasons for final actions not being taken vary with each audit. For example, if collections for payments are annualized over several years, the audit will remain open until the final collection is made or a debt is paid. Some performance audits have recommendations that mandate construction projects, the completion of which can take several years.

In addition, audits that involve the reporting of funds to be put to better use will remain open until all work has been completed and the savings can be calculated. This is to ensure accurate reporting of the funds to be put to better use. Program development, implementation of new information systems, appeal of audit determinations, and technological enhancements of existing systems all can cause audits to remain open beyond a year. Staff within DM and the bureaus will continue to monitor these audits and assist in the implementation process.

SUMMARY OF ACTIVITY ON AUDIT REPORTS
AUGUST 1, 2003 - MAY 31, 2004

	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	62	$ 16,548,224	34	$ 55,444,966	45	141
New Reports	33	11,130,550	7	4,472,077	19	59
Total Reports	95	27,678,774	41	59,917,043	64	200
Reports Closed	(41)	(4,529,887)	(15)	(16,077,854)	(36)	(92)
Ending Balance	54	$ 23,148,887	26	$ 43,839,189	28	108

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 that funds be applied to a more efficient use.*
3. *Includes performance, contract, grant, loan, and financial statement audit reports with nonmonetary recommendations.*

BIENNIAL REVIEW OF FEES

The Chief Financial Officers Act of 1990 requires the biennial review of agency fees, rents, and charges imposed for services, and other things of value provided to specific beneficiaries as opposed to the American public in general. The objective of these reviews is to identify such activities and, where permitted by law, to begin charging fees. The reviews also support the periodic adjustment of existing fees to reflect current costs or market value, in order to minimize the general taxpayer subsidization of specialized services or things of value, such as rights or privileges, provided directly to identifiable non-federal beneficiaries.

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 legislative requirement to recover the full cost of goods or services provided to the public. ITA was deemed acceptably in compliance with OMB Circular A-25 by OMB, as they are implementing program changes to recover the full cost of goods and services provided to the public.

IMPROPER PAYMENTS INFORMATION ACT (IPIA) OF 2002

Narrative Summary of Implementation Efforts for FY 2004

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 for indications of a breach of those controls. None of the financial statement audits have uncovered any problems with erroneous payments or the internal controls that surround disbursements.

In FY 2004, the Department introduced new requirements for quarterly reporting by its bureaus on 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. Department analysis of the data collected from the bureaus shows that Department-wide erroneous payments are below 1 percent.

During the year, the Department's Office of Inspector General (OIG) conducted a comprehensive review of disbursements for improper payments at the Department's largest payment office; and in a separate effort, the Office of Financial Management conducted a systematic sampling process to draw and review a stratified sample of disbursements from a Department-wide universe of FY 2004 disbursements. Results of both tests revealed no significant erroneous payments or internal control deficiencies. Overall, its 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.

Also, the Department has contracted with a private vendor to perform recovery auditing across the Department's major payment offices, in compliance with Section 831 of the Defense Authorization Act.

For FY 2005 and beyond, the Department will continue its efforts to ensure the integrity of its programs' payments.