



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

May 23, 2007

Control Number
ED-OIG/A19G0012

William Vajda
Chief Information Officer
Office of the Chief Information Officer
U.S. Department of Education
550 12th Street, SW
Washington, DC 20202

Dear Mr. Vajda:

This **Final Audit Report**, (Control Number ED-OIG/A19G0012) presents the results of our audit of the *Termination of EDNet Access for Separated Employees*. The objectives of our audit were (1) to determine whether access to the Department of Education (Department) Network (EDNet) was terminated timely for employees who separated from the Department, and (2) in cases where access was not terminated timely, determine whether separated employees accessed EDNet after their departure, and if so, assess the impact of that access. Overall, we found improvements are needed in the Department's process for terminating EDNet access for separated employees.

BACKGROUND

EDNet is a major information system that supports primary information technology (IT) services for the Department and also serves as the chief communications link between Headquarters' offices and the various regional and satellite offices. It is comprised of the network infrastructure (routers, local area network cables, servers, etc.), desktops, standard desktop software and email, Blackberries, printers, and telephony.

The system is owned and operated by the Office of the Chief Information Officer (OCIO), whose responsibilities include management of the Department's IT Security Program for automated information systems, and development of agency-wide policy for the protection and control of information resources directly or indirectly related to the activities of the Department. This includes policies and procedures related to the creation, modification, and termination of EDNet user accounts. To assist in the achievement of its principal objectives, the Department awarded a

contract for EDNet services effective May 1, 2005. The EDNet contractor provides IT support services including user account management.

The account termination process, as described by Department officials and the EDNet contractor, requires communication within each Principal Office (PO), as well as coordination between the POs, contractor-operated Help Desk, and OCIO. Within the PO, supervisors must notify their Executive Officer when they learn an employee is leaving or has been terminated. They must also complete an Account Termination Form (ATF) and submit this for approval by the PO IT Coordinator. The PO IT Coordinator approves and submits the ATF to the Help Desk for processing.

When the ATF is received, the Help Desk creates an electronic record (Help Desk Ticket) to track the request. The Help Desk Ticket must be forwarded to the EDNet Account Manager, an OCIO employee, for review and approval before any further action is taken. If approved, the EDNet Account Manager sends the request back to the Help Desk, who disables the individual's EDNet access and marks their account for deletion.¹ After 15 workdays, the Help Desk deletes the account from the Active Directory (AD), a listing of all network accounts.

Ongoing monitoring occurs in the form of account revalidations, performed by OCIO at the end of each month to identify accounts that have not been accessed over the previous 90 days. A list of inactive accounts is provided to the POs for confirmation of employee status. If the PO determines an employee has separated from the Department, it notifies the EDNet Account Manager, who completes and submits an ATF to the Help Desk for processing.

AUDIT RESULTS

We found improvements are needed in the Department's process for terminating EDNet access for separated employees. We determined requests for account terminations were not submitted timely, documentation of Help Desk actions was not always maintained, and procedures established to identify users whose accounts should be removed were not followed. As a result, accounts belonging to former employees remained active after their separation from the Department. Because these accounts remained active, six permanently separated individuals accessed their email accounts after their separation date. These separated employees may have used the Department's computer systems for unauthorized purposes.

In its response to the draft audit report, OCIO concurred with the finding and all associated recommendations. OCIO proposed corrective actions to strengthen controls to ensure the timely

¹ It is important to note that disabled accounts are no longer active and cannot be accessed by the separated employee. The account disable period exists so that, should anything occur that would require the account to be re-enabled (i.e., need for user files, etc.), it can be done so relatively easily.

and coordinated termination of EDNet access for separated employees. The complete text of the response is included as Attachment 4 to this report.

FINDING – Improvements Are Needed in the Department’s Process for Terminating EDNet Access for Separated Employees

We reviewed data related to personnel who separated from the Department in Fiscal Year (FY) 2006 and noted the following:

- POs did not request the termination of EDNet access for separated employees in accordance with established standards. Specifically, POs did not submit ATFs used to start this process in a timely manner. Of the 389 accounts for which PO-initiated Help Desk Tickets were located, 195 (50 percent) included ATFs that were submitted more than 2 workdays after the employee’s departure from the Department (see **Attachment 1**). On average, POs waited 11 workdays after the employee’s separation date before submitting an ATF to the Help Desk for processing. We noted failure to submit ATFs in a timely manner was systemic throughout the Department.²
- Help Desk Tickets were not available for 83 of the 487 accounts (17 percent) that were no longer in the AD or were inactive.
- Procedures designed to identify users whose accounts should be removed were not followed. Specifically, we found the Office of Management’s (OM) Human Resources Systems Team (HRS) no longer provides OCIO with a biweekly report on personnel changes.

Handbook OCIO-01, *Handbook for Information Assurance Security Policy* (Handbook), dated March 31, 2006, Section 4.1.5, states,

Supervisors shall notify system administrators within two (2) business days of the departure of employees and contractors; notification shall be immediate in the case of involuntary separation. System access for voluntarily separated personnel shall be terminated as soon as possible, but no later than two business days of notification. Access for involuntarily separated personnel shall be revoked immediately. This applies to passwords, account user IDs, and all other access devices. When an employee or contractor’s termination is processed, system administrators must be advised immediately by the designated supervisor to disable or delete all accounts.

Standard Operating Procedure OCIO Computer Help Desk (Help Desk SOPs), dated October 12, 2006, Section 3.5.2, states,

² In discussions with OCIO and Help Desk staff, and through review of the EDNet Access Control and Help Desk SOPs, it was noted that ATFs are the expected form of notification when requesting the termination of an employee’s accounts, and that all accounts should be disabled within 48 hours of an employee’s separation from the Department. This would require that POs notify system administrators within two (2) business days of departure, as specified in the Handbook. Help Desk staff further stated requests lacking ATFs will not be processed.

Closing the OCIO Computer Help Desk Ticket is the final step in problem resolution. The OCIO Computer Help Desk is responsible for closing all OCIO Computer Help Desk Tickets.

The OCIO Computer Help Desk Ticket is available for a specified period for [service level agreement] SLA reporting, Root Cause Analysis, and Customer Status requests. At specified intervals, the Closed OCIO Computer Help Desk Tickets are archived or purged from the Problem Management System database.

The *EDNet Support Services Contract* (Contract) also includes documentation requirements for Help Desk service requests. Table 71 (Help Desk Administration Roles and Responsibilities) states the EDNet contractor shall,

...Provide a system to document, manage and track all requests for service, problem reports and inquiries regardless of the means by which the request is submitted (e.g., telephone, email, fax, direct online input by end-users, etc.), ... Monitor and track all requests for service to closure.

According to *Standard Operating Procedure EDNet Access Control* (EDNet Access Control SOPs), dated March 22, 2006, Section 7.4, OM HRS provides OCIO and the Help Desk with a biweekly report on personnel changes in the Department. This procedure is intended to lessen security risks and support the EDNet security policy to maintain the integrity of the user database. Upon receipt of the report, the Help Desk updates the EDNet Exchange and Windows account database.

As shown in **Attachment 2**, a lack of clear guidance regarding the account termination process in various Departmental policies and procedures contributed to delays in the termination of EDNet accounts for separated employees. For example, Departmental Directive OM: 3-104 (Directive), *Clearance of Personnel for Separation or Transfer*, does not explicitly state that POs must complete and submit an ATF to the Help Desk when an employee separates from the Department. Although ensuring the termination of network access is listed as a responsibility of the Executive/Administrative Officer on an attachment to the Directive, how this is to be done, and in what time frame, is not addressed. As further shown in **Attachment 2**, there is conflicting guidance relating to responsibilities and timeliness requirements in the *Handbook for Information Assurance Security Policy, Information Technology Security Controls Reference Guide*, and *EDNet System Security Plan*.

We found there is no specific time requirement for the retention of documentation related to account terminations in the Department's policies and procedures, EDNet Access Control and Help Desk SOPs, or the Contract. We contacted the EDNet contractor to determine how an account could be disabled without an associated Help Desk Ticket, either generated per PO request or as a result of the name appearing on the 90-day inactivity report, but the contractor was unable to provide a definitive explanation. We asked if the Help Desk Tickets were purged or archived from the system, as specified in the Help Desk SOPs, but contractor staff were unable to confirm whether or not this occurred.

We learned the decision to discontinue use of OM HRS' biweekly personnel change report was made by OCIO in September 2005. OCIO staff stated the EDNet contractor was already producing a 90-day report that listed inactive accounts as part of its revalidation process, and that the OM HRS report often included extraneous information (i.e., data on individuals changing POs, changes in the status of interns and other temporary employees, etc.) that made it difficult to determine which accounts needed to be terminated and which ones were to remain active. We were also told that because the biweekly report came from the payroll system, it was generally about three weeks behind. As a result, by the time OCIO obtained the list of names, the employees had been separated for weeks.

Failure to terminate access for separated employees may result in the exploitation of computer systems for unauthorized use. It also increases the vulnerability of agencies to fraud and abuse.

Without adequate documentation to support requests for account terminations and actions taken, the Department lacks assurance that accounts have been terminated in accordance with established policies and procedures. This may also result in an inability to track requests internally, provide feedback when customers seek updates, and assess the overall efficiency and effectiveness of the process.

Failure to coordinate with OM HRS prevents OCIO and Help Desk staff from identifying inactive accounts in a more timely manner (i.e., sooner than after 90 days of inactivity). In addition, because the 90-day report identifies only those accounts that have been inactive, it is possible that employees who left the Department but did not have their accounts terminated could continue to access the system(s) and never show on the EDNet contractor's report.

Interim Audit Memorandum Issued

We issued an interim audit memorandum entitled, "Termination of EDNet Access for Separated Employees," to OCIO on December 12, 2006. The memorandum included the names of 45 individuals who separated from the Department in FY 2006 but remained in the AD as of October 25, 2006. OCIO responded, indicating that the accounts for all but 13 individuals, who were determined to be active employees, were subsequently deleted. We determined these individuals returned to the Department after separating in FY 2006.

We determined six of the permanently separated individuals accessed their email accounts after their separation date. Although this represents only a small percentage of employees who separated from the Department in FY 2006, the impact of just one individual accessing a system with malicious intent could be substantial. We are currently conducting further analyses to determine whether any of these individuals accessed other Department systems, and for what purpose. Due to the time required to complete these analyses, the results are not included in this audit report.

Recommendations:

We recommend that the Chief Information Officer take the following actions to ensure EDNet access for separated employees is terminated in a timely manner:

- 1.1 Review the *Handbook for Information Assurance Security Policy, Information Technology Security Controls Reference Guide*, the Department's Directive on the *Clearance of Personnel for Separation or Transfer*, and the *EDNet System Security Plan* and make revisions, as necessary, to ensure consistency of guidance with regard to timeliness of notification of separation, method of notification (ATF or other acceptable form), and account termination. Consider consolidating some of these documents, if feasible, to reduce duplication and confusion.
- 1.2 Revise the clearance form (ED Form EP2) to require PO Information Technology coordinators to certify that an ATF has been completed and will be submitted to the Help Desk immediately upon the employee's separation from the Department.
- 1.3 Amend the Department's policies and procedures, EDNet Access Control and Help Desk SOPs, and the Contract to establish consistent guidance on the retention period for requests and other supporting documentation related to account terminations, as well as archiving and purging procedures and timeframes.
- 1.4 Work with OM HRS to develop and implement a report for biweekly submission that includes only the names of those individuals who separated from the Department in the preceding pay period, and other information deemed relevant to OCIO. Ensure the appropriate termination of EDNet access for all separated employees.

OCIO Response:

In its response to the draft report, OCIO concurred with the finding and all associated recommendations. OCIO stated it will revise policies and procedures to ensure consistency of guidance with regard to the timeliness of notification of account terminations, as well as the retention period for related requests, and consolidate documentation where feasible to reduce duplication and confusion. In addition, it will revise the clearance form to require PO IT coordinators to certify that an ATF has been completed and submitted when an employee leaves the Department. Furthermore, OCIO will work with OM HRS to implement a process for acquiring a biweekly report of recent employee separations. OCIO also noted it expects to make significant improvements to the EDNet security posture after the award of the Managed Services Security Provided (MSSP) and EDUCATE acquisitions.

OTHER MATTERS

During our review, we noted no warning against unauthorized access of systems is provided when individuals attempt to log in to their email accounts remotely via Outlook Web Access (<http://email.ed.gov>). Such a warning not only would serve as a possible deterrent and valuable security practice, but also is required by law.

The Department's *Information Technology Security Controls Reference Guide*, referencing Public Law 99-474, states that, "...if a system uses any external telecommunications mediums (e.g. dial-up, Internet, etc), a warning banner must appear before the log-on sequence." Furthermore, the banner, "must state that the system is a U.S. Government system, information contained in it is 'For Official Use Only' ([sic] FOUO), and that attempts to illegally log on to the system could lead to criminal prosecution punishable by fines or imprisonment."

The *Handbook for Information Assurance Security Policy* states,

Department computers and IT systems must display a sign-on warning banner at all log-on points, where technically practical. . . . At a minimum, warning banners must state that the use of the Department IT systems is subject to monitoring and is for limited personal use by Department personnel; all data contained on Department IT systems are property of the U.S. Government; and there can be no expectation of personal privacy on the Department IT systems.

We also noted the clearance form (**Attachment 3**) does not require employees to certify that they will not attempt to access their email or any other systems once they have left the Department.

We suggest the CIO take the necessary steps to bring the Department into compliance with the law as well as Department policy. We also suggest that the CIO revise the clearance form to provide for the appropriate employee certification regarding unauthorized system access.

OCIO responded to the Other Matters presented, stating it has already implemented a new warning banner on Outlook Web Access. OCIO also indicated it will revise the clearance form to require employees to certify that they will not attempt to access their email or any other systems once they have left the Department.

OBJECTIVES, SCOPE, and METHODOLOGY

The objectives of our audit were (1) to determine whether access to EDNet was terminated timely for employees who separated from the Department, and (2) in cases where access was not terminated timely, determine whether separated employees accessed EDNet after their departure, and if so, assess the impact of that access. To accomplish our objectives, we performed a review of internal control applicable to the account termination process. We reviewed applicable laws and regulations, and Department and EDNet contractor policies and procedures. We conducted interviews with Department officials and EDNet contractor staff to gain an understanding of how EDNet accounts are terminated.

The scope of our review included employees who separated from the Department during FY 2006. We obtained a list of employees who separated from the Department in FY 2006 from OM HRS. This list contained 530 records. We compared these records to a list of deleted

accounts obtained from the OCIO to determine if and when user accounts were deleted. We also compared the list of separated employees to a list of accounts in the AD obtained from the EDNet contractor to determine whether any accounts remained active after an employee separated from the Department. See table below for a breakout of accounts:

Description	Count
Separated Employee, No AD Account	394
Separated Employee, Inactive AD Account	93
Separated Employee, Active AD Account	43
TOTAL	530

We determined that 487 of the 530 accounts belonging to employees who separated from the Department in FY 2006 were no longer in the AD or were inactive as of October 25, 2006. We evaluated the timeliness of account terminations for these 487 accounts. To do this, we reviewed the Help Desk Tickets generated by the EDNet contractor upon receipt of each ATF. We located Help Desk Tickets for 404 of the 487 employees (83 percent) whose accounts were no longer active. We determined 14 of these were generated by the EDNet Account Manager as a result of the individual appearing on the 90-day inactivity list, meaning an ATF was likely never submitted by the PO. These 14 were not included in our analysis of timeliness as a result. We also judgmentally decided to remove one name because the account was disabled months before the PO submitted the ATF.

We reviewed the Help Desk Tickets for the remaining 389 accounts to determine the average time between an employee's separation from the Department and PO submission of an ATF. We also reviewed the Help Desk Tickets to determine the average time between receipt of an ATF and disabling of the account by the EDNet contractor.

We relied on computer-processed data initially obtained from OM HRS to identify the universe of employees who separated from the Department in FY 2006. An alternate data source was not available to directly test the accuracy or completeness of this data. As a result, we were not able to validate the reliability of the data provided by OM HRS. However, because this data was used as a starting point for the reconciliation process, we deemed it sufficiently reliable for purposes of our audit.

We conducted fieldwork at Department offices in Washington, DC, during the period of October 11, 2006 through January 30, 2007. We provided our audit results to OCIO staff during an exit conference conducted on February 20, 2007. Our audit was performed in accordance with generally accepted government auditing standards appropriate to the scope of the review described above.

ADMINISTRATIVE MATTERS

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). Department policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the finding and recommendation contained in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with the Freedom of Information Act (5 U.S.C. § 522), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation provided to us during this review. Should you have any questions concerning this report, please call Michele Weaver-Dugan at (202) 245-6941. Please refer to the control number in all correspondence related to the report.

Sincerely,

George A. Rippey /s/
Acting Assistant Inspector General for Audit Services

cc: Sally Budd, Chief of Staff
Stephanie Hammes, Audit Liaison Officer

Attachments

Attachment 1

PO	No. of accounts for which Help Desk Tickets were located:	No. of accounts for which ATF was NOT submitted by the PO within 2 workdays of separation date:	Percent NOT submitted in a timely manner:	Average no. of days between separation date per OM and submission of ATF (per Help Desk Ticket):
FSA	99	46	46.46%	9
IES	13	12	92.31%	13
NAGB	1	1	100.00%	3
NIL	1	0	0.00%	(2)
OCFO	21	5	23.81%	6
OCIO	9	3	33.33%	10
OCO	19	16	84.21%	19
OCR	38	20	52.63%	19
ODS	4	0	0.00%	1
OELA	1	1	100.00%	12
OESE	19	8	42.11%	8
OGC	2	1	50.00%	58
OIG	21	2	9.52%	6
OII	9	8	88.89%	23
OLCA	2	2	100.00%	20
OM	24	10	41.67%	10
OPE	21	5	23.81%	1
OPEPD	10	4	40.00%	4
OS	22	8	36.36%	13
OSDFS	6	4	66.67%	7
OSERS	36	33	91.67%	17
OUS	2	0	0.00%	0
OVAE	9	6	66.67%	24
TOTALS	389	195	50.13%	

Attachment 2

Criteria	Deactivation for Voluntary Separation	Deactivation for Involuntary Separation	Identified Action Officials	Use of ATF Included in Criteria
Section 4.1.5 of the Handbook for Information Assurance Security Policy	Two work days for a supervisor to notify system administrators of employee's separation and then up to two additional work days after notification for account termination	Immediately	Supervisor and System Administrators	No
Section 4.1.1 of the Information Technology Security Controls Reference Guide	Within 24 hours of the employee's separation from the Department	Immediately	Not established	No
Section VI.E of the Directive on Clearance of Personnel for Separation or Transfer, and ED Form EP2	Not established	Not established	Executive Officer and OCIO	No
Section 5.1.3.1.5 of the EDNet System Security Plan	Within 24 hours of notification	Within 24 hours of notification, or immediately if requested	Principal Office Coordinator or Computer Security Officer and EDNet Account Manager	No

Attachment 3

Clearance of Personnel for Separation or Transfer			
Name of employee (Last, First, and Middle Initial)			
Forwarding address		Name of organization	
		Building and room #	Office Phone #
		Home Phone #	
Reason for separation			
<input type="checkbox"/> Resignation <input type="checkbox"/> Transfer to another		<input type="checkbox"/> Retirement <input type="checkbox"/> Involuntary	
<input type="checkbox"/> Other (specify)			
_____ federal agency		_____ separation	
Date SF 52 initiated	Date of separation	<input type="checkbox"/> Position sensitive	<input type="checkbox"/> Position non-sensitive
Part I – Executive/Administrative Officer			
A. Appropriate action must be taken to obtain clearances in the areas shown below. <i>Do NOT check boxes until clearances are obtained.</i>			
<input type="checkbox"/> Advanced annual leave (# of hours _____) <input type="checkbox"/> Travel advances <input type="checkbox"/> Advanced sick leave (# of hours _____) <input type="checkbox"/> Property release <input type="checkbox"/> Computer property <input type="checkbox"/> Training agreements <input type="checkbox"/> Network access terminated <input type="checkbox"/> Service agreements <input type="checkbox"/> Data files <input type="checkbox"/> Overpayments (one example is Salary Overpayments)			
Comments			
Exit interview – GS-15 and above		Date clearance package issued to employee	
<input type="checkbox"/> Yes <input type="checkbox"/> No			
B. Must be cleared by last day <i>Do NOT check boxes until clearances are obtained.</i>			
<input type="checkbox"/> Parking permit <input type="checkbox"/> Office property <input type="checkbox"/> Photo ID <input type="checkbox"/> Telephone calling cards <input type="checkbox"/> Transit benefits <input type="checkbox"/> Travel card			
Comments			
Part II – Security Services			
<i>Do NOT check boxes until clearances are obtained</i>			
<input type="checkbox"/> Security determination (debriefed)		<input type="checkbox"/> Special ID Pass	
Certification			
I understand that if I have outstanding obligations that have not been satisfied before my last day in the Department that my final paycheck and lump sum annual leave will not be released. I also understand that my retirement fund may be offset. (5 U.S. Code 5514)	Signature of employee		Date
	For return of government purchase card.		Date
	Employee cleared all items. Arrangements have been made for the employee to make restitution for monies owed.		Date
		Signature of OCFO/CAM	Date
		Signature of Executive Officer	Date
ED Form EP2			



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

DATE: May 11, 2007

TO: George Rippey
Acting Assistant Inspector General for Audit Services
Office of Inspector General

FROM: William Vajda
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Response to Draft Audit Report ED-OIG/A19G0012

Thank you for your draft audit report, *Termination of EDNet Access for Separated Employees, ED-OIG/A19G0012* dated March 19th, 2007. The Department sincerely values the audit activity conducted by the Office of the Inspector General (OIG) and appreciates the benefits of the collaborative environment between OIG and the Department, formed through many years of partnering and the sharing of mutual goals and objectives. The Department concurs with all findings described in the aforementioned audit report.

Strong logical access control policies and procedures are essential to ensuring that information resources and the information that they process, store and transmit are adequately protected by maintaining confidentiality, integrity and availability. The Department concurs with the OIG's findings that weaknesses exist in the implementation of logical access control, particularly in the areas of AC-1, *Access Control Policies and Procedures*, AC-2, *Account Management* and AC-3, *Access Enforcement* as promulgated by NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* and the Department's policies for access control.

The Office of the Chief Information Officer (OCIO) in coordination with the Office of Management (OM) fully intends to implement the recommendations of the OIG in strengthening access controls on EDNet through timely and coordinated termination of logical access as mandated by policy. Additionally, the Department expects to make significant improvements to the EDNet security posture after the award of the Managed Services Security Provider (MSSP) and EDUCATE acquisitions.

Corrective Action Plan

Table 1.0 describes the corrective actions that will take place to remediate the findings presented by the OIG. Proposed corrective actions will be entered in the AARTS and as each finding is completed, evidence demonstrating remediation will be submitted to the Office of the Chief Financial Officer (OCFO) for records management by the Post Audit Group (PAG).

Table 1.0 Corrective Action Plan

1.1	Review the <i>Handbook for Information Assurance Security Policy</i> , <i>Information Technology Security Controls Reference Guide</i> , the Department's Directive on the <i>Clearance of Personnel for Separation or Transfer</i> , and the <i>EDNet System Security Plan</i> and make revisions, as necessary, to ensure consistency of guidance with regard to timeliness of notification of separation, method of notification (ATF or other acceptable form), and account termination. Consider consolidating some of these documents if feasible to reduce duplication and confusion.	The Department will revise policies, procedures and Directives as necessary to ensure consistency of guidance with regard to timeliness of notification of account termination. Furthermore, the Department will consolidate documentation where feasible to reduce duplication and confusion.	August 31, 2007
1.2	Revise the clearance form (ED Form EP2) to require PO Information Technology coordinators to certify that an ATF has been completed and will be submitted to the help desk immediately upon the employee's separation from the Department.	The Department will revise clearance form (ED Form EP2) to require PO Information Technology coordinators to certify that an ATF has been completed and submitted.	June 30, 2007
1.3	Amend the Department's policies and procedures, EDNet Access Control and Help Desk SOPs, and the Contract to establish consistent guidance on the retention period for requests and other supporting documentation related to account terminations, as well as archiving and purging procedures and timeframes.	The Department's will amend relevant policies and procedures, EDNet Access Control, Help Desk SOPs, and the Contract to establish consistent guidance on the retention period for requests related to account terminations.	August 31, 2007
1.4	Work with OM HRS to develop and implement a report for biweekly submission that includes only the names of those individuals who separated from the Department in the preceding pay period, and other information deemed relevant to OCIO. Ensure the appropriate termination of EDNet access for all separated employees.	The Department will work with OM HRS to implement a process for acquiring a report for biweekly submission that includes only the names of those individuals who separated from the Department in the preceding pay period.	June 30, 2007
1.5	No warning against unauthorized access of systems is provided when individuals attempt to log in to their email accounts remotely via Outlook Web Access. We suggest the CIO take necessary steps to bring the Department into compliance with the law as well as Department policy.	The Department has implemented the new warning banner on Outlook Web Access.	April 21, 2007
1.6	Clearance Form, ED Form EP2, does not require employees to certify that they will not attempt to access their email or any other systems once they have left the Department. We also suggest that the CIO revise the clearance form to provide for the appropriate employee certification regarding unauthorized system access.	The Department will revise clearance form, (EP2) that will require employees to certify that they will not attempt to access their email or any other systems once they have left the Department.	June 30, 2007

CC:

Michell Clark, Assistant Secretary for Management, OM
 Brian Burns, Deputy CIO, OCIO
 Jerry L. Davis, Director, Information Assurance, OCIO
 Corey Wells, Senior Advisor to OCIO