TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Managers and System Administrators Need to Limit Employees' Access to Computer Systems

July 2005

Reference Number: 2005-20-097

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-927-7037
Email Address | Luis.Garcia@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 8, 2005

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Managers and System Administrators Need to Limit Employees' Access to Computer Systems (Audit # 200420036)

This report presents the results of our review to assess the effectiveness of the Internal Revenue Service's (IRS) controls over authorizing user access to its computer systems. A fundamental principle of effective computer security is employees should be given access to only those systems and applications for which they have a business need. Giving employees access beyond their job responsibilities creates unnecessary opportunities for unauthorized access to or misuse of tax return data, such as selling data for identity theft purposes.

In prior Treasury Inspector General for Tax Administration reviews, we have identified weaknesses where IRS employees or former employees had unnecessary access to tax data. The IRS implemented the Online 5081 (OL5081) system[1] in July 2002 to address these deficiencies.

Synopsis

By implementing the OL5081 system and related processes, the IRS has taken a major step to improve the process of authorizing user access to IRS systems. For example, the automated process for requesting and approving access to systems is less cumbersome and eliminates the need for paper forms to be sent and received by various parties throughout the process. Authorizing access to an account, which took weeks using the paper Information System User Registration/Change Request (Form 5081), can now be done as quickly as 1 day.

[1] The OL5081 system was named after the Information System User Registration/Change Request (Form 5081) the IRS uses to request and authorize user accounts for employees on all systems. The OL5081 system automates some of the manual processes and provides a centralized system for all system access authorizations.

Nevertheless, we identified the same three problems we reported before the implementation of the OL5081 system. These weaknesses continue to occur because managers and system administrators have not adhered to the OL5081 system procedures.

First, managers and system administrators did not ensure user accounts for employees were removed from systems when employees left the IRS, transferred to another function, or changed job responsibilities. Keeping these user accounts active increased the risk they could be used for unauthorized disclosure of taxpayer data.

Second, managers and system administrators did not have documentation of employees' access authorizations. One possibility is managers did not ensure all system users were added to the OL5081 system when the IRS converted from paper to the automated system. Another explanation is system administrators may have granted employees access to systems without proper authorization from the employees' managers. Without the required documentation, accountability for authorizing access could not be determined. The lack of documentation to support employee access increases the risk that employees could have more access than needed.

Finally, those employees not included on the OL5081 system were never required to acknowledge awareness of their security responsibilities. In addition, some managers and employees did not appear to act on reminders generated by the OL5081 system to recertify their awareness of security policies and procedures. Requiring employees to acknowledge security rules before being granted access to a system and requiring annual recertification promotes employee awareness of security policies and can make the IRS a more security-minded organization.

Recommendations

We recommended the Chief Information Officer enforce current procedures by configuring systems to automatically disable users' accounts after 45 days of inactivity and to automatically delete the accounts after 90 days of inactivity. We also recommended the OL5081 system be enhanced to automatically generate notifications to system administrators when employees have not recertified their awareness of security rules within 45 days. System administrators should disable access privileges for those employees until they reapply for access and recertify their awareness of security rules. We also recommended the Chief, Mission Assurance and Security Services, coordinate with the business units to include tests of access controls during annual self-assessments required by the Federal Information Security Management Act (FISMA).[2]

[2] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

Response

The IRS agreed with our recommendations. However, it noted that disabling and deleting accounts for inactivity cannot be applied to all systems. Certain systems exist where employee inactivity beyond the recommended time periods is normal. These systems require employee access only upon completion of a specific activity, such as travel and training. We concur with these comments.

The Chief Information Officer will issue a revised policy statement requiring the timely deletion or disabling of inactive accounts in accordance with current procedures and the evaluation of the feasibility of automating the deletion and disabling of unused accounts. In addition, the Chief Information Officer implemented enhancements to the OL5081 system so employees and managers will be unable to perform any actions on a system until annual recertifications have occurred. The Chief, Mission Assurance and Security Services, will coordinate with the other business units for conducting testing of access controls, as part of the IRS' annual FISMA processes. Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background....................Page 1

Results of Review....................Page 3

The Online 5081 System Improves the User Account Authorization Process....................Page 3

Managers and System Administrators Did Not Carry Out Their Responsibilities....................Page 3

Recommendations 1 and 2:....................Page 8

Recommendation 3:....................Page 9

Appendices

Appendix I – Detailed Objective, Scope, and Methodology....................Page 10

Appendix II – Major Contributors to This Report....................Page 12

Appendix III – Report Distribution List....................Page 13

Appendix IV – List of Treasury Inspector General for Tax Administration Audit Reports With Unauthorized or Unnecessary User Accounts Issues....................Page 14

Appendix V – Description of Internal Revenue Service Automated Systems Selected for Review....................Page 15

Appendix VI – Management's Response to the Draft Report....................Page 16

Background

The Internal Revenue Service (IRS) has over 300 computer systems to process and maintain over 222 million tax returns. The data in these systems are considered sensitive and require protection from unauthorized use, modification, disclosure, and destruction. The importance of protecting these data was illustrated when the President signed into law the Taxpayer Browsing Protection Act of 1997.[1] This Act makes the willful unauthorized access and inspection of taxpayer records a crime.

A fundamental principle of effective computer security is employees should be given access to only those systems and applications for which they have a business need. Giving employees access beyond their job responsibilities creates unnecessary opportunities for unauthorized access to or misuse of tax return data, such as selling data for identity theft purposes. To limit the opportunities for misuse of sensitive data, the IRS requires that employees be given access to only those systems they need to execute their job responsibilities. To fulfill this requirement, the IRS established the Information System User Registration/Change Request (Form 5081) to request and authorize employees' system user accounts.

The IRS requires that employees be given access to only those systems they need to execute their job responsibilities.

The IRS has acknowledged that procedures associated with the Form 5081 process were not being followed as intended. For example, user accounts for employees who had separated from the IRS were not deleted from systems, or Form 5081 documentation was not being maintained to support proper authorization for access to systems. Since 1998, the IRS had also designated the Separating Employee Clearance process as a significant control deficiency under the Federal Managers' Financial Integrity Act of 1982.[2] The deficiency mainly deals with processes related to employees who leave the IRS, which includes the management and deletion of user accounts for separated employees.

[1] 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).

[2] 31 U.S.C. §§ 1105, 1113, 3512 (2000). This Act requires Federal Government agencies to annually assess the adequacy of controls and identify any areas of control weaknesses, designated as either material weaknesses or significant control deficiencies. The Department of the Treasury defines material weaknesses as "shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements." Significant control deficiencies are defined as "problematic issues which do not rise to the level of materiality, but which warrant special management attention to ensure improvement, rather than deterioration to the point where they become material weaknesses."

Prior Treasury Inspector General for Tax Administration (TIGTA) reviews have also identified similar problems as they related to the Form 5081 process. Appendix IV presents a list of prior audit reports that contain these types of issues.

To address these deficiencies, the IRS automated the process by developing the Online 5081 (OL5081) system.[3] In implementing this system in October 2002, the former Deputy Commissioner required all IRS managers to conduct a thorough review of their employees' access profiles and complete an OL5081 system record for each of their employees with current access privileges. Additionally, in May 2004, the Acting Director, End User Equipment and Services (EUES), required the use of paper Forms 5081 be terminated by November 2004. In December 2004, the EUES organization completed improvements to the OL5081 system, including giving the system a more user-friendly appearance and expanding screen instructions and menu accessibility.

The following five systems were judgmentally selected for our review. Appendix V provides a description of these systems.

- Appeals Centralized Database System (ACDS).
- Automated Collection System (ACS).
- Automated Underreporter System (AUR).
- Integrated Case Processing (ICP).
- Taxpayer Advocate Management Information System (TAMIS).

This review was performed in the Office of Information Technology Services at the IRS National Headquarters in Washington, D.C., during the period July 2004 through January 2005. We also contacted managers located in several IRS locations. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[3] The OL5081 system was named after the Form 5081 the IRS uses to request and authorize user accounts for employees on all systems. The OL5081 system automates some of the manual processes and provides a centralized system for all system access authorizations.

Results of Review

The Online 5081 System Improves the User Account Authorization Process

By implementing the OL5081 system in July 2002, the IRS has taken a major step to improve the process of authorizing user access to IRS systems. The automated process for requesting and approving access to systems is less cumbersome and eliminates the need for paper forms to be sent and received by various parties throughout the process. Authorizing access to an account, which previously took weeks using paper Forms 5081, can now be done in as fast as 1 day. The OL5081 system is used to grant access to almost all IRS systems.

The IRS has taken a major step to improve the process of authorizing user access to its computer systems.

The OL5081 system process starts with an employee completing an online Form 5081 with all required information. When the employee completes the request, the OL5081 system sends an email message to the employee's manager regarding the request. The manager then accesses the OL5081 system to approve the request. Once the request has been approved, the OL5081 system generates an email to the system administrator who creates the user account. The user is then notified his or her user account is active and ready for access.

To delete a user who no longer has a need to access a system, the manager initiates the removal process on the OL5081 system. An email is then sent to the system administrator to remove the account.

In addition to expediting the addition and removal of employees' access rights to a system, the OL5081 system is also used to document that employees have certified they understand IRS security rules. IRS procedures require employees to make this certification annually as a means to enhance security awareness and understanding.

Managers and System Administrators Did Not Carry Out Their Responsibilities

Although the OL5081 system automates the process for creating and deleting user accounts, certain responsibilities continue to rely on human initiation and intervention. For example, managers must ensure employees need access to a system before granting access and promptly notify system administrators to remove employees from a system when access is no longer necessary. Managers are also required to annually review the appropriateness of their employees' access privileges.

In turn, system administrators are responsible for adding and removing system users when authorized, monitoring users' accesses, maintaining an up-to-date list of authorized users, and annually generating a list of current system users and their access profiles to provide to the appropriate managers for review.

The Federal Information Security Management Act (FISMA)[4] requires business units to annually conduct self-assessments of the security of their systems. Access to computer systems should be evaluated as part of these self-assessments to determine whether managers and employees have implemented the controls effectively.

However, our review of the five systems identified employees who:

- Had access to systems they did not need to assist them in carrying out their responsibilities.
- Had access to systems that were not properly authorized and documented.
- Had not certified they were aware of IRS security procedures.

These conditions occurred because managers and system administrators did not adhere to OL5081 system procedures. In addition, prior FISMA self-assessments had not addressed access controls.

Employees had access to systems they did not need

In our review of the 5 systems, we identified 139 (21 percent) of 652 employees with active user accounts who, according to their managers, no longer had a business need to have system access. Table 1 presents these numbers by the systems reviewed.

[4] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

Table 1: Active Accounts With and Without a Business Need

Systems	Number of Total Users	Number of Users in Our Sample	Number of Users Without a Business Need	Number of Users With a Business Need
ACDS	2,464	113	5	108
ACS	5,297	166	26	140
AUR	2,319	88	17	71
ICP	34,342	167	82	85
TAMIS	3,235	118	9	109
Total	47,657	652	139	513

Source: TIGTA analysis.

Discussions with managers of the system account users identified the following reasons why access was no longer needed.

- Employees (54) had separated from the IRS and their managers agreed their access rights should have been removed. One employee who still had access separated from the IRS over 2 years before our review.
- Employees (47) were transferred to other positions.
- Employees (38) remained in their current positions but no longer needed access to the system due to changing job duties.

Managers and system administrators did not follow IRS procedures to terminate these employees' access privileges. The existence of active user accounts for employees who no longer have a business need poses an unnecessary risk for unauthorized disclosure of taxpayer data. Out of the 54 employees who separated from the IRS but still had active user accounts, we identified 5 user accounts that had been accessed after the employees separated from the IRS.

Managers and system administrators did not follow IRS procedures to terminate employees' access privileges.

We have previously reported the issue of unnecessary user accounts on systems in application-specific reviews (see Appendix IV for specific reports.) The implementation of the OL5081 system has had little effect on this issue, even though the system gives managers and system administrators a single place to identify employee access to multiple systems and initiate system separation action when an employee's responsibilities change.

Some systems have the capability to automatically disable an employee's user account if he or she had not accessed the system within a predetermined time period. The IRS requires that an employee's access rights be disabled if he or she has not used a system within 45 days; access rights are to be removed from a system if not the employee has not accessed it within 90 days. System administrators had not configured the systems to ensure these requirements were met.

Employees' access capabilities were not always authorized or documented

Managers did not carry out their responsibilities, or system administrators may have added employees to systems without a manager's authorization.

In our sample of 652 employees, 513 employees had a business need to access the systems. As previously indicated, a manager's authorization is required and must be documented prior to granting a user system access. We found no indications on the OL5081 system that 128 (25 percent) of the 513 employees had been properly authorized. We were also unable to find paper copies of approved authorizations in the employees' personnel folders or from the employees' current managers.

Without the Form 5081 information, it is impossible to determine how these employees obtained access to the systems. We believe either managers did not carry out their responsibilities, or system administrators may have added employees to systems without a manager's authorization.

When the IRS transitioned to the OL5081 system in July 2002, it attempted to enter all paper Forms 5081 into the OL5081 system. We acknowledge this is an ongoing effort and could explain why we were unable to find records on the OL5081 system for all user accounts in our sample. However, managers may not have carried out their responsibilities for ensuring all system users were added to the OL5081 system.

Another explanation for the lack of documentation is system administrators, rather than managers, authorized access to systems. Without documentation of access authorizations, accountability for granting access cannot be readily determined and the risk that employees had more access than needed is increased.

In addition, managers and system administrators will be unable to use the OL5081 system to identify all user accounts for employees who separate from the IRS. To illustrate, when the 128 employees in our sample above separate from the IRS, the OL5081 system will not identify all systems to which the employees have access and the user accounts could remain active and useable. If a former employee was able to enter an IRS facility and logon to an IRS computer, he or she could access the system to obtain tax return data.

Employees did not certify they were aware of IRS security procedures

The IRS requires systems users to know, understand, and agree to practice the rules of system use, prior to accessing a system. Managers must ensure users acknowledge they understand the system security requirements, rules, and responsibilities prior to granting them system access. Managers must also ensure users annually recertify their awareness of the system security rules for all systems to which access has been granted.

These requirements have been automated through the OL5081 system. When users request access to a system, they need to acknowledge, in the OL5081 system, that they understand system security rules. In addition, the OL5081 system automatically sends email reminders to users and their managers when annual recertification is needed.

Of the 513 employees reviewed, 173[5] (34 percent) did not meet their annual recertification requirement indicating their understanding of IRS security rules. Among these 173 employees were 45 employees who had initially certified they understood the security rules over 1 year ago but had not annually recertified their awareness of the security rules. It appears employees and managers did not act on the recertification email reminders generated by the OL5081 system.

Employees and managers did not act on recertification email reminders generated by the OL5081 system.

Requiring employees to acknowledge security rules before being granted access to a system and requiring annual recertification promotes employee awareness of security policies and can make the IRS a more security-minded organization. In not doing so, employees could unknowingly compromise security within the IRS. For example, the system security rules state employees must protect their passwords at all times and should not share them with anyone else regardless of that person's position inside or outside the IRS. A TIGTA audit report[6] on employees' susceptibility to social engineering tactics showed that 35 of 100 managers and employees provided their user accounts and changed their passwords when we posed as an Information Technology helpdesk employee.

To further ensure employees are aware of their security responsibilities, we believe the OL5081 system could be used to systemically generate an email to system administrators for the purpose of disabling user accounts if employees had not recertified.

[5] The 173 employees include the 128 employees whose access rights were never entered into the OL5081 system. There is no indication these 128 employees ever acknowledged the security rules.
[6] *While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques* (Reference Number 2005-20-042, dated March 2005).

Recommendations

***Recommendation 1*:** The Chief Information Officer should enforce current procedures on all systems by configuring systems to automatically disable employees' accounts after 45 days of inactivity and to automatically delete the accounts after 90 days of inactivity.

> ***Management's Response*:** The Chief Information Officer will issue a revised policy statement requiring the timely deletion or disabling of inactive accounts in accordance with current procedures. The policy statement will require each system and application owner to identify inactive accounts and take the appropriate actions to ensure managers and system administrators delete separated employees' accounts from the IRS network, disable user accounts after 45 days of inactivity, and delete accounts after 90 days of inactivity on all applicable systems and applications.
>
> The Chief Information Officer's revised policy will also require each affected system and application owner to evaluate the feasibility of automating the disabling and deletion of unused accounts. The feasibility report will identify the systems and applications that can be automated with a projected schedule to include implementation and completion dates. A justification statement with detailed information will be prepared for each system and application that cannot be automated.

***Recommendation 2*:** The Chief Information Officer should enhance the OL5081 system by automatically generating reminders to system administrators when employees have not recertified their awareness of security rules within 45 days. System administrators should disable access privileges for those employees until they reapply for access and recertify their awareness of security rules. We believe these actions would highlight the importance of annual recertification of system access for users and managers.

> ***Management's Response*:** The Chief Information Officer has completed the following actions. The OL5081 system was reprogrammed to provide account/system administrators with automatic notifications that direct them to disable the accounts of employees who are placed in a furloughed or other nonpay status and to generate automatic notifications to "managers gaining new employees," to validate these employees' system accesses. In addition, the OL5081 system will default to the recertification message requiring a manager to recertify his or her employees each time the manager logs into the OL5081 system, prior to allowing the employees to perform any other action.
>
> In addition, the Chief Information Officer will ensure employee access privileges will be disabled if employees fail to acknowledge or recertify the Information Technology System Security Rules within 45 days of their notification for systems managed by the Modernization and Information Technology Services (MITS) organization. For systems

managed by the business units, system administrators will receive notification and be mandated to disable access privileges for those employees who fail to recertify. The MITS organization will also review a report generated by the OL5081 system that lists all accounts marked for disabling or deletion and notify the appropriate system owner if further action is required.

Recommendation 3: The Chief, Mission Assurance and Security Services, should coordinate with the business units to include tests of access controls during annual self-assessments required by the FISMA. These tests should eventually increase all managers' awareness of their responsibilities to limit employees' system access to those who need it to accomplish their responsibilities, document authorizations to access the systems, and ensure employees recertify their awareness of security procedures.

Management's Response: The Chief, Mission Assurance and Security Services, will coordinate with the other business units for conducting testing of access controls. The testing of management, operational, and technical controls will be implemented as a part of the IRS' annual FISMA processes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the Internal Revenue Service's (IRS) controls over authorizing user access to its computer systems. To accomplish our objective, we:

I. Determined whether the Online 5081 (OL5081) system[1] process is effective in reducing risks associated with users' access to applications.

A. Identified areas of responsibility and work flow processes for the OL5081 system by interviewing:

1. Personnel in the Office of Information Technology Services to determine how the system works, the roles of different individuals (e.g., employee, manager, application project office, system administrators), and the current status of the application rollout implementation.

2. Security personnel and system administrators to determine the procedures for adding and deleting employees and contractors from systems using the OL5081 system.

B. Confirmed whether system users had acknowledged security rules and regulations.

C. Determined whether the OL5081 system provided management with a notification when recertifications were due for users under its jurisdiction.

D. Interviewed IRS management to ascertain why the OL5081 system process was not used when accesses to applications were being granted using a paper Information System User Registration/Change Request (Form 5081).

E. Reviewed the process for establishing managerial approval for authorizing access and determined how those designations were kept current.

II. Determined whether user accounts had been established for only those individuals with a business need.

A. Identified all user accounts for the following five IRS systems:

[1] The OL5081 system was named after the Information User Registration/Change Request (Form 5081) the IRS uses to request and authorize user accounts for employees on all systems. The OL5081 system automates these processes and provides a centralized area for all system access authorizations.

- Appeals Centralized Database System.
- Automated Collection System.
- Automated Underreporter.
- Integrated Case Processing.
- Taxpayer Advocate Management Information System.

These 5 systems were judgmentally selected from over 300 systems based on concurrent audit work on specific applications, sensitivity of data, applicability to IRS employees, and the availability of certain data fields (e.g., date last accessed).

B. Judgmentally selected 66 managers located in several IRS offices.[2] The managers were responsible for 652 employees with active user accounts on these 5 systems. We judgmentally selected the managers because we did not plan to project our audit results.

C. Contacted the managers to determine whether the 652 users truly needed access to the systems.

D. Obtained "last accessed" date for the sample of users selected to determine whether the users had accessed the application within 90 days. For user accounts not accessed within 90 days, we determined whether the account had been disabled or deleted, or we obtained an explanation as to why the user account was still active.

E. Determined whether the selected applications had user accounts for separated employees by cross-referencing user accounts with separated employee data from the IRS' time and attendance system and the OL5081 system, respectively.

III. Determined whether users had been properly authorized for access.

A. Determined whether policies and guidelines had been followed and employees had been properly authorized for access to applications by obtaining the Form 5081 (electronic or paper) for the sample selected in Step II. B.

B. Determined whether temporary authority to approve access to applications had been properly controlled.

C. Determined whether recertifications were timely completed.

[2] We could not readily determine the population of managers for each system because two of the five systems did not contain manager names for each user account. For those systems, we had to conduct specific queries and research the IRS' Discovery Directory to identify managers for our sample.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Audit Manager
Myron Gulley, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Midori Ohno, Senior Auditor
William Simmons, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Wage and Investment Division SE:W
Chief, Appeals AP
National Taxpayer Advocate TA
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Business Systems Development OS:CIO:I:B
Director, End User Equipment and Services OS:CIO:I:EU
Director, Enterprise Operations OS:CIO:I:EO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief Information Officer OS:CIO
    Chief, Mission Assurance and Security Services OS:MA

Appendix IV

List of Treasury Inspector General for Tax Administration Audit Reports With Unauthorized or Unnecessary User Accounts Issues

In the following five Treasury Inspector General for Tax Administration audit reports, we reported employees had access to systems they did not need to carry out their responsibilities and user accounts were available on systems that were not supported with an Information System User Registration/Change Request (Form 5081).[1] The lack of a Form 5081 indicated that access was not properly authorized and users had not certified their awareness of security rules.

The Security of the Integrated Collection System Needs to Be Strengthened (Reference Number 2003-20-119, dated May 2003).

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented (Reference Number 2003-20-211, dated September 2003).

Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses (Reference Number 2004-20-027, dated January 2004).

Security Controls for the Counsel Automated System Environment Management Information System Could Be Improved (Reference Number 2005-20-036, dated February 2005).

Security Controls for the Appeals Centralized Database System Could Be Improved (Reference Number 2005-20-069, dated March 2005).

[1] The Internal Revenue Service established the Form 5081 to request and authorize employees' system user accounts.

Appendix V

Description of Internal Revenue Service Automated Systems Selected for Review

The following Internal Revenue Service (IRS) systems were judgmentally selected based on concurrent audit work on specific applications, sensitivity of data, applicability to IRS employees, and the availability of certain data fields (e.g., date last accessed).

Appeals Centralized Database System – An Appeals organization system used for case receipt, control, and processing, as well as to record case activities and time charges.

Automated Collection System – A telephone contact system through which telephone assistors collect unpaid taxes and secure tax returns from delinquent taxpayers who have not complied with previous notices.

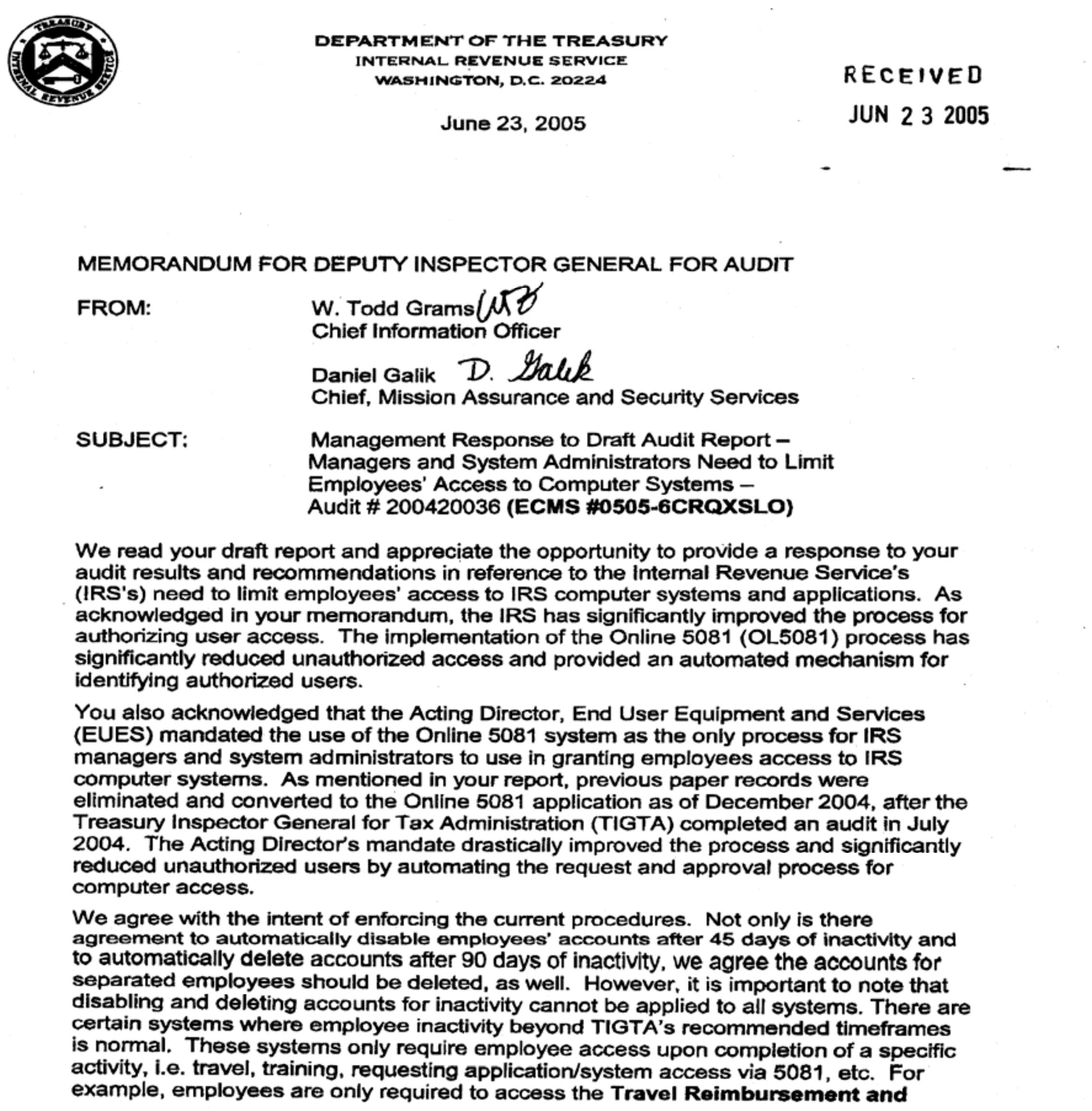
Automated Underreporter System – An automated system that matches taxpayer income and deduction information submitted by third parties to amounts reported on individual income tax returns.

Integrated Case Processing – An integrated system that provides employees with information to respond to a taxpayer inquiry and resolve most kinds of issues.

Taxpayer Advocate Management Information System – A Taxpayer Advocate Service (TAS) organization system used to record and manage all case activity involving the handling and resolution of significant hardship cases and other taxpayer problems that fall within the TAS organization's jurisdiction.

Appendix VI

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

June 23, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams
Chief Information Officer

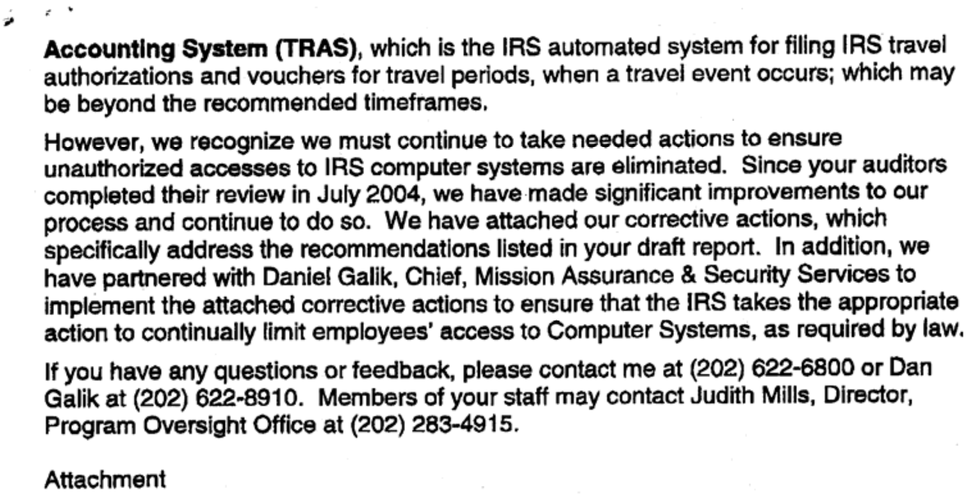
Daniel Galik D. Galik
Chief, Mission Assurance and Security Services

SUBJECT: Management Response to Draft Audit Report – Managers and System Administrators Need to Limit Employees' Access to Computer Systems – Audit # 200420036 **(ECMS #0505-6CRQXSLO)**

We read your draft report and appreciate the opportunity to provide a response to your audit results and recommendations in reference to the Internal Revenue Service's (IRS's) need to limit employees' access to IRS computer systems and applications. As acknowledged in your memorandum, the IRS has significantly improved the process for authorizing user access. The implementation of the Online 5081 (OL5081) process has significantly reduced unauthorized access and provided an automated mechanism for identifying authorized users.

You also acknowledged that the Acting Director, End User Equipment and Services (EUES) mandated the use of the Online 5081 system as the only process for IRS managers and system administrators to use in granting employees access to IRS computer systems. As mentioned in your report, previous paper records were eliminated and converted to the Online 5081 application as of December 2004, after the Treasury Inspector General for Tax Administration (TIGTA) completed an audit in July 2004. The Acting Director's mandate drastically improved the process and significantly reduced unauthorized users by automating the request and approval process for computer access.

We agree with the intent of enforcing the current procedures. Not only is there agreement to automatically disable employees' accounts after 45 days of inactivity and to automatically delete accounts after 90 days of inactivity, we agree the accounts for separated employees should be deleted, as well. However, it is important to note that disabling and deleting accounts for inactivity cannot be applied to all systems. There are certain systems where employee inactivity beyond TIGTA's recommended timeframes is normal. These systems only require employee access upon completion of a specific activity, i.e. travel, training, requesting application/system access via 5081, etc. For example, employees are only required to access the **Travel Reimbursement and**

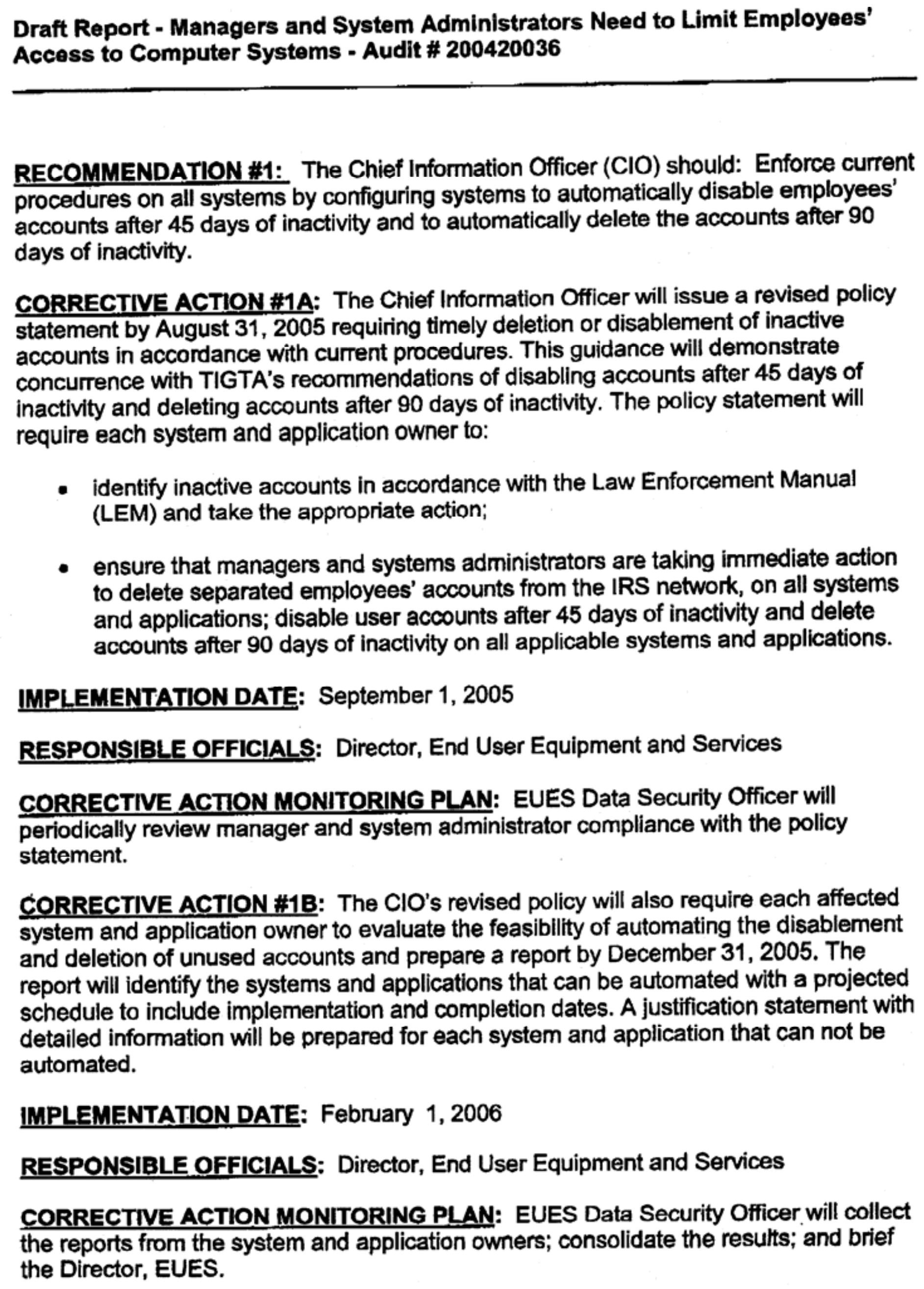


Accounting System (TRAS), which is the IRS automated system for filing IRS travel authorizations and vouchers for travel periods, when a travel event occurs; which may be beyond the recommended timeframes.

However, we recognize we must continue to take needed actions to ensure unauthorized accesses to IRS computer systems are eliminated. Since your auditors completed their review in July 2004, we have made significant improvements to our process and continue to do so. We have attached our corrective actions, which specifically address the recommendations listed in your draft report. In addition, we have partnered with Daniel Galik, Chief, Mission Assurance & Security Services to implement the attached corrective actions to ensure that the IRS takes the appropriate action to continually limit employees' access to Computer Systems, as required by law.

If you have any questions or feedback, please contact me at (202) 622-6800 or Dan Galik at (202) 622-8910. Members of your staff may contact Judith Mills, Director, Program Oversight Office at (202) 283-4915.

Attachment



Draft Report - Managers and System Administrators Need to Limit Employees' Access to Computer Systems - Audit # 200420036

RECOMMENDATION #1: The Chief Information Officer (CIO) should: Enforce current procedures on all systems by configuring systems to automatically disable employees' accounts after 45 days of inactivity and to automatically delete the accounts after 90 days of inactivity.

CORRECTIVE ACTION #1A: The Chief Information Officer will issue a revised policy statement by August 31, 2005 requiring timely deletion or disablement of inactive accounts in accordance with current procedures. This guidance will demonstrate concurrence with TIGTA's recommendations of disabling accounts after 45 days of inactivity and deleting accounts after 90 days of inactivity. The policy statement will require each system and application owner to:

- identify inactive accounts in accordance with the Law Enforcement Manual (LEM) and take the appropriate action;
- ensure that managers and systems administrators are taking immediate action to delete separated employees' accounts from the IRS network, on all systems and applications; disable user accounts after 45 days of inactivity and delete accounts after 90 days of inactivity on all applicable systems and applications.

IMPLEMENTATION DATE: September 1, 2005

RESPONSIBLE OFFICIALS: Director, End User Equipment and Services

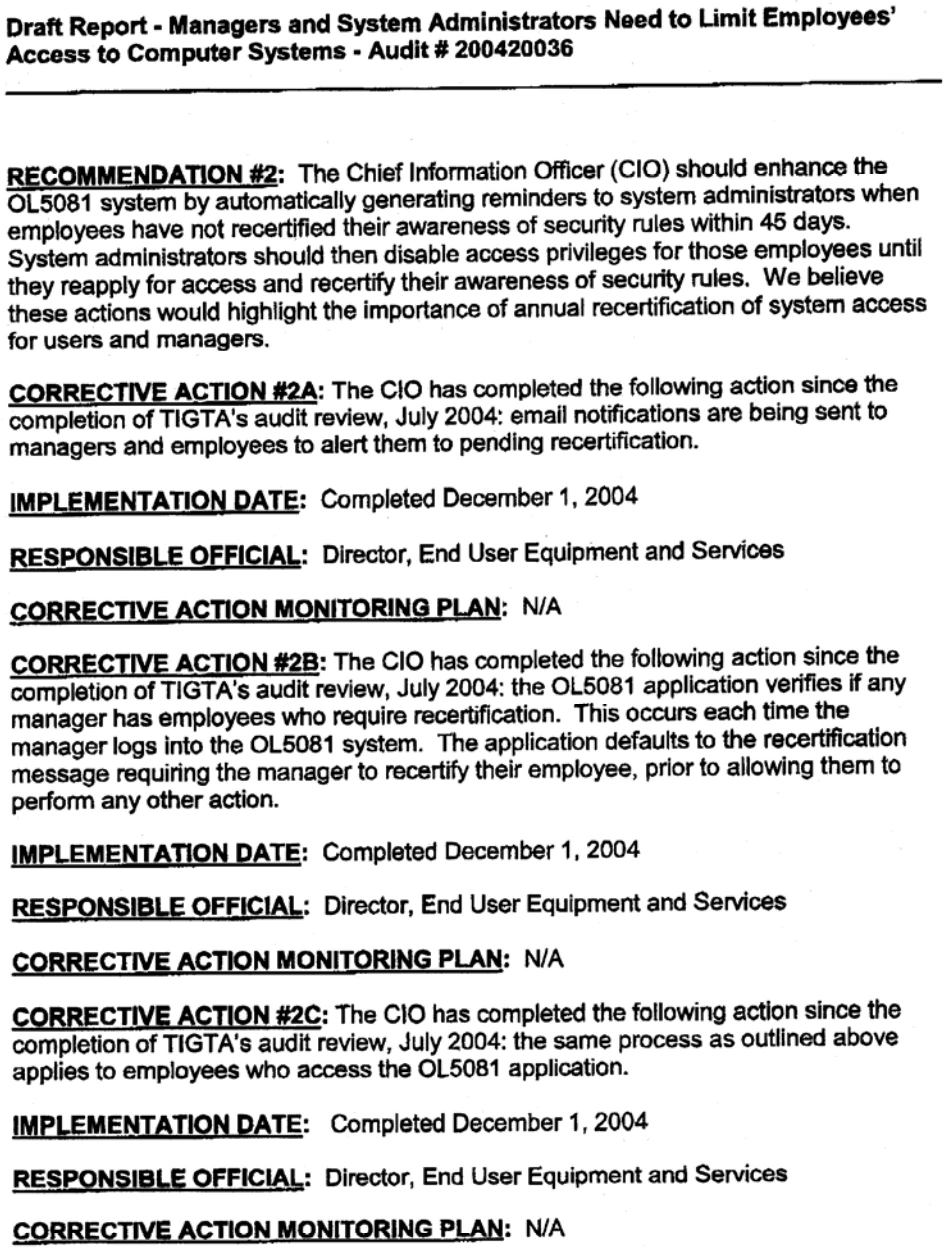
CORRECTIVE ACTION MONITORING PLAN: EUES Data Security Officer will periodically review manager and system administrator compliance with the policy statement.

CORRECTIVE ACTION #1B: The CIO's revised policy will also require each affected system and application owner to evaluate the feasibility of automating the disablement and deletion of unused accounts and prepare a report by December 31, 2005. The report will identify the systems and applications that can be automated with a projected schedule to include implementation and completion dates. A justification statement with detailed information will be prepared for each system and application that can not be automated.

IMPLEMENTATION DATE: February 1, 2006

RESPONSIBLE OFFICIALS: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: EUES Data Security Officer will collect the reports from the system and application owners; consolidate the results; and brief the Director, EUES.



Draft Report - Managers and System Administrators Need to Limit Employees' Access to Computer Systems - Audit # 200420036

RECOMMENDATION #2: The Chief Information Officer (CIO) should enhance the OL5081 system by automatically generating reminders to system administrators when employees have not recertified their awareness of security rules within 45 days. System administrators should then disable access privileges for those employees until they reapply for access and recertify their awareness of security rules. We believe these actions would highlight the importance of annual recertification of system access for users and managers.

CORRECTIVE ACTION #2A: The CIO has completed the following action since the completion of TIGTA's audit review, July 2004: email notifications are being sent to managers and employees to alert them to pending recertification.

IMPLEMENTATION DATE: Completed December 1, 2004

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION #2B: The CIO has completed the following action since the completion of TIGTA's audit review, July 2004: the OL5081 application verifies if any manager has employees who require recertification. This occurs each time the manager logs into the OL5081 system. The application defaults to the recertification message requiring the manager to recertify their employee, prior to allowing them to perform any other action.

IMPLEMENTATION DATE: Completed December 1, 2004

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

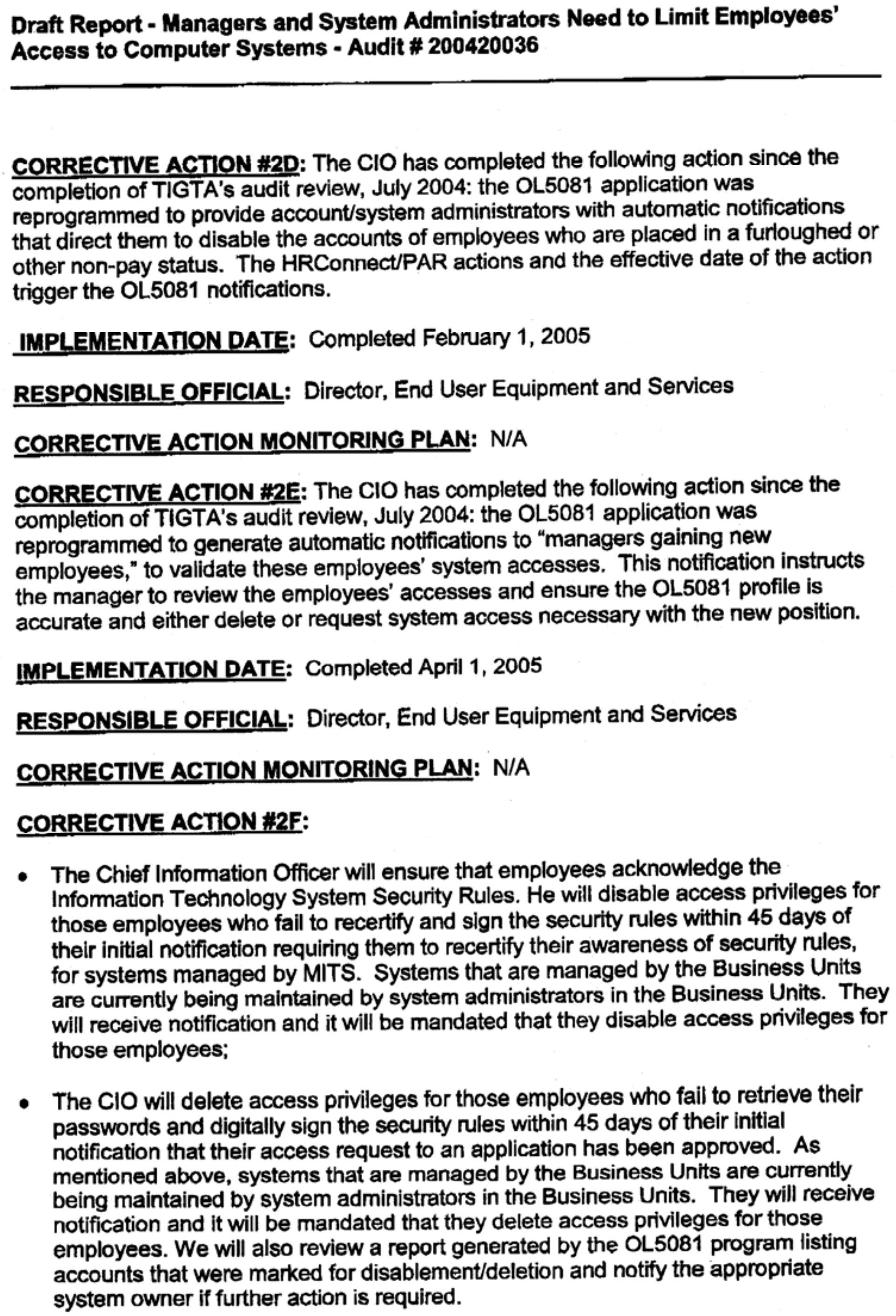
CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION #2C: The CIO has completed the following action since the completion of TIGTA's audit review, July 2004: the same process as outlined above applies to employees who access the OL5081 application.

IMPLEMENTATION DATE: Completed December 1, 2004

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: N/A



Draft Report - Managers and System Administrators Need to Limit Employees' Access to Computer Systems - Audit # 200420036

CORRECTIVE ACTION #2D: The CIO has completed the following action since the completion of TIGTA's audit review, July 2004: the OL5081 application was reprogrammed to provide account/system administrators with automatic notifications that direct them to disable the accounts of employees who are placed in a furloughed or other non-pay status. The HRConnect/PAR actions and the effective date of the action trigger the OL5081 notifications.

IMPLEMENTATION DATE: Completed February 1, 2005

RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION #2E: The CIO has completed the following action since the completion of TIGTA's audit review, July 2004: the OL5081 application was reprogrammed to generate automatic notifications to "managers gaining new employees," to validate these employees' system accesses. This notification instructs the manager to review the employees' accesses and ensure the OL5081 profile is accurate and either delete or request system access necessary with the new position.

IMPLEMENTATION DATE: Completed April 1, 2005

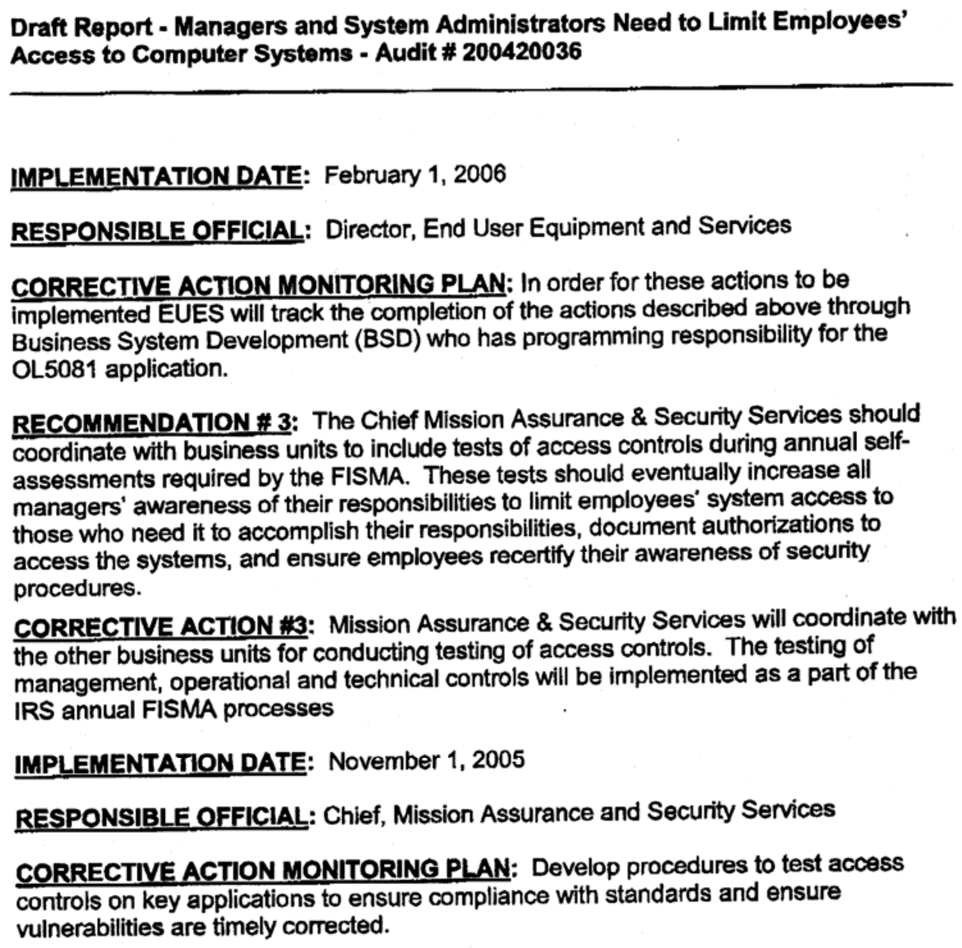
RESPONSIBLE OFFICIAL: Director, End User Equipment and Services

CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION #2F:

- The Chief Information Officer will ensure that employees acknowledge the Information Technology System Security Rules. He will disable access privileges for those employees who fail to recertify and sign the security rules within 45 days of their initial notification requiring them to recertify their awareness of security rules, for systems managed by MITS. Systems that are managed by the Business Units are currently being maintained by system administrators in the Business Units. They will receive notification and it will be mandated that they disable access privileges for those employees;

- The CIO will delete access privileges for those employees who fail to retrieve their passwords and digitally sign the security rules within 45 days of their initial notification that their access request to an application has been approved. As mentioned above, systems that are managed by the Business Units are currently being maintained by system administrators in the Business Units. They will receive notification and it will be mandated that they delete access privileges for those employees. We will also review a report generated by the OL5081 program listing accounts that were marked for disablement/deletion and notify the appropriate system owner if further action is required.



Draft Report - Managers and System Administrators Need to Limit Employees' Access to Computer Systems - Audit # 200420036

<u>IMPLEMENTATION DATE</u>: February 1, 2006

<u>RESPONSIBLE OFFICIAL</u>: Director, End User Equipment and Services

<u>CORRECTIVE ACTION MONITORING PLAN</u>: In order for these actions to be implemented EUES will track the completion of the actions described above through Business System Development (BSD) who has programming responsibility for the OL5081 application.

<u>RECOMMENDATION # 3</u>: The Chief Mission Assurance & Security Services should coordinate with business units to include tests of access controls during annual self-assessments required by the FISMA. These tests should eventually increase all managers' awareness of their responsibilities to limit employees' system access to those who need it to accomplish their responsibilities, document authorizations to access the systems, and ensure employees recertify their awareness of security procedures.

<u>CORRECTIVE ACTION #3</u>: Mission Assurance & Security Services will coordinate with the other business units for conducting testing of access controls. The testing of management, operational and technical controls will be implemented as a part of the IRS annual FISMA processes

<u>IMPLEMENTATION DATE</u>: November 1, 2005

<u>RESPONSIBLE OFFICIAL</u>: Chief, Mission Assurance and Security Services

<u>CORRECTIVE ACTION MONITORING PLAN</u>: Develop procedures to test access controls on key applications to ensure compliance with standards and ensure vulnerabilities are timely corrected.