



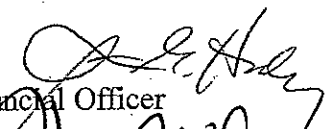
**United States
Department of
Agriculture**

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

TO: Agency Deputy Administrators for Management
Agency Chief Financial Officers
Agency Chief Information Officers

FROM: Patricia E. Healy 
Deputy Chief Financial Officer

JAN 16 2007

Jerry Williams 
Deputy Chief Information Officer

JAN 16 2007

SUBJECT: Consolidation of IT internal control deficiencies

As you are aware, the Office of the Chief Financial Officer (OCFO) and the Office of the Chief Information Officer (OCIO) joined together this year to address the Department's ongoing Information Technology (IT) material internal control weakness and to provide leadership and direction in remediating this weakness.

As Co-Chairs of the IT Executive Steering Committee, we have recognized the need for a comprehensive set of data for all IT weaknesses/vulnerabilities and planned corrective actions that exist department-wide. This comprehensive data set will assist us in focusing and monitoring our efforts in resolving this material internal control weakness.

At this time, the Department uses two systems to track such information. The Automated Security Self-Evaluation and Remediation Tracking (ASSERT) system assists managers in gathering system data, managing remediation activities for IT weaknesses, and creating reports in support of Federal Information Security Management Act (FISMA). As you know, the Department uses the ASSERT system to meet its obligations under the FISMA. The second method is through Corrective Action Plan (CAP) manual process for tracking A-123 remediation activities.

The Data Analysis Task force, under the direction of the IT Executive Steering Committee, examined data within the ASSERT system and identified the need for agencies to:

- Expand the scope of existing FISMA Plan of Actions and Milestones (POA&Ms) in ASSERT to include overlapping/similar IT deficiencies that were identified in the OMB Circular A-123 assessment process.

- Create new POA&Ms in ASSERT for any outstanding A-123 IT deficiencies that are not similar to an existing POA&M.
- Include the applicable security control from the National Institute of Standards and Technology (NIST) Special Publication 800-53 within the POA&M records in ASSERT.

Effective immediately, agencies shall take the above actions in order for the ASSERT system to include all current IT weaknesses/vulnerabilities and planned corrective actions that exist department-wide. In addition to providing us with a comprehensive data set of IT deficiencies and corrective actions, these steps should allow us to replace the existing manual process of reporting A-123 remediation activities for IT deficiencies with the automated process of POA&M reporting.

Our Data Analysis Task force, which is led by Michael A. Fiene, is currently meeting with each agency CIO and CFO to discuss this consolidation of IT deficiencies into the ASSERT system.

If you have any questions, please contact either Patricia Healy at (202) 720-0727 or Jerry Williams at (202) 720-8833.