**UNITED STATES DEPARTMENT OF COMMERCE**
**Chief Information Officer**
Washington, D.C. 20230

July 28, 2004

MEMORANDUM FOR: Heads of Operating Units
Chief Information Officers

FROM: Thomas N. Pyke, Jr.

SUBJECT: DOC IT Security Program Policy and Minimum Implementation Standards for Control Reviews and Plans of Action and Milestones

This memorandum announces an update to section 3.2 of the Department of Commerce's IT Security Program *Policy and Minimum Implementation Standards* and issuance of associated procedures for "plans of action and milestones" and IT system inventory management. These are part of the Commerce IT Management Handbook, and are applicable Department-wide.

The *DOC IT Security Program Policy and Minimum Implementation Standards*, section 3.2 (Attachment 1) establishes the policy for performance of program- and system-level self-assessments and the development and management of plans of action and milestones (POA&Ms) to track corrective actions when external reviews or self-assessments reveal deficiencies in a Department of Commerce (DOC) information technology (IT) security program or system security controls. It also describes minimum standards for periodic vulnerability testing, and Departmental compliance reviews. In addition, it requires the establishment and maintenance of an IT system inventory of IT security-related management information for all Commerce IT systems.

The standard entitled *IT Security Plans of Action and Milestones (POA&Ms) and Performance Metrics* (Attachment 2) provides process guidance and minimum implementation requirements for completion of POA&Ms by all DOC operating units. In addition, this standard describes the specifications for the consistent and comprehensive completion of required updates of its IT security POA&Ms and establishes reporting schedules and formats for POA&Ms and IT security performance metrics.

The DOC *Process Guidance and Minimum Implementation Standards for IT System Inventory Management* (Attachment 3) details the process guidance and minimum implementation requirements for DOC operating unit completion of semi-annual IT system inventory updates. The IT system inventory provides a summary of valuable management data that reflects the status of an operating unit's implementation of its IT Security Program for national security and non-national security (unclassified) systems.

Please review, and update as necessary, your operating unit's policies and procedures to ensure they are consistent with the new policy and procedures. The policy and procedures in the attachment become effective 30 days from the date of this memo.

If you have questions, please contact Nancy DeFrancesco, the Department's IT Security Program Manager, at (202) 482-3490, or me at (202) 482-4797.

Attachments