OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Could Improve Controls Over Mainframe System Software

Report No. 2007-P-00008

January 29, 2007

Abbreviations

EPA	U.S. Environmental Protection Agency
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OTOP	Office of Technology Operations and Planning
RTP	Research Triangle Park

U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00008
January 29, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine if access to and modification of mainframe system software at the U.S. Environmental Protection Agency (EPA) National Computer Center in Research Triangle Park in Raleigh, North Carolina, is controlled in accordance with Agency and Federal guidance, as well as best practices.

Background

The EPA's Office of Inspector General contracted KPMG, LLP (KPMG) to conduct an audit of mainframe system software. Controls over system software access and modifications are designed to (1) limit and/or monitor access to system software resources to protect against unauthorized modification, loss, and disclosure; (2) reduce the risk of the introduction of unauthorized changes; and (3) limit and monitor access to powerful system software programs.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:
www.epa.gov/oig/reports/2007/20070129-2007-P-00008.pdf

EPA Could Improve Controls Over Mainframe System Software

What KPMG Found

KPMG identified several weaknesses in EPA's internal controls over its mainframe system software, including:

- Roles and responsibilities were not clearly assigned.
- Change controls were not performed in accordance with Agency policies.
- Policies, procedures, and guides could be strengthened.
- Security settings for sensitive datasets and programs were not effectively configured or implemented.

As a result of these weaknesses, EPA is exposed to greater risk since its mainframe system software could potentially be compromised.

What KPMG Recommends

KPMG recommends that the Office of Environmental Information:

- Improve management oversight and review of primary support contractor activity, and clearly assign roles and responsibilities to ensure personnel are held accountable.
- Ensure change control procedures are performed in accordance with existing Agency and Federal guidance.
- Strengthen existing policies, procedures, and guides to establish standards for implementing key security controls for mainframe system software.
- Appropriately configure and implement security settings for sensitive datasets and programs.

This report contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of the report's technical findings, the Office of Inspector General removed Appendices A and B from the public version of the report.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

January 29, 2007

MEMORANDUM

SUBJECT: EPA Could Improve Controls Over Mainframe System Software
Report No. 2007-P-00008

TO: Molly A. O'Neill
Assistant Administrator for Environmental Information and
Chief Information Officer

This is the final report on the subject audit conducted by KPMG, LLP, on behalf of the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems KPMG auditors have identified and corrective actions KPMG recommends. This audit report represents the opinion of KPMG and does not necessarily represent the final EPA position. Final determination on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The estimated cost of this report – calculated by adding the contract costs and multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $554,029.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days. You should include a corrective action plan for agreed upon actions, including milestone dates. Due to the sensitive nature of the technical findings, we have removed Appendices A and B from the report version made available to the public. The public copy of this report will available at http://www.epa.gov/oig. Additional copies of the full report can be obtained by contacting our Office of Congressional and Public Liaison at (202) 566-2391.

If you or your staff have any questions, please contact Rudolph M. Brevard, Director, Information Resources Management Assessments at (202) 566-0893 or brevard.rudy@epa.gov.

Sincerely,

Bill A. Roderick
Acting Inspector General

Final Audit Report

EPA Could Improve Controls Over Mainframe System Software

January 29, 2007

Table of Contents

Chapters

Appendices

Chapter 1
Overview

Background

The U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) engaged KPMG, LLP to conduct an audit of access to and modification of the EPA's mainframe system software housed at the Agency's National Computer Center (NCC). The NCC is located at the Research Triangle Park (RTP) campus in Raleigh, North Carolina.

The EPA's mainframe is a general support system that supports large-scale data processing and provides a national data repository for the Agency's environmental, administrative, financial, and scientific systems. Users of the mainframe include the Agency's program and regional offices, laboratories, and external business partners (e.g., states, universities, and others, such as qualified agencies and contractors, with public access requirements).

The NCC has organizational responsibility for the mainframe. The NCC is part of the EPA's Office of Environmental Information's (OEI) Office of Technology Operations and Planning (OTOP). Maintenance and security administration of the mainframe is performed by a primary support contractor.

Objectives and Scope

Controls over access to and modifications of system software are designed to (1) limit and/or monitor access to system software resources to protect against unauthorized modification, loss, and disclosure; (2) reduce the risk of the introduction of unauthorized changes; and (3) limit and monitor access to powerful system software programs.

KPMG was engaged to audit only the system software controls associated with the mainframe system. The audit was conducted to assess whether EPA implemented adequate controls over access to and modification of the mainframe system software. The scope of our audit included an evaluation of system software and logical access controls as defined by the Government Accountability Office's (GAO's) Federal Information System Control Audit Manual (FISCAM):

- *System Software Controls*. System software is a set of programs designed to operate and control the processing activities of computer equipment. Examples of system software include operating system software, system utilities, program library systems, file maintenance software, security software, data communication systems, and database management systems.

System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired.

- *Access Controls.* Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The objectives of limiting access are to ensure that:

  - users have only the access needed to perform their duties;
  - access to very sensitive resources, such as security software programs, is limited to very few individuals; and
  - employees are restricted from performing incompatible functions or functions beyond their responsibility.

Methodology

Our audit methodology was primarily derived from Section 3.4 of GAO's FISCAM. The FISCAM provides guidance that describes the computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data. We supplemented our FISCAM-based audit procedures with additional auditor-designed steps to ensure that the audit was appropriately tailored to EPA's mainframe environment. Controls were tested for compliance with National Institute of Standards and Technology (NIST) 800-series guidance, EPA-specific policies and procedures, and other Federal guidance and industry best practices. For specific criteria, refer to Appendix B.

We conducted the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States.

We conducted audit steps to determine if:

- access authorizations over mainframe system software are approved, limited to access necessary to perform assigned functions, and periodically reviewed;

- system software changes are authorized, tested, and approved prior to implementation;

- installation of system software is documented and reviewed;

- policies and procedures have been implemented to define appropriate authorized use of and to monitor use system utilities; and

- inappropriate or unusual activity is investigated and appropriate actions taken.

Audit fieldwork consisted of inspecting documentation, interviewing NCC federal and primary support contractor personnel, and conducting tests. Examples of tests we performed included assessing (1) security configurations and settings, (2) programmer access and privileges to system software and sensitive programs, and (3) recent software changes against Agency guidelines and best practices. Fieldwork was performed at the NCC from March 2006 through June 2006.

At the start of audit fieldwork, KPMG obtained documentation for review and conducted an initial site visit to the NCC to gain an understanding of how EPA manages configuration, access to, and modifications of mainframe system software. During the initial visit, the audit team also validated the mainframe environment, which had been documented in a survey completed by EPA management prior to the start of the audit. Over the course of the audit, additional site visits were conducted to interview NCC and primary support contractor personnel and to conduct audit testing.

Chapter 2
Results in Brief

We positively noted EPA management's and the primary support contractor's dedication and proactive approach to ensuring and improving the security of the mainframe system software and protecting the Agency's information assets. While our audit did not uncover any breaches in mainframe system software security, we noted that controls over access to and modification of mainframe system software can be improved. These weaknesses are discussed in the following chapters:

- Improvements Needed in the Assignment of Roles and Responsibilities (Chapter 3)

- Change Controls Need Improvements (Chapter 4)

- Policies, Procedures, and Guides Can Be Improved (Chapter 5)

In general, we recommend that EPA management:

- Improve management oversight and review of primary support contractor activities and clearly assign roles and responsibilities to ensure personnel are held accountable.

- Ensure change control procedures are performed in accordance with existing Federal and Agency guidance.

- Strengthen existing policies, procedures, guides, and supporting processes to establish standards for implementing key security controls for mainframe system software.

- Appropriately configure and implement security settings for sensitive datasets and programs.

Each of the weaknesses included in this report were initially discussed with EPA management during audit fieldwork as potential observations to validate the factual accuracy of our results. Chapters 3 through 5 of this report provide a summary discussion of each audit finding. Due to the sensitive nature of the findings related to the mainframe technical controls, we summarized the results in Appendix A and provided the details to EPA personnel. Appendix A will be removed from the final report released to the public.

Chapter 3
Improvements Needed in the Assignment of Roles and Responsibilities

EPA does not have effective oversight processes in place to help ensure that technical controls over sensitive datasets and programs are appropriately implemented. The OEI *Information Security Manual* requires Information Managers to receive written requests before creating system accounts or granting users privileges to use a system. The manual also requires Information Managers to conduct monthly reviews of system logs, support requests, and previous review findings. The *Enterprise Server (Mainframe) Security Plan* also states that monitoring of system and user activity for security violations is to be performed daily and in real time. However, we found that NCC personnel did not follow established policy. In addition, we requested but were unable to obtain evidence that NCC personnel performed periodic reviews and revalidation of the mainframe access. Further, NCC personnel had not activated system logging to create the necessary audit trails to verify system changes and users' activity.

These weaknesses exist because EPA had not assigned the roles and responsibilities for monitoring and reviewing mainframe system software security. EPA had not clearly defined the duties for monitoring and reviewing mainframe system software security. Nor had the NCC assigned the duties to specific groups, personnel, or contractors to ensure accountability. We also found that NCC personnel or primary support contractors, who are responsible for monitoring and reviewing mainframe system software, do not have clearly defined job descriptions.

As a result, EPA management does not have sufficient oversight processes in place to assure the operating environment of the mainframe. In addition, management does not have processes to determine whether controls are in place and working as intended. As noted in Appendix A, we found instances where current security configurations and settings could be exploited through backdoors to the system. Given the lack of adequate management authorization and review of programmers' access/privileges and system programmers' activities, the risk of exploitation of these weaknesses is increased.

Furthermore, without logging of system changes and access, management does not have a record to confirm that approved system activity and settings are appropriate. As such, programmers could make unauthorized changes to sensitive datasets and libraries, and management would not have a method to detect the activity. We discuss the specific mainframe technical weaknesses in Appendix A.

Following issuance of the draft audit report, EPA management took steps toward implementing corrective action to address these weaknesses. EPA updated the *Enterprise Server Standards and Procedures* document to require the monitoring of sensitive programs and utilities. EPA also updated the *Enterprise Server Standards and Procedures* document to require reviews of the system activity during weekly status meetings. EPA management also revised the *Enterprise Server (Mainframe) Security Plan* to include a process for documenting and reviewing/revalidating management approvals of system software access.

Additionally, in response to the draft audit report, EPA management provided us with examples of minutes from the weekly status meetings with the primary support contractor. EPA management felt the meeting minutes documented management's review and approval of the primary contractor activity. We noted that the meeting minutes did not sufficiently document evidence of management discussions or reviews of the primary support contractor's implementation of system software configurations, security settings, and access controls in adherence with EPA guidelines.

Management also provided us with a position description for an EPA management official with mainframe security responsibility. Our review noted that the position description defined major duties such as developing application programs and performing risk and security assessments. However, the position description did not document responsibility for monitoring and routinely reviewing mainframe system software to help ensure that the primary support contractor appropriately implements controls.

Recommendations

We recommend that the Director for the Office of Technology Operations and Planning (OTOP):

1. Enforce implementation of updated policies and procedures for (a) documenting and reviewing/revalidating management approvals of programmers' access and privileges to sensitive datasets, libraries, utilities, and programs including the continued use of the newly created Programmer Access and Privileges form and (b) logging and monitoring the use of sensitive utilities and programs. Additionally, ensure NCC personnel are conducting, at a minimum, monthly reviews of programmer's access\privileges in accordance with EPA guidance and maintaining on file the reviews and any followup actions taken to investigate any exceptions.

2. Revise the mainframe security position description to include responsibilities for monitoring and routinely reviewing mainframe system software updates to help ensure the primary support contractor appropriately implements the controls. Additionally, ensure the position description requires the EPA

personnel to document and retain copies of EPA management reviews of system software.

Agency's Response and KPMG's Evaluation

Management officials generally agreed with the recommendations. EPA management has updated and formalized its processes for documentation of approval for system software access. Additionally, management has updated *EPA's Standards and Procedures for the NCC Enterprise Server* to include a matrix on EPA and federal contractor personnel roles and responsibilities as it applies to managing the mainframe system software activities.

Following receipt of the Agency's response to the draft report, we held a meeting with NCC officials to clarify the findings and recommendations reported in this chapter. During the meeting, the auditors agreed to revise the findings and recommendations discussed in this chapter to more accurately communicate the information provided. NCC officials agreed to provide additional documentation for the audit team's consideration and review. The revisions to the findings and recommendations and our evaluation of the additional documentation provided by NCC are reflected in this report.

Chapter 4
Change Controls Need Improvements

We noted that EPA has documented policies and procedures regarding system software change controls. This guidance includes practices for normal and emergency system software changes. However, during testing of the selection of change requests, we found that EPA management is not (1) enforcing current policies and procedures and (2) providing the necessary oversight to ensure mainframe system software changes are appropriate. We found software changes are not adequately and consistently authorized, tested, approved, implemented, or reconciled. Specifically, during fieldwork we noted that:

- Thirteen percent (2 of 15) of selected change requests (CRs) were tested prior to implementation into the production environment. Additionally, one CR was incorrectly entered as an emergency change and subsequently incorrectly automatically approved.

- Documentation of the review of end-user and programmer testing results for changes is not maintained.

- Documentation of CR approval for 73 percent (11 of 15) of selected CR was maintained on file. The emergency CR was one of the four without the required documented approval.

- EPA was unable to provide evidence that Agency personnel routinely conduct steps to (1) identify and select the changes that should be implemented based on management's determination and (2) analyze the impact of planned changes on the security and processing reliability of the mainframe environment.

- A reconciliation of changes made to the mainframe production environment to approved changes does not exist.

- System programmers have access to test and production environments and are often responsible for implementing their own changes in the production mainframe environment.

These weaknesses exist because the NCC does not enforce the existing policy for authorizing, testing, and approving system software changes. Nor does management consistently document its oversight practices to help ensure all system changes are approved and implemented as intended. Based upon our review of procedures and standards and inquiry of NCC officials, we determined that policies and/or procedures requiring the routine analysis of costs and benefits

of changes and the consideration of the impact on processing reliability and security prior to implementation had not been formally or informally implemented. Additionally, an audit trail, which would assist management to reconcile approved to implemented system changes, does not exist. Furthermore, EPA management is not enforcing segregation of duties for systems programmers to prevent an individual from testing changes and consequently, implementing their own changes into the production environment.

Changes that are not adequately authorized, tested, and approved prior to implementation could result in the implementation of unauthorized and potentially inaccurate program changes. This could possibly lead to corruption of data or system downtime. As a result, the operating environment may be adversely impacted or system failures may occur. Furthermore, when a single programmer is responsible for testing a change and implementing that same change, there is the increased risk of the change control process being inadvertently or willfully subverted. This could result in unauthorized system changes being placed into production without the Agency's knowledge.

In response to the draft audit report, EPA management took steps to implement corrective actions to address the finding. Management updated the *Enterprise Server Standards and Procedures* to document a process for reconciling changes through the use of a new change activity reports and Remedy system logs of approved changes. The new procedures require management to review system changes at weekly meetings with the primary support contractor and monitor change activity reports. We determined that the new process, once implemented, will be a key component in helping EPA management identify any unapproved changes introduced in the mainframe environment. However, the process will not validate that all approved changes have been properly implemented and documented in accordance with existing change control procedures. The reconciliation process should include a comparison of a report of the changes approved by management with a system generated change activity report that includes an official record of the changes implemented into production. The reports should include dates of management approval and implementation to provide the ability to validate that approvals and implementation are occurring in a timely manner.

Upon inspection of a sample change activity report provided by NCC management, we noted that activity details, such as the type of action performed on the datasets (i.e., update, alter, etc.), associated with the logged user action is not included in the report. We also noted the updated *Enterprise Server Standards and Procedures* document does not identify who is responsible for conducting the new reconciliation procedures.

Recommendations

We recommend that the Director for OTOP:

3. Issue a memorandum to the National Computer Center (NCC) reinforcing management's responsibility for complying with applicable Agency policy for system change management.

4. Direct the NCC to develop and implement a management review process to help ensure personnel are following procedures for testing, approving, and implementing system software changes. Ensure the developed procedures require NCC management to document management's review of (1) system changes before implementing into production and (2) emergency changes to the mainframe to confirm all required procedures were followed.

5. Update the *Enterprise Server Standards and Procedures* to include procedures for documenting mainframe change management decisions. Ensure the procedures include identifying and documenting (1) the steps management uses to identify the changes to implement and (2) management's assessment of the impact of planned changes on the security and reliability of the mainframe processing environment.

6. Implement the newly developed reconciliation procedures and ensure that an audit trail of changes made to production datasets is maintained and compared to approved/authorized changes. Revise the new procedures to (1) assign related responsibilities to the appropriate individuals; (2) log modifications made to production datasets, to include logging user IDs and actions performed (i.e., alter, update, etc); and (3) retain evidence of the mandated daily reviews, reconciliations, and followup actions.

7. Conduct and document a review of the business need for systems programmers to test and implement their own changes into the production environment. If EPA management makes the determination that these duties cannot be segregated amongst different individuals, then implement compensating controls to prevent one individual from having complete control of the change process and update the *Enterprise Server Standards and Procedures* and the *Enterprise Server Security Plan*, accordingly.

Agency's Response and KPMG's Evaluation

Management generally disagreed with these recommendations. Management believes the EPA's operational approvals are recorded within the Remedy Change Control System. Additionally, all changes are discussed and documented during the weekly Enterprise Server (Mainframe) manger's meeting with the primary support contractors. A review of proposed system software changes and post review of changes are performed, reconciled, and maintained on file with the primary support contractor.

Management has implemented mitigating controls to prevent system programmer from testing and implementing their own changes into the production environment. System administrators need concurrence from back-up system administrators prior to product implementation.

Following receipt of the Agency's response to the draft report, we held a meeting with NCC officials to clarify the findings and recommendations reported in this chapter. During the meeting the auditors agreed to revise the findings and recommendations discussed in this chapter to more accurately communicate the information provided. NCC officials agreed to provide additional documentation for the audit team's consideration and review. The revisions to the findings and recommendations and our evaluation of the additional documentation provided by NCC are reflected in this report.

Chapter 5
Policies, Procedures, and Manuals Can Be Improved

NCC management needs to improve its structure for defining the NCC's overall security program. EPA's Information Security Manual requires organizational heads to establish an information security program that implements Agency-level information security policies and procedures. Although EPA management has listed datasets in the updated *Enterprise Server Standards and Procedures* document, EPA has not documented (1) specifications that EPA management uses for determining which system datasets are considered sensitive and (2) procedures for using system utilities to monitor and review the use of sensitive programs on the mainframe. In particular, we noted that:

- During audit fieldwork, EPA has not documented sensitive system datasets in existing policies or procedures. Following issuance of the draft audit report, NCC management resolved this finding by updating the *Enterprise Server Standards and Procedures* document to include the list of sensitive datasets.

- The *Office of Environmental Information (OEI) Information Security Manual* and the *EPA Information Security Manual*, which include policies and procedures for limiting access to system software, have not been updated for at least 4 years. OEI management is currently updating these guidance documents and the revisions have not been finalized and officially approved.

Promulgated and up-to-date policies, procedures, and standards serve as management's communication of the organization's standards that must be met. Without clearly defined requirements, management does not have an effective basis to evaluate performance outcomes against expectations. As such, there is an increased likelihood of:

- unauthorized or inappropriate use of sensitive programs going undetected, or

- inadequate monitoring of system resources necessary to assure the integrity of data processed by the mainframe.

Recommendations

We recommend that the Director of OTOP:

8. Update the Enterprise Server Standards and Procedures document to include (1) specifications that EPA management uses for determining which system datasets are considered sensitive and (2) procedures for using system utilities to monitor and review the use of sensitive programs on the mainframe.

9. Complete efforts to update the *Office of Environmental Information (OEI) Information Security Manual* and the *EPA Information Security Manual*. Subsequent to finalizing the changes, ensure the manuals are (1) reviewed timely by EPA management for adequacy, accuracy, and completeness; and (2) approved by EPA management in a timely manner.

10. Establish a Plan of Action and Milestone (POA&M) for all weaknesses identified in Chapters 3, 4, 5 and Appendix A**.**

Agency's Response and KPMG's Evaluation

Management concurred with these recommendations.

Following receipt of the Agency's response to the draft report, we held a meeting with NCC officials to clarify the findings and recommendations reported in this chapter. Although management concurred with our recommendations, the auditors agreed to revise the findings presented in this chapter to more accurately communicate the information provided. NCC officials agreed to provide additional documentation for the audit team's consideration and review. The revisions to the findings and our evaluation of the additional documentation provided by NCC are reflected in this report.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	6	Enforce implementation of updated policies and procedures for (a) documenting and reviewing/revalidating management approvals of programmers' access and privileges to sensitive datasets, libraries, utilities, and programs including the continued use of the newly created Programmer Access and Privileges form and (b) logging and monitoring the use of sensitive utilities and programs. Additionally, ensure NCC personnel are conducting, at a minimum, monthly reviews of programmer's access\privileges in accordance with EPA guidance and maintaining on file the reviews and any followup actions taken to investigate any exceptions.	U	Director, Office of Technology Operations and Planning		0	
2	6	Revise the mainframe security position description to include responsibilities for monitoring and routinely reviewing mainframe system software updates to help ensure the primary support contractor appropriately implements the controls. Additionally, ensure the position description requires the EPA personnel to document and retain copies of EPA management reviews of system software.	U	Director, Office of Technology Operations and Planning		0	
3	10	Issue a memorandum to the National Computer Center (NCC) reinforcing management's responsibility for complying with applicable Agency policy for system change management.	U	Director, Office of Technology Operations and Planning		0	
4	10	Direct the NCC to develop and implement a management review process to help ensure personnel are following procedures for testing, approving, and implementing system software changes. Ensure the developed procedures require NCC management to document management's review of (1) system changes before implementing into production and (2) emergency changes to the mainframe to confirm all required procedures were followed.	U	Director, Office of Technology Operations and Planning		0	
5	10	Update the *Enterprise Server Standards and Procedures* to include procedures for documenting mainframe change management decisions. Ensure the procedures include identifying and documenting (1) the steps management uses to identify the changes to implement and (2) management's assessment of the impact of planned changes on the security and reliability of the mainframe processing environment.	U	Director, Office of Technology Operations and Planning		0	

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
6	10	Implement the newly developed reconciliation procedures and ensure that an audit trail of changes made to production datasets is maintained and compared to approved/authorized changes. Revise the new procedures to (1) assign related responsibilities to the appropriate individuals; (2) log modifications made to production datasets, to include logging user IDs and actions performed (i.e., alter, update, etc); and (3) retain evidence of the mandated daily reviews, reconciliations, and followup actions.	U	Director, Office of Technology Operations and Planning		0	
7	10	Conduct and document a review of the business need for systems programmers to test and implement their own changes into the production environment. If EPA management makes the determination that these duties cannot be segregated amongst different individuals, then implement compensating controls to prevent one individual from having complete control of the change process and update the *Enterprise Server Standards and Procedures* and the *Enterprise Server Security Plan*, accordingly.	U	Director, Office of Technology Operations and Planning		0	
8	12	Update the Enterprise Server Standards and Procedures document to include (1) specifications that EPA management uses for determining which system datasets are considered sensitive and (2) procedures for using system utilities to monitor and review the use of sensitive programs on the mainframe.	U	Director, Office of Technology Operations and Planning		0	
9	13	Complete efforts to update the *Office of Environmental Information (OEI) Information Security Manual* and the *EPA Information Security Manual*. Subsequent to finalizing the changes, ensure the manuals are (1) reviewed timely by EPA management for adequacy, accuracy, and completeness; and (2) approved by EPA management in a timely manner.	U	Director, Office of Technology Operations and Planning		0	
10	13	Establish a Plan of Action and Milestone (POA&M) for all weaknesses identified in Chapters 3, 4, 5 and Appendix A.	U	Director, Office of Technology Operations and Planning		0	

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Details of Findings Related to Technical Controls Over Sensitive Datasets and Programs

This Appendix is for restricted distribution. This Appendix contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of these findings, the Office of Inspector General removed this Appendix from the public version of the report. For a complete copy of this report, contact the Environmental Protection Agency, Office of Inspector General, Office of Congressional and Public Liaison at (202) 566-2391.

Appendix B

Agency Response to Technical Control Findings Disclosed in Appendix A

This Appendix is for restricted distribution. This Appendix contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of these findings, the Office of Inspector General removed this Appendix from the public version of the report. For a complete copy of this report, contact the Environmental Protection Agency, Office of Inspector General, Office of Congressional and Public Liaison at (202) 566-2391.

Appendix C

Agency Response to Draft Audit Report

September 5, 2006

MEMORANDUM

SUBJECT: Office of Environmental Information Response to Draft Audit Report:
EPA Could Improve Controls Over Mainframe System Software
Assignment/Project No: 2006-000215

FROM: Linda A. Travers
Acting Assistant Administrator and Chief Information Officer

TO: Rudolph M. Brevard
Director, Information Resources Management Assessments
Office of Inspector General

Thank you for the opportunity to respond to the draft audit report conducted by KPMG, LLC on behalf of the U.S. Environmental Protection Agency, Office of the Inspector General (OIG). The Office of Environmental Information (OEI) has placed great emphasis on building and maintaining a secure mainframe environment as noted by observations made in the report regarding the proactive approach of EPA/OEI to improve mainframe system software controls, while protecting the Agency's information assets. It is also important to note that while many of the findings highlight improvements in procedural documentation, the report was clear to point out the absence of any security breaches in mainframe system software.

Attached is OEI's response to the audit recommendations and specific comments on the findings. Please contact Marian Cody, Director, Technology and Information Security Staff and Chief Information Security Officer, at 202-566-0302, if you have any questions regarding our comments. Thank you again for the opportunity to respond.

Attachments

Linda A. Travers
Acting Assistant Administrator and Chief Information Officer
Office of Environmental Information,
Environmental Protection Agency
Room 5000 AR North

Chapter 3: Improvements Needed in the Assignment of Roles and Responsibilities

OIG Recommendations (in bold):

We recommend that the Director of Office of Technology Operations and Planning (OTOP) should:

1. Develop and implement formalized processes in accordance with existing policy for documenting approvals of system software access, conducting periodic reviews/revalidation of access, and maintaining related documentation on file. Also, clearly and formally assign roles and responsibilities and hold personnel accountable for the performance of the processes.

OEI Response:

OEI accepts this recommendation. OEI has updated and formalized its processes for documentation of approvals for system software access. The processes are documented in the Enterprise Server (Mainframe) Security Plan. In addition, OEI has created a Programmer Access and Privileges Form to document management approvals.

OEI conducts weekly reviews of system software access with the Primary Support Contractor. This process is documented in the Enterprise Server (Mainframe) Security Plan.

Documentation of reviews is maintained in the National Computer Center (NCC) Records Management Center.

Roles and responsibilities are formally assigned. However, to clarify the assignment, a Roles and Responsibilities Matrix has been incorporated into the *EPA Standards and Procedures for the Enterprise Server* (Mainframe) *(Section 13.7 and Appendix G).*

2. Conduct periodic management reviews to ensure that the processes are appropriately performed and effective.

OEI Response:

OEI disagrees with this recommendation. On a weekly basis, management reviews approvals for system software access. Further, OEI has updated the Enterprise Server Security Plan to incorporate this process.

3. Identify NCC management responsible for security of the mainframe system software and implement periodic EPA management reviews of system software to ensure that primary support contractors have implemented controls in compliance with existing regulations, policies, procedures, and guidelines.

OEI Response:

OEI disagrees with this recommendation. In accordance with the NCC Enterprise Server (Mainframe) Security Plan, responsibility for maintaining the integrity of the mainframe system belongs to the EPA Enterprise Server (Mainframe) Manager. On a weekly basis, management reviews approvals for system software security controls. In addition, OEI uses a commercial auditing tool to measure compliance with existing mainframe policies procedures, and guidelines. These practices are all documented in the Enterprise Server Security Plan.

4. Perform, document, and maintain file reviews of controls for monitoring the use of sensitive system utilities.

OEI Response:

OEI disagrees with this recommendation. Auditing Procedures for the Enterprise Server (Mainframe) are documented in the Enterprise Server Security Plan. The EPA Primary Support Contractor reviews security audit logs and maintains the results of these reviews for at least three years. In addition, oversight is periodically performed by the EPA Enterprise Server (Mainframe) manager and results of these EPA reviews are maintained in the NCC Records Management Center. Listed below are the logs reviewed and their frequency:

- Quarterly
  - (Data Set profile reports (UACC accesses))
  - Bypass Label Processing (BLP)
  - Authorized Program Facility (APF) for sensitive data sets
- Monthly
  - Trivial Password reports
  - Supervisory Command (SVC) reports (systems special mainframe system security administrators and backup processes)
- Weekly
  - DSMON reports (operating system integrity procedure)

5. Implement processes to correct technical mainframe weaknesses identified in Appendix A.

Please see OEI's specific response listed below.

Chapter 4: Change Controls Need Improvements

OIG Recommendations (in bold)

We recommend that the Director of Office of Technology Operations and Planning (OTOP) should:

6. Ensure that formal procedures supporting existing Agency policies and standards related to system software changes are developed, implemented, and enforced with appropriate EPA management oversight.

OEI Response:

OEI disagrees with this recommendation. *EPA Standards & Procedures for the Enterprise Server* (Mainframe) documents procedures for system software changes.

The Remedy Change Control System is the official process for system software changes and approvals. EPA NCC's operational approval is recorded within the Remedy Change Control System.

Additionally, all changes are discussed and documented during the weekly Enterprise Server (Mainframe) manager meetings with the Primary Support Contractor. During this meeting, a review of proposed system software changes, as well as a post review of changes is performed, reconciled and documented. Documentation is on file with the Primary Support Contractor.

7. Maintain an audit trail of changes implemented into production. The audit trail should be used by management to review and reconcile implemented changes to approve system software changes and to ensure that changes are appropriately authorized.

OEI Response:

OEI disagrees with this recommendation. The Remedy Change Control System is the official process for system software changes and approvals. This system also provides for OEI's official audit trail of software changes.

EPA NCC's operational approval is recorded within the Remedy Change Control System. Additionally, a system of checks and balances is in place for change requests requiring independent approval from the NCC's operational security and hosting operations groups. The approvals are recorded in the Remedy Change Control System. These groups consist of both federal and contracting staff.

All changes are discussed and documented during the weekly Enterprise Server (Mainframe) manager's meetings with the Primary Support Contractor. During this meeting, a review of proposed systems software changes, as well as post review of changes are performed and documented. Documentation is on file with the Primary Support Contractor.

8. Review the business need for systems programmers to test and implement their own changes into the production environment. If EPA management makes the determination that these duties cannot be segregated amongst different individuals, compensating controls should be put in place to prevent complete control of the change process by one individual.

OEI Response:

OEI accepts this recommendation. The Primary Support Contractor's IBM Systems group convenes weekly to discuss all changes, including test results before changes are implemented in the production environment. Additionally, as described above, EPA performs oversight of this process through the weekly Enterpriser Server (Mainframe) manager's meeting.

Formal documentation of testing results by the system administrator responsible for installation of a specified product is required and must include concurrence from the back-up system administrator prior to production implementation. *EPA Standards and Procedures for the Enterprise Server (Section 4.2).*

Where total separation of duties is not practical due to limited staffing, mitigating controls have been put into place. In accordance with formal processes, system administrators are responsible for testing of the specific product prior to implementation and concurrence from the back up system administrator is required prior to production implementation. EPA performs oversight of the process through the weekly meeting.

Chapter 5: Policies, Procedures, and Manuals Can Be Improved

OIG Recommendations (in bold):

We recommend that the Director of Office of Technology Operations and Planning (OTOP) should:

9. Develop and implement formal procedures and guidelines for ensuring that appropriate access control software configuration settings for the EPA's mainframe environment are implemented. As noted in chapter 3, accountability of associated roles and responsibilities should be clearly defined and assigned.

OEI Response:

OEI disagrees with this recommendation. OEI has formal procedures requiring reviews of resource access violations and system logs for other potential security violations. To strengthen this practice, OEI will update its procedures to reflect an additional compensating control by which the Primary Support Contractor audits the IBM Systems group's use of sensitive programs. Anomalies and suspected computer security incidents are reported to the Agency's CSIRC.

10. Identify and document sensitive datasets in existing policies and standards.

OEI Response:

OEI disagrees with this recommendation. The list of datasets is maintained in the EPA Standards and Procedures for the Enterprise Server. Industry standards for the mainframe industry do not recommend specifically identifying datasets as "sensitive" in system documentation for security reasons.

11. Develop and implement clearly defined formal procedures for monitoring and reviewing the use of sensitive programs on the mainframe. Ensure that accountability of roles and responsibilities are clearly defined and assigned.

OEI Response:

OEI accepts this recommendation.

12. Complete the ongoing efforts to update outdated security manuals. The manuals should be reviewed by EPA management for adequacy, accuracy, completeness and approved by EPA management in a timely manner.

OEI Response:

OEI accepts this recommendation. OEI acknowledges the need to update the EPA & OEI Information Security Manuals.

13. Establish a Plan of Action and Milestone (POA&M) for all weaknesses identified in this report.

OEI Response:

OEI accepts this recommendation.

Appendix D

Audit Criteria

The following details the laws, requirements, and/or guidelines used as criteria in guiding our audit of information system controls over access to and modification of mainframe system software at the National Computer Center in Research Triangle Park.

Improvements Needed in the Assignment of Roles and Responsibilities

- The *OEI Information Security Manual,* Sections 7.3, states:

  "Information Managers must receive a signed written request from a designated manager prior to creating an account or assigning privileges.

  - The written request must provide the user's name and explicitly detail the access privileges requested. *Creation of User accounts or assignment of access privileges without the approved written request is forbidden.*

  - If a request is received via e-mail, the request will be verbally confirmed with the requester prior to granting access privileges, and the e-mail annotated with the date and time of the verbal verification."

  Additionally, Section 7.5 of the manual states:

  "Information Managers will conduct a monthly review of logs, support requests, inventories, authorized user lists, previous review findings, and/or technical problems and corrections for their information system(s) to help identify any current, recurring, or potential problems. Information Managers will attempt to resolve any discrepancies and, where necessary, present review findings to the appropriate management."

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security – The NIST Handbook*, states:

  "From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth."

  "The responsibilities and accountability of owners, providers, and users of computer systems and other parties concerned with the security of computer systems should be explicit."

"In effect, checks and balances need to be designed into both the process as well as the specific, individual positions of personnel who will implement the process. Ensuring that such duties are well defined is the responsibility of management."

"Software is the heart of an organization's computer operations, whatever the size, and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption. Organizations should give care to the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls."

Change Controls Need Improvement

- OTOP Directive 210.08, *National Computer Center (NCC) Compatible Enterprise Server Mainframe Security,* Section 6.4 – Installation and Maintenance guides that all operating system software installs, modifications, and maintenance will be conducted in a controlled, accountable, and auditable manner.

- The EPA *Enterprise Server Security Plan,* states that:

  The NCC computer systems are subject to formal change management and problem management methodologies as follows:

  - All operating system and application development software is placed in a test environment before installation in the production environment.

  - All applications running in the central database environment are placed in a test environment before installation in the production environment.

  - The test environments are isolated from the production environment in a manner that prevents failures in the test environment from causing failures in the production environment.

  - All software and hardware upgrades must be approved by the NTSD technical manager on the Change Management System before being applied to the production environment."

- *EPA's Standards and Procedures for the NCC Enterprise Server* establishes numerous standards and responsibilities related to system software changes, including the following:

  - Whenever any product is changed, the product and anything else that might be affected by that change must be tested, to include security.

  - Review is conducted to delete any remaining test data sets after a production installation.

  - NCC Systems Manager responsibilities include identifying the need for a product or component upgrade and informing EPA of the need to install an upgrade.

- Systems programmer responsibilities included monitoring software installations and upgrades to determine impact of the change on the system and customer community and reviewing vendor information sources for any known problems or customer impact.

- Appendix III to Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources,* states guides that separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Policies, Procedures, and Manuals Can Be Improved

- The EPA *Information Security Manual*, Section 12 states:

  "This Information Security Manual is issued through the central program and presents information security policy and procedure derived from the EPA *IRM Policy Manual*, Chapter 8, *Information Security*. Each organization must establish an organizational information security program that implements these Agency-level information security policy and procedures."

  "The procedural and technical methods used to achieve these goals will differ from organization to organization because security controls must be based on the types of information and information system platforms, threats, vulnerabilities, and level of risk for a given organization. To be effective, all security controls must support the Program's policies and goals."

- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, states:

  "Software is the heart of an organization's computer operations, whatever the size, and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption. Organizations should give care to the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls."

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* states:

  "A review of the security controls in each system and application should be performed when significant modifications are made to the system, but at least every three years."

Technical Controls Over Sensitive Datasets and Programs

- OTOP Directive 210.08, *National Computer Center (NCC) Compatible Enterprise Server Mainframe Security,* Section 6.3 – Data Security and Integrity, states:

- "Job Control Language (JCL), programs, and CLISTs for production control applications, and job schedulers for their execution, will be protected through mainframe system security at a level sufficient to prevent their unauthorized access or destruction, as well as prevent unauthorized changes to their mainframe system security profiles.

- Personnel responsible for maintaining automated job schedulers will develop procedures to prevent exploitation of identified and inherent security exposures."

Additionally, Section 6.4 of the Directive states:

- "All operating system software will be protected from unauthorized access through mainframe system security data set profiles. All access attempts will be audited through mainframe system security.

- Operating system privileges will be restricted to the minimum required by designated individuals or processes for the purpose of the specific system operation to be performed and will be approved by the OTOP ADP Security Officer.

- NCC Primary Support Contract Enterprise Server Support will develop and maintain procedures for requesting, granting, and rescinding privileges granted through operating system software. The procedures will provide for the maintenance of a list of privileges and personnel granted those privileges."

➢ The *EPA Information Security Manual, Sections 3.2, 10.3, 11.2.7, and 12,* state that:

Everyone who uses or manages EPA's information must be held accountable for his/her actions while using the Agency's information systems. EPA holds information system users accountable for unauthorized activities. Unauthorized activities may result in intentional or unintentional damage, inappropriate disclosure, or denial of access to information resources, often referred to as denial of service. Information system owners and managers must ensure that there is a positive means of identifying each user. General support systems and major applications must have audit trails that maintain a record of each user's activities while accessing the system or application. Audit trails must be reviewed regularly to ensure that users are held accountable for their actions.

To the extent possible, the following functions within the Agency should be assigned to different individuals:

- Data Creation and Control Functions
  - Data collection and preparation
  - Data entry
  - Data base administration

- Software Development and Maintenance Functions
  - Applications programming
  - Design review

- Application testing and evaluation
- Application maintenance"

Major applications containing moderately and highly sensitive information and all general support systems must generate audit trails of accesses and changes to the system and to information and applications at the individual user level.

- The *Enterprise Server Security Plan,* Section 3.6, states:

  "Data and software integrity are maintained through the following procedures:

  - Limits on user privileges ensure that only data belonging to the user is accessed or modified.
  - Use and review of system audit trails.
  - Restricting access to workstations used by Systems Programming personnel."

- Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* states:

  "Agencies must "obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST."

- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, states:

  "The MOU/A [Memorandum of Understanding/Agreement] documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU/A defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement, including apportionment of costs and the timeline for terminating or reauthorizing the interconnection."

- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, states:

  "The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements."

Appendix E

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Director, Office of Technology Operations and Planning
Director, Technology and Information Security Staff
Director, National Computer Center
Chief, Security and Business Management Branch
National Computer Center Security Officer
Audit Followup Coordinator, Office of Environmental Information
Audit Followup Coordinator, Technology and Information Security Staff
Agency Followup Official (the CFO)
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Acting Inspector General