March 8, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum/RA/
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS (OIG-05-A-18)

REFERENCES: DEPUTY EXECUTIVE DIRECTOR FOR INFORMATION SERVICES AND ADMINISTRATION AND CHIEF INFORMATION OFFICER, OFFICE OF THE EXECUTIVE DIRECTOR FOR OPERATIONS MEMORANDUM DATED FEBRUARY 6, 2006

Attached is the Office of the Inspector General's analysis and status of recommendations as discussed in the agency's responses dated February 6, 2006. Recommendations 1 through 8 are resolved. Please provide an updated status of the resolved recommendations by September 30, 2006.

If you have any questions or concerns, please call me on 415-5915.

Attachments: As stated

cc: W. Dean, OEDO
M. Malloy, OEDO
P. Tressler, OEDO

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 1:	Provide users guidance for implementing security controls on standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. The Office of Information Services (OIS) will develop guidance for implementing security controls on standalone PCs and laptops. The guidance will be posted in the computer security web page and offices will be notified that the guidance is available. Completion date: August 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives a copy of the guidance and determines that it clarifies the roles and responsibilities of users for implementing security controls on standalone PCs and laptops.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 2:	Develop and require users to sign a rules of behavior agreement accepting responsibility for implementing security controls on standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. OIS will develop a standard rules of behavior implementing security controls on standalone PCs and laptops. The standard agreement will be posted on the computer security web page and offices will be notified of the requirement for all users of standalone PCs and laptops to sign the agreement as a condition for using any standalone PC or laptop. Completion date: March 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives the standard agreement for review and determines the applicability of the standard rules of behavior agreement.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 3:	Develop and implement procedures for verifying all required security controls are implemented on standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. OIS will develop procedures for verifying all required security controls are implemented on standalone PCs and laptops. OIS will then work with the offices to implement the procedures to ensure that required security controls are implemented on standalone PCs and laptops. Completion date: December 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG reviews the procedures and confirms that they have been implemented.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 4:	Provide users guidance on compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. OIS will develop clear guidance on compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. OIS will then post the guidance on the computer security web site and will notify all offices that the guidance is available. Completion date: August 31, 2006
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the guidance on compliance with Executive Order 13103, Computer Software Piracy, and confirms the posting of the guidance on the computer security web site notifying all offices that the guidance is available.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 5:	Develop and require users to sign a rules of behavior agreement acknowledging their compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. OIS will develop a standard rules of behavior agreement for users to acknowledge their compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. The standard agreement will be posted on the computer security web page and offices will be notified of the requirement for all users of standalone PCs and laptops to sign the agreement as a condition for using any standalone PC or laptop. Completion date: August 31, 2006
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the agency's standard rules of behavior agreement for users to acknowledge their compliance with the conditions for using any standalone PC or laptop.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 6:	Develop and implement procedures for monitoring compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops.
Response Dated February 6, 2006:	Agree. OIS will develop procedures for monitoring compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. OIS will then work with the offices to implement the procedures to ensure compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. Completion date: August 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG receives and evaluates the procedures for monitoring compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 7:	Develop detailed procedures in the appropriate Management Directives for the disposal of equipment used to process safeguards and/or classified information. These procedures should then be referenced in the appropriate chapters of the Volume 12 series of directives.
Response Dated February 6, 2006:	Agree. The Office of Administration (ADM) will develop procedures in the appropriate Management Directives for the disposal of equipment used to process safeguards and/or classified information. These procedures will then be referenced in the appropriate chapters of the Volume 12 series of directives. Completion date: January 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG verifies that the directives have been updated to include procedures for the disposal of equipment used to process safeguards and/or classified information.
Status:	Resolved.

Audit Report
Audit of the System Evaluation of Security Controls for Standalone Personal Computers and Laptops
OIG-05-A-18

Status of Recommendations

Recommendation 8:	Include the procedures for the disposal of equipment containing safeguards and/or classified information in the security plan templates.
Response Dated February 6, 2006:	Agree. OIS will modify the security plan templates for standalone systems that process Safeguards Information or classified information to reference the procedures for the disposal of equipment containing safeguards and/or classified information. Completion date: March 31, 2007
OIG Analysis:	The proposed corrective action addresses the intent of OIG's recommendation. This recommendation will be closed when OIG verifies that the modified security plan templates include the citations to reference the appropriate disposal procedures.
Status:	Resolved.