OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Could Improve Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus

Report No. 2006-P-00005

December 14, 2005

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00005
December 14, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency's (EPA) current physical access and service continuity/contingency controls for selective applications at the Research Triangle Park (RTP) campus adhere to Federal and EPA guidelines.

Background

The Office of Inspector General (OIG) contracted with KPMG, LLP, to audit physical access controls and service continuity/contingency planning controls for select financial and mixed-financial systems hosted at EPA's RTP campus. Physical access controls protect EPA's resources from unauthorized access, theft, or destruction. Service continuity/ contingency controls ensure that EPA can continue operations of critical financial and mixed-financial applications should an outage occur.

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/2006/20051214-2006-P-00005.pdf

EPA Could Improve Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus

What KPMG Found

Physical Access. Controls needed to be improved in areas such as visitor access to facilities, use of contractor access badges, and general physical access to the National Computer Center (NCC), computer rooms outside the NCC, and media storage rooms.

Service Continuity/Contingency. Controls needed to be improved in areas such as completing a Business Impact Analysis, application contingency plans, authorizing to move backup data between key facilities, and environmental controls.

In many cases, EPA has in place compensating controls that help reduce the risk of the above issues. However, KPMG believes that controls can be improved to further reduce the risks.

What KPMG Recommends

KPMG recommends that EPA

- Improve controls, processes, and procedures related to physical access to the RTP campus and associated facilities.
- Improve controls, processes, and procedures related to moving tape backups between key facilities.
- Provide additional training regarding physical access and service continuity planning.
- Revisit the service continuity strategies for key applications to ensure that all necessary recovery strategies and efforts are ranked in terms of priority, then developed, documented, implemented, and tested.
- Improve environmental controls at key RTP facilities.

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

OFFICE OF
INSPECTOR GENERAL

December 14, 2005

MEMORANDUM

SUBJECT: EPA Could Improve Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus
Report No. 2006-P-00005

FROM: Rudolph M. Brevard /s/
Director, Information Technology Audits

TO: Kimberly T. Nelson
Assistant Administrator for Environmental Information
and Chief Information Officer

Luis A. Luna
Assistant Administrator for Administration and
Resources Management

Lyons Gray
Chief Financial Officer

George M. Gray, Ph.D.
Assistant Administrator for Research
and Development

Thomas P. Dunne
Acting Assistant Administrator for Solid Waste
and Emergency Response

This is the final report on physical access and service contingency/continuity controls audit conducted by KPMG, LLP, on behalf of the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe areas of improvements that KPMG consultants have identified and corrective actions that KPMG recommends.

This audit report represents the opinion of KPMG and the findings in this audit report do not necessarily represent the final EPA position. EPA managers, in accordance with established EPA audit resolution procedures, will make final determinations on matters in this audit report.

The OIG reviewed KPMG's report and related documentation and inquired of their representatives and found no instances where KPMG did not comply, in all material respects, with Generally Accepted Government Auditing Standards.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days of the date of this report. You should include a corrective action plan for agreed upon actions, including milestone dates. We have no objection to further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff has any questions regarding this report, please contact me at (202) 566-0893, or Charles Dade, Assignment Manager, at (202) 566-2575.

Final Audit Report

EPA Could Improve Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus

Report No. 2006-P-00005

December 14, 2005

Key Abbreviations Used in this Report

BIA	Business Impact Analysis
CIO	Chief Information Officer
DRS	Disaster Recovery Services
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
FISCAM	Federal Information Systems Control Audit Manual
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OARM	Office of Administration and Resources and Management
OCFO	Office of the Chief Financial Officer
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
RTP	Research Triangle Park
SP	Special Publication

Table of Contents

Chapters

Appendices

EPA's Response to the Draft Report

Chapter 1
Overview

Background

In support of the Environmental Protection Agency (EPA) Office of Inspector General (OIG), KPMG audited physical access controls and service contingency/continuity planning controls for select financial and mixed-financial applications hosted at EPA's Research Triangle Park (RTP) Campus. The RTP Campus is located in the greater Raleigh/Durham, North Carolina area and is a major EPA center for air pollution research and regulation. RTP supports EPA's mission by working towards a cleaner environment by concentrating on three major functions: administration and management, regulations, and research and development.

The main RTP campus facility consists of seven buildings: A, B, C, D, E, H, and the National Computing Center (NCC) and two associated off-campus facilities: the local alternate processing site and the local storage facility. NCC opened in January 2002 and provides large-scale computing services for EPA nationwide, including support for regulatory program offices and administrative activities, as well as advanced super-computing for scientific research in air quality protection and other environmental studies. While the major computing activities occur at the NCC, other buildings have smaller computer and communication rooms that host financial and mixed financial applications that connect to the campus' network.

Objectives and Scope

The objectives of our review were focused on three primary areas:

- Gather the inventory of financial and mixed financial applications hosted at the RTP facility to guide our review;
- Evaluate physical security controls in accordance with relevant Federal and EPA criteria and best practices; and
- Evaluate service continuity/contingency controls in accordance with relevant Federal and EPA criteria and best practices.

For the service continuity/contingency testing portion of the audit, we initially received from EPA a listing of 33 financial and mixed-financial applications residing at the RTP campus. We discussed and validated these applications with EPA RTP officials to ensure the accuracy of the listing. We then selected a judgmental sample of 12 applications for detailed review based primarily on whether the Agency indicated, within EPA's Automated Security Self-Evaluation and Remediation Tracking (ASSERT), that the applications had a contingency plan and/or the

criticality of the applications to EPA. EPA uses ASSERT to centrally track remediation of weaknesses associated with information technology systems. ASSERT serves as the Agency's official record for Plan of Actions and Milestones activities. Appendix B contains the list of applications included in the scope of our audit.

Our review did not include an evaluation of financial and mixed-financial applications that did not have service contingency/continuity plans in place. Additionally, our review did not include the assessment of logical access controls for EPA systems or applications.

Methodology

Our evaluation methodology was derived primarily from the Government Accountability Office's (GAO's) Federal Information Systems Control Audit Manual (FISCAM). FISCAM is designed to provide guidance to information technology auditors on the scope of issues that generally should be considered in any review of controls over the integrity, confidentiality, and availability of computerized data associated with Federal systems and applications. We specifically addressed the following two FISCAM control areas:

- *Access control.* These controls limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure. Examples of tests we performed under this control area included interviewing data center managers and personnel, reviewing data center access listings, observing data center physical access security controls, and observing data center environmental controls. In addition, we conducted tests over the adequacy of physical access security controls for entry onto the RTP campus and into RTP facilities.

- *Service continuity.* These controls involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur. Examples of tests we performed under this control area included interviewing application owners, reviewing application contingency plans, and reviewing data backup and recovery processes.

Additionally, we supplemented our FISCAM based approach with relevant EPA policy requirements and relevant guidance from the National Institute of Standards and Technology (NIST). Appendix A contains the complete list of applicable criteria. Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS).

Results in Brief

In summary, we noted that although EPA has many controls in place regarding physical access and service continuity/contingency planning, controls can be improved. For example:

- *Physical access.* We noted that controls needed to be improved in areas such as visitor access to facilities, use of contractor access badges, and general physical access to the National Computer Center (NCC), computer rooms outside the NCC, and media storage rooms.

- *Service continuity.* We noted that controls needed to be improved in areas such as the completion of a Business Impact Analysis (BIA), application contingency plans, authorization to move backup data between key facilities, and environmental controls.

In many cases, EPA has in place compensating controls that help reduce the risks in the above areas. However, we believe that controls can be improved to further reduce the risks. In this report, we have provided detailed recommendations for each identified issue.

In general, we recommend that EPA:

- Improve controls, processes, and procedures related to physical access to the NCC, media storage rooms, server rooms, and associated facilities;

- Improve controls, processes, and procedures related to the movement of tape backups between key facilities;

- Provide additional training regarding physical access and service continuity controls;

- Revisit the service continuity strategies for key applications to ensure that all necessary recovery strategies and efforts are documented, implemented, and tested; and

- Improve environmental controls at key RTP facilities.

Chapter 2
Physical Access

Access controls should provide reasonable assurance that information technology resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. These controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

KPMG conducted a review of physical access controls surrounding select information technology assets within the RTP campus. Specifically, we reviewed the physical security of assets within the NCC, computer rooms outside of the NCC, and media storage rooms (specific names of the local storage and processing sites are not provided for security reasons). As previously noted, our review did not assess logical security controls over EPA systems or applications. Although EPA had many physical access controls in place, we noted conditions associated in the following areas, which increased the risks to the RTP physical security environment:

- Contractor Access Badges
- NCC Data Center Door Alarms
- Evacuation Re-entry
- Computer Room Sign-in Procedures
- RTP Campus Visitor Identification

Additional details on each of these areas, as well as related recommendations, follow.

Contractor Access Badges

Per inspection, 29 of the 144 (20%) of the NCC data center access badges we reviewed were either assigned to temporary contractors or to temporary EPA staff. This issue occurred because NCC has many contractors that require access to the data center 24 hours per day in case of system emergencies. We inquired about assigning badges to specific contractor personnel and NCC officials informed us that this would be difficult to implement because of the need for contractor maintenance support during emergencies. In these situations, the specifically badged contractor may not be available and another contractor from the same company may arrive to perform the required maintenance support. In addition, similarly to the maintenance support contractors, the janitorial service contractors use generic badges to access the data center to perform routine cleaning services. Therefore, management felt that assigning the badges to specific contractors was not practical.

Subsequent to our testing, we met with management officials to discuss this issue, and management identified several compensating controls, such as the data center is staffed continuously, entrances are monitored by a video surveillance system, and NCC officials perform a limited badge reconciliation review. Management provided documentation supporting the NCC's badge reconciliation process. However, we reviewed the badge reconciliation documentation and noted that it was not detailed enough to sufficiently reconcile the badges. Specifically, we noted that the badge reconciliation only accounted for the total number of badges opposed to being used as a control to ensure that badges are issued to authorized contractors. Also, there was no documentation to support that the NCC maintained a valid contractor personnel roster listing authorized employees from the contracting company and that these contractors had appropriate background security screenings. Furthermore, management provided no evidence to support that the NCC implemented controls to ensure that contractors without current and appropriate background security screenings are escorted while inside the NCC.

Although management has some compensating controls in place, we believe management should enhance controls by enforcing individual accountability for access to the data center. By not enforcing accountability there is an increased risk that inappropriate access may be gained to a sensitive processing area. Also, should any damage result from the unauthorized access, it would be difficult and time consuming for the NCC to identify the perpetrator and possibly limit NCC's ability to recoup damages and/or take appropriate legal action.

Recommendations:

We recommend that the Director, Office of Technology Operations and Planning (OTOP) implement policies and controls to ensure that:

1) All contractors who have access to the data center have individually identifiable badges.

2) More comprehensive periodic reviews of contractor access to the data center are performed, and badge access is adjusted as necessary.

However, if the Director of OTOP determines that the current process is sufficient and accepts the risk, then OTOP should:

3) Obtain a complete access roster from the contractor companies (e.g., maintenance support and the janitorial services contractor) with the employee names and the current status of the employee background security screening.

4) Implement a procedure where only contractors with current and the appropriate background security screenings are allowed unescorted access in the NCC.

5) Implement a procedure to ensure that contractor personnel have appointments and are on their company's access roster before issuing them temporary badges to the NCC.

6) Implement a procedure where contractors without current and appropriate background security screenings are escorted while inside the NCC.

Agency's Response and KPMG's Evaluation:

Management agrees there are 29 temporary contractor badges that not assigned to specific individuals. In addition, management agrees that the NCC should conduct more frequent reviews of contractor access to the data center. However, management disagrees with some elements of this finding and believes that compensating controls are in place to mitigate some of the risk. As noted earlier, KPMG believes that although some compensating controls are in place, additional accountability over contractors could be obtained by requiring contractors to possess individually identifiable access badges. Subsequent to the completion of fieldwork, we meet with EPA officials to discuss this finding. Based on our discussions and review of additional documentation, we modified this finding where appropriate.

NCC Data Center Door Alarms

Per inspection and observation, we noted that the NCC data center doors do not emit an audible alarm if a door is open for an extended period. By not having an audible alarm on the data center doors, the data center employees would not be aware of potential security breaches until a security guard in building C contacts them. In this regard, equipment could be stolen or intentionally damaged prior to any data center personnel being alerted of the breach. We noted some compensating controls for this issue, such as: 1) the NCC data center door alarms are monitored centrally by the main guard facility in building C, 2) the doors are continuously monitored by a video surveillance system, and 3) the data center is constantly staffed. Although these compensating mitigate a portion of this risk controls, the lack of audible door alarms elevate the risk that unauthorized individuals could access sensitive NCC areas.

Recommendation:

7) We recommend that the Director of OTOP install audible alarms on all key access points to the NCC data center that would promptly alert NCC security personnel should a door be left open for a designated period of time.

Agency's Response and KPMG's Evaluation:

Management concurs with this finding.

Evacuation Re-Entry

Per inspection and observation, we noted that there is no apparent evidence of documented policies or procedures regarding reentry requirements in the event of a personnel emergency evacuation from RTP. By not having policy and procedures for re-entry, there is an increased

risk of unauthorized access by large numbers of personnel returning after an evacuation, particularly if pre-planned entry points are not designated and monitored. This control weakness increases the risk of unauthorized access to other RTP campus facilities and computer equipment, because these areas lack implemented compensating controls present at the NCC.

Recommendations:

8) We recommend that the Director of the Office of Administration and Resources Management (OARM) at RTP implement detailed policies and procedures regarding the re-entry of staff to the RTP campus and buildings after an event that would trigger an emergency evacuation.

Agency's Response and KPMG's Evaluation:

Management concurs with the recommendation. Management officials stated that procedures are currently being written requiring all employees to badge in upon reentry into the buildings after an emergency evacuation.

Computer Room Sign-in Procedures

We noted that there is no sign-in sheet for visitors to other computer rooms outside the NCC or to several media storage rooms. Access to the rooms is currently logged by the badge access card system, but the system does not log visitor access. A sign-in sheet is a key operational control because it serves as a visitor registry, providing auditable documentation containing the date of visit, the visitor's name, company, purpose of visit, local employee escorting the visitor, time of arrival, and time of departure. This documentation provides a means for management to assign accountability to the employee escorting the visitor and to each individual for actions occurring in the computer room.

Generally, this issue existed because the computer rooms outside of the NCC and media storage rooms were not originally designed as computing facilities and do not generally have visitors. Subsequent to the completion of fieldwork, we met with EPA officials to discuss this finding. Based on our discussions, management took immediate actions to correct this deficiency and implemented a sign-in sheet. We subsequently reviewed management's implementation of the control and found it to be sufficient.

RTP Campus Visitor Identification

Per inspection and observation, we noted the following issues that, if corrected, could help enhance the physical security controls at the RTP campus:

- Perimeter gate security guards did not consistently stop vehicles with a permanent (non-visitor) parking pass and check the vehicle occupants' identification. Rather, the perimeter gate security guards place assurance in the removable vehicle-parking pass.

- Perimeter gate security guards did not inspect the identification of all vehicle occupants for vehicles with a visitor parking pass. We noted on several occasions that the guards inspected the identification of the driver only and not the passenger. Additionally, our test, of the "identification verification" process, revealed that a vehicle was allowed onto the RTP campus without the occupants' identification being properly checked.

- Internal building security guards did not consistently verify RTP visitor's identification. Once a visitor has passed through the security screening station, they are allowed to approach the front desk to sign the visitor log and state their purpose, which will then be verified by the security officer. However, our walkthrough determined that the security officer did not consistently verify or check identification.

- Unmanned entry points are not properly controlled. On several occasions at different locations, we were able to gain access through unguarded side doors controlled by the badge access card and video surveillance systems by following behind EPA employees who gained authorized building access *"piggybacking."*

We noted that these issues occurred because the RTP security guards are not required to verify the identification of each vehicle occupant, and that security guards are not verifying permanent parking decals assigned to RTP employees. Also, the security guards are not consistently following procedures for verifying visitor's identification, and access to other campus buildings and the NCC is not limited to the main entrance. Therefore, employees and contractors may enter through doors with no security guard presence. Although compensating controls exist, such as a security guard presence and 24 hour monitoring of campus entry and exit points for vehicles, there is an increased risk that unauthorized individuals may gain inappropriate access to sensitive campus areas.

Recommendations:

We recommend that the Director of OARM at RTP:

9) Issue guidance to remind the security guards at RTP campus entrances to randomly inspect the identification of all occupants in vehicles entering the campus.

10) Ensure that guards randomly check that the permanently assigned parking passes correspond to the appropriate individual.

11) Conduct periodic checks to ensure that procedures are consistently followed for verifying visitor identification.

12) Provide, periodically, additional security training to other RTP program offices' employees/contractors addressing good physical security practices. The training should include lessons on challenging persons whom are attempting to enter the building without a RTP badge, not allowing individuals to piggyback through unguarded doors, other security concerns.

Agency's Response and KPMG's Evaluation:

Management concurred with these findings and indicated that they are taking steps to improve physical access security. Management also indicated that various checks have been conducted during conferences held at RTP and coordination has been done to inform personnel of a heightened security posture and asking them to not allow others to "piggyback" into the building once one person badges through a door.

Chapter 3
Service Continuity/Contingency Planning

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have: 1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and 2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises, understood by personnel with key responsibilities, and supported by management and staff throughout the organization.

KPMG conducted a review of service continuity/contingency planning controls surrounding select financial and mix-financial applications located at the RTP campus. We noted that the Chief Information Officer (CIO) issues high-level policy and guidance regarding EPA's contingency planning strategies. Program offices are responsible for implementing controls to comply with the CIO policy and guidance, such as contingency plan development and testing. The NCC provides service continuity services for many mission critical EPA applications through the Disaster Recovery Services (DRS) program, which is a fee for service arrangement through EPA's working capital fund. In addition, program offices that do not subscribe their applications to the DRS are required to implement full contingency planning strategies for their applications. Therefore, program offices should coordinate closely with NCC officials, as NCC hosts many of the financial and mixed-financial applications.

During our audit, we noted conditions associated with the following areas which increased the risks to EPA's service continuity/contingency planning strategy:

- Business Impact Analysis (BIA)
- Application Contingency Planning
- Authorization to Move Tapes to the Alternate Storage Facility
- Local Alternate Processing Site Access
- Environmental Controls

Business Impact Analysis

We noted a formal BIA for the NCC has not been conducted to address the identification and prioritization of critical data and operations for major applications. Consequently, the NCC does not have a BIA, approved by senior leadership that reflects the current information technology processing conditions. NCC is critical because it provides large-scale computing services for EPA nationwide, including financial reporting applications. Additionally, the NCC supports

EPA program offices by providing supercomputing resources for research in its environmental studies.

Although EPA established formal policies, procedures, and guidance for developing BIAs, the NCC did not complete the analysis. Without performing a BIA, there are risks that EPA may not be fully characterizing the necessary system requirements, processes, and interdependencies for its information technology contingency planning and business continuity strategies. Such risks could have a significant impact should a major outage occur.

Recommendations:

We recommend that the Director of the OTOP:

13) Reiterate the importance of completing the BIA to system owners through existing training vehicles and established policies, procedures, and guidance.

14) Conduct a BIA at the NCC that is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, and utilize the results to conduct a forum with the appropriate EPA program offices leadership to facilitate a decision-making process on the program offices' behalf on updating and/or modifying their current contingency planning and business continuity strategies.

Agency's Response and KPMG's Evaluation:

Management agreed with the finding to conduct a BIA at the NCC. However, management did not agree that additional training is necessary since the Agency has already documented the requirement to conduct BIA and conducted contingency planning training at the 2004 Security and Operations conference. However, during our testing, personnel we interviewed were not aware of the policies, procedures, and guidance. As such, we believe additional efforts are necessary to help ensure personnel are aware of the requirements and management's commitment to develop a BIA for the NCC.

Application Contingency Planning

Although, in some cases, the reviewed contingency plans contained many of the necessary elements, eleven of the twelve plans did not fully comply with relevant Federal or EPA requirements. We noted that the following areas needed improvement:

Applications Included in DRS:

We noted that for the applications included in DRS, the contingency plans did not consistently identify all elements guided by NIST SP 800-34. For example:

- The NCC DRS contingency plan for the Integrated Financial Management System (IFMS); Management and Accounting Reporting System (MARS); and the Combined Payroll Redistribution and Reporting System (CPARS), does not clearly identify the: 1) alternate processing procedures and 2) critical requirements for hardware, software, telecommunications, office facilities, and offices supplies. In addition, it was difficult to determine which steps in the plans related to the recovery of the three applications, nor had the plan been updated since PeoplePlus replaced the CPARS application. Finally, we noted that the contingency plan test results did not include definitive results regarding the recovery of the applications.

- The NCC contingency plan does not contain a section on reconstitution and returning to normal operations.

- The PeoplePlus contingency plan does not list primary and secondary contacts; although the contacts are included in the Critical Applications Disaster Recovery Plan. Furthermore, neither plan clearly specifies which of the two plans would be in operation should an outage occur.

Applications Not Included in DRS:

- We noted that the following applications, not subscribing to the NCC DRS program, contained contingency plan information in the application's security plans:

  - Integrated Grants Management System (IGMS);
  - Travel Manager +;
  - Financial Data Warehouse (FDW);
  - Working Capital Fund (WCF); and
  - Bank Card.

However, the information was vague, incomplete, and/or inconsistent regarding some contingency plan procedures. For example, the IGMS security plan contains a contingency planning section that indicates how critical IGMS is to EPA, but it does not contain detailed procedures for how the system would be recovered during an outage. In addition, the security plans for Travel Manager +, FDW, WCF, and Bank Card do not document detailed steps to recover application hardware, software, or telecommunications, and the contingency information does not identify alternative processing locations for the applications.

In addition, for the applications that had separate contingency plans, the level of detail in these plans was not consistent with Federal and EPA requirements. For example:

- The Budget Automation System (BAS) is not referenced in the Office of the Chief Financial Officer (OCFO), Office of Budget contingency plan. In addition, in reviewing the OCFO's Annual Planning and Budget Division Disaster Preparedness and Recovery Guide - Budget Automation System, version six, we noted many incomplete elements. These incomplete elements included the emergency telephone list and listings of vendors, suppliers, and other service providers. Such inconsistencies and incomplete information can present significant

challenges for EPA should a significant BAS outage occur, as some in the organization may believe that BAS has a well-documented recovery strategy, when in fact the planning efforts are inconsistent and incomplete.

- The Comprehensive Environmental Response, Compensation and Liability Information System (CERCLIS) contingency plan does not identify critical resources needed during an outage (e.g., personnel, telecommunications, and hardware and office facilities and supplies). In addition, the contingency plan's recovery test does not address the recovery of the application. We were also unable to determine whether contracts are in place for the restoration of the application.

- The Office of Research and Development Management Information System (OMIS) contingency plan call tree contained only business phone numbers for essential personnel, and did not include the information that should be relayed to the personnel. In addition, we noted that the recovery operations section of the contingency plan did not adequately document the steps necessary to restore operations, and it did not document whether the contingency plan had been tested. Subsequent to our review, OMIS took immediate action to remedy these conditions.

These various issues appear to have occurred because of inconsistency in training for relevant contingency planning officials. For example, for the applications that are not part of the DRS program, EPA officials informed us that any contingency planning efforts and agreements are the responsibility of the application owner, thereby increasing the possibility of developing and implementing contingency plans and procedures that are inconsistent with relevant Federal and EPA requirements.

These application contingency plan weaknesses are critical for EPA, because without documenting the essential operations and supporting resources, management may not be able to: 1) predict the negative effects of lost data and interrupted operations and 2) determine how long specific operations can be suspended or postponed. Additionally, without current and complete application contingency plans, management may not be able to efficiently recover from unplanned service interruptions.

Recommendations:

We recommend that the Director of OTOP:

15) Use existing training vehicles to remind all EPA application owners about the importance of: 1) developing application contingency plans/procedures in accordance with Federal and EPA requirements, 2) documenting test results, and 3) revising the contingency plans/procedures based on the test results.

16) Ensure that the NCC DRS contingency plan is updated and tested on an annual basis. The updated NCC DRS contingency plan should identify: 1) applicable recovery steps for IFMS, MARS, and PeoplePlus; 2) alternate processing procedures; 3) critical requirements; and 4) definitive test results regarding the recovery of all applications.

17) Revisit the NCC contingency plan and ensure it contains a section on reconstitution and returning to normal operations.

We recommend that the Office of the Chief Financial Officer ensure that the:

18) Director, Office of Financial Services revises the PeoplePlus contingency plan to: 1) contain primary and secondary personnel information consistent with the Critical Applications Disaster Recovery Plan, and 2) clearly describe which plan takes precedence during a recovery process.

19) Director, Office of Financial Management revises contingency plans for all of their applications not subscribing to the NCC DRS plan (e.g., Financial Data Warehouse), in accordance with relevant Federal and EPA requirements.

20) Director, Office of Budget revises the BAS contingency plan to contain an emergency contact list and listings of vendors, suppliers and service providers.

We recommend that the Director of the Office of Solid Waste and Emergency Response:

21) Revisit CERCLIS contingency plan and ensure that it: 1) identifies critical resources; 2) ensures the recovery test addresses all elements of application recovery; and 3) specifies which contracts are in place for the restoration of the application.

Agency's Response and KPMG's Evaluation:

In general, all the affected program offices agreed with our findings and recommendations. However, OEI requested that recommendations to correct the noted contingency plan weaknesses be addressed to the applicable program office. Further, OEI disagreed with the recommendation to analyze all contingency plan test results, adjust contingency plans and send a "lessons learned" report to senior management. OEI also did not agree with the recommendation to establish monitoring procedures to ensure that application contingency plans are tested at least once every year, because OEI already has such a procedure in place and uses the ASSERT system to track the status of contingency plan testing.

KPMG agrees that guidance is available to EPA program offices related to the development of contingency plans. However, given that we identified inconsistent approaches within the program offices for developing and testing contingency plans, we believe that additional management emphasis and training is necessary.

Subsequent to the completion of fieldwork, management officials, in several cases, provided additional documentation, such as updated contingency plans and details regarding EPA's contingency planning practices. KPMG inspected this information and where appropriate modified this finding.

Authorization to Move Tapes to the Alternate Storage Site

The alternate storage site serves as a temporary storage location for backup tapes being sent from NCC to the backup tape storage vendor. We inspected the logs tracking the movement of backup tapes between NCC and the alternate storage site and noted that there is no documented authorization to move the tapes, although there are comparable logs tracking the movement of backup tapes from the alternate storage site to tape store vendor.

According to RTP officials, the movement of backup tapes from the NCC to the alternate storage site is an informal process, and there are only a few people involved in the process, which limits the risk. For example, there is one primary person and one alternate person authorized to approve the moving of tapes between the NCC and the alternate storage site. Consequently, formal procedures for this process have not been developed. We recognize that the limited number of people involved in this process reduces the risk. However, there is an increased risk that accountability for the tapes may be lost if there is no documented authorization supporting the movement of tapes.

Recommendation:

22) We recommend that the Director of OTOP implement a procedure and control whereby the backup tapes being sent from NCC to the alternate storage site have documented authorization for movement.

Agency's Response and KPMG's Evaluation:

Management concurs with the recommendation and indicated OEI will document procedures to authorize movement of backup tapes from NCC to the alternate storage site.

Local Alternate Processing Site Access

The local alternate processing site is utilized as a continuity of operations facility for the NCC data center and is located on the border of the RTP campus. Additionally, the site contains research equipment and serves as a general warehouse. The NCC has one room designated as a contingency facility for emergency situations, and this room is equipped with several operational computers, telephones, and one television. However, we noted that the site lacks an active security monitoring process, such as camera surveillance or security guards. The security present at the facility consists of badge access card system, which is used to control entry.

EPA officials indicated that a previous physical security assessment categorized the facility as low risk, therefore not requiring a strong security presence. Additionally, EPA officials indicated that should an event occur that raises the threat level of the campus, additional guards and security measures would be deployed at all facilities. The emergency response process for the facility is dependant on the threat level to the campus, which is directed by the Department of Homeland Security threat level. However, by not actively controlling access to the facility, there

is an increased risk that unauthorized individuals may gain inappropriate access to a sensitive area, especially during a continuity of exercise or actual continuity of operations activities.

Recommendation

23) We recommend that the Director of the NCC coordinate with the Director of OARM at RTP to document the expected physical security controls for the local processing site in the event of an emergency and include these procedures in the National Computer Center's contingency plan.

Agency's Response KPMG's Evaluation:

OEI concurs with the recommendation, and agreed to work with OARM to assess the risks, costs and benefits to make a risk-based decision on additional controls. OARM responded by stating that a Physical Security Assessment of the RTP main campus facility was performed in 2004, which identified the facility as a "LOW Threat Level Facility." Based on this finding, OARM decided to mitigate this risk by including some of these corrections in a future lease agreement

KPMG recognizes EPA's need to implement cost effective security controls to mitigate risks. However, the acceptance of risks should be coordinated, documented, and approved by appropriate senior Agency officials. As such, we believe that OARM's rationale for accepting the risks associated with the local processing site should be formally documented and communicated to all affected Agency offices so that appropriate contingency planning activities can occur. Based on discussions with Agency officials, we modified the recommendation.

Environmental Controls

KPMG noted examples where EPA environmental controls at key RTP facilities could be improved:

- KPMG noted during the walkthrough of the NCC data center that food and drinks were allowed in the computer areas. This violates posted signs throughout the data center stating that eating and drinking are prohibited.

- KPMG noted, during the walkthrough of the computer rooms outside of the NCC, that emergency procedures were not posted in case of fire, plumbing leakage, or premature water release from the sprinklers. Additionally, during our walkthrough of another computer room, we observed a water stain from a previous leak on the ceiling tiles. We also noted that emergency water shut-off values and electric power sources were not easily identifiable.

It appears that these issues existed because: 1) EPA management officials have not fully enforced the requirement of not having food and drinks in the NCC data center, and 2) EPA did not develop and implement processes for these critical procedures for the computer rooms outside of the NCC. One computer room was not originally designed to host computer

equipment; as such, water lines run through the room thereby increasing the risk of water damage from a leak or burst pipe.

Allowing food and drink in the NCC data centers increases the risk that key processing equipment or other materials, such as recovery plans and procedures, could be damaged by a spill. In addition, if the appropriate EPA personnel are not aware of the emergency procedures and can not easily locate the emergency water shut-off values and electrical power sources, EPA personnel may not promptly respond to an emergency to protect the computer equipment in case of a burst water pipe or plumbing leakage.

Subsequent to completing fieldwork, RTP personnel provided KPMG with additional documentation regarding environmental controls over the computer rooms. Specifically, KPMG was provided with documents containing bullet-point procedures for both fire and water emergencies in the computer rooms and EPA OIG auditors observed these policies posted in the computer rooms. Additionally, RTP personnel also provided work orders to identify the shut off valves for the water and plumbing lines and for the installation of water detectors. EPA OIG auditors inspected the computer rooms and verified that environmental controls existed.

Recommendations:

24) We recommend that the Director of OTOP should make a determination whether to enforce the posted notices regarding not having food and drinks in the NCC data center and remind employees of the policy. If management decides to accept the risk of allowing food and drinks in the data center, then the acceptance of the risk should be documented in the NCC security risk assessment.

Agency's Response and KPMG's Evaluation:

Management officials agree with our findings and recommendations. OARM at RTP disagreed with implementing compensation controls such as having security guards perform visual inspections of computer rooms. As such, OARM officials provided additional documentation and details regarding its efforts to provide effective environmental controls over the computer rooms. Where appropriate, we modified this finding.

Appendix A
Criteria

The following laws, requirements, and/or guidelines were used as criteria in guiding our review of physical security and service continuity at RTP.

- The *EPA Information Security Manual* states that:

  - Physical security measures be in place to protect information systems against unauthorized access, theft, or destruction.

  - Continuity of support and/or contingency plans must be developed. Specifically, the manual requires that: 1) contingency and continuity of support plans should be reviewed and updated on an annual basis and in coordination with COOP planning efforts; 2) recovery plans should be developed for re-establishing a permanent, ongoing processing site; 3) the plans should be tested; 4) EPA should conduct training on the plan and its elements; 5) the plans should be documented; and 6) the plans should be periodically re-tested and revised.

  - Food, smoke, heat, and excess moisture can damage equipment.

- The Federal Information Security Management Act (FISMA), issued as part of the E-Government Act of 2002, requires Federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. FISMA further requires Federal agencies to follow information security guidance issued by NIST.

- The Federal Manager's Financial Integrity Act (FMFIA) requires Federal agencies to maintain accountability over assets.

- National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook* guides that contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer. This will allow an organization to assign priorities to resources since not all elements of all resources are crucial to the critical functions.

- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, guides that organizations should require users to identify themselves uniquely before being allowed to perform any actions on the system.

- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems* guides that:

- The completion of a BIA is a key step in the contingency planning process, as it helps identify and prioritize critical information technology systems and components. According to NIST, the BIA enables the organization to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's contingency planning and business continuity strategies.

- Contingency plan testing is a critical element of a viable contingency capability, and each element of the contingency plan should be tested, first individually and then as a whole, to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. Additionally, it states that this testing should occur at least annually and when significant changes occur to the IT system, supported business process(es), or the IT contingency plan.

- Common fire prevention measures include water sensors in the computer room ceiling and floor.

- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* guides that Federal agencies should:

  - Develop and keep current lists of personnel with authorized access to facilities containing information systems and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards).

  - Assign designated officials within the organization to review and approve access lists and authorization credentials per a defined time period, but at least annually.

  - Centrally monitor real-time intrusion alarms and surveillance equipment, and employ automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

  - After an emergency-related event, restrict reentry to facilities to authorized individuals only.

  - Authenticate visitors (including government contractors) prior to authorizing access to facilities or areas.

  - Maintain a visitor access log that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. NIST further guides that designated officials within the organization should review the access logs.

- Consider surveillance and security guards as key physical access controls**.**

- Office of Management and Budget (OMB) Circular Number A-123, *Management Accountability and* Control, requires that accountability for the custody and use of resources be assigned and maintained.

- OMB Circular A-130, *Management of Federal Automated Information Resources*, guides that agencies shall:

  - Implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

  - Establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users continue to perform essential functions in the event their information technology support is interrupted.

Appendix B
Applications Reviewed

	Application	Program Office	Description	Major Application	Risks
1.	**BAS** (Budget Automation System)	Office of the Chief Financial Officer (OCFO)	BAS is the central Agency system used to integrate strategic planning, annual planning, budgeting, and financial management. The system contains resource (dollars and FTE), planning and performance data. The system supports budget formulation, annual planning and operating plan development. BAS links to the IFMS to send the Agency's Initial Operating Plan in the format of IFMS Appropriation & Apportionment (AA) documents. BAS receives from IFMS the revised operating plan and actual obligations/outlays data.	Yes	High
2.	**CERCLIS** (Comprehensive Environmental Response, Compensation and Liability Information System)	Office of Superfund Remediation and Technology Innovation (OSRTI)	The Agency's system for supporting the Superfund program. CERCLIS receives downloads of IFMS Superfund financial transactions. This is not an OCFO application and no information from this system is sent to the Integrated Financial Management System (IFMS).	Yes	High
3.	**CPS** (Contracts Payment System)	Office of the Chief Financial Officer	CPS is an NCC mainframe application with ADABAS database. The application tracks and pays EPA contractors. This application is a subscriber to the NCC Disaster Recovery Program.	Yes	High
4.	**MARS** (Management and Accounting Reporting System)	Office of the Chief Financial Officer	MARS provides standard and ad hoc financial reports based on data from IFMS. The source for the MARS data is the IFMS journal. It is run out of the NCC and is an ADABAS/Mainframe application.	Yes	High

	Application	Program Office	Description	Major Application	Risks
5.	**IGMS** (Integrated Grants Management System)	Office of Administration and Resources Management (OARM)	IGMS is the Agency's system for the processing and management of all forms of assistance agreements with State and local governments, non-profit organizations, educational institutions, and individuals, as well as interagency agreements with other Federal agencies. IGMS receives commitment data from IFMS. This Lotus Notes application is owned by the Grants Department.	Yes	High
6.	**OMIS** (Office of Research and Development Management Information System)	Office of Research and Development (ORD)	OMIS is comprised of five independent modules. Only the Integrated Resource Management System (IRMS) interface with IFMS. The real-time interfaces are used to electronically transmit transactions (commitment and reprogramming) to IFMS. Extract files are created after the nightly IFMS close to bring down to IRMS the approvals/disapprovals of the reprogramming transactions as well as operating plan, commitments, obligations, and expenditures from the Suballowance Spending Control Inquiry Table (SASP) and General Ledger tables.	Yes	High
7.	**TM+** (Travel Manager +)	Office of the Chief Financial Officer	TM+ is a COTS product used to streamline and fully automate the Agency's travel process. TM+ sends Travel Order (TO) and Travel Voucher (TV) documents to IFMS. TM+ automates the travel process for EPA. It was developed by Gelco and runs on its own servers. The application will be phased out in September 2006 when E-Travel (a.k.a. GovTrip) is implemented. EPA had one of three choices in the replacement of TM+ and opted for the Northrop Grumman GovTrip web-based application.	Yes	High

	Application	Program Office	Description	Major Application	Risks
8.	**WCF** (Working Capital Fund)	Office of Environmental Information (OEI)	WCF Service Providers generate monthly entries to record depreciation, cost transfers, and application of Overhead and G&A as well as customer billing information. They transmit that data automatically via an interface file containing Asset Voucher (AV)/Month End Adjustment Voucher (MV), and Project Charge (CH) documents to IFMS. All information is placed on the IFMS SUSF table for the RTP, FMC staff to review and process online or through batch mode. Any errors found are researched and corrected prior to processing. WCF is run by the Office of Technology Operations and Planning (OTOP) group. Some servers are maintained at RTP, however OCFO does not know what is contained on them. Regular backups are performed for the application.	Yes	High
9.	**IFMS** (Integrated Financial Management System)	Office of the Chief Financial Officer	IFMS is a mainframe application hosted at the NCC. It is the EPA's core financial system and does subscribe to Disaster Recovery services at the NCC.	Yes	High
10.	**People Plus**	Office of the Chief Financial Officer and the Office of Human Resources and Organizational Services (OHROS)	EPA's new payroll processing system. People Plus is a co-owned system between the OCFO and the OHROS. The application is hosted at the NCC on a UNIX machine.	Yes	High
11.	**Bankcard**	Office of the Chief Financial Officer	Bank Card Interface System was developed to properly allocate funds in paying for items purchased with credit cards. The daily files of transactions are maintained on an Oracle Database with an upload to the financial statements. The application has a web interface to allow users the ability to see payments and obligations.	No	Medium

	Application	Program Office	Description	Major Application	Risks
12.	**Financial Data Warehouse (FDW)**	Office of Financial Management and Office of Financial Services	FDW houses periodic snapshots of IFMS data to provide reporting capability. The FDW offers standard reports from IFMS, EPAYS, CPARS and CPS. Access to FDW is controlled by FSD. The application is hosted at NCC on a Unix NIX Digital machine with Oracle 8.1 database tables.	Yes	High

Appendix C
Distribution

Office of the Administrator
Director, Office of Technology Operations and Planning
Director, Office of Administration and Resources Management at RTP
Director, Technical Information Security Staff
Director, National Computer Center
National Computer Center Security Operations Manager
Agency Follow-up Coordinator
Audit Follow-up Coordinator, Office of Administration and Resources Management
Audit Follow-up Coordinator, Office of Environmental Information
Audit Follow-up Coordinator, Office of the Chief Financial Officer
Audit Follow-up Coordinator, Office of Research and Development
Audit Follow-up Coordinator, Office of Solid Waste and Emergency Response
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Association Administrator for Public Affairs
Inspector General

Appendix D
Office of Environmental Information

Draft Report Response from the Office of Environmental Information (OEI)

October 21, 2005

MEMORANDUM

FROM: Kimberly T. Nelson /s/
Assistant Administrator and Chief Information Officer

TO: Rudolph M. Brevard
Acting Director, Business Systems Audits
Office of Inspector General

Thank you for the opportunity to respond to the draft audit report on Information System Service Contingency and Physical Access Controls. We appreciate your efforts to hold informational meetings to ensure clarity of your findings and recommendations and to give us an opportunity to recommend revisions.

As we discussed at the informational meetings on October 4, 2005, we have concerns about some of the findings and recommendations regarding the physical access and information system service contingency findings. We conveyed these concerns to your staff at the October 4 meeting and appreciate their receptivity to ensuring that the findings are accurate and that the final recommendations will effectively address real deficiencies.

Our detailed comments are attached. Please feel free to contact George Bonina, Director of the Technology and Information Security Staff and Chief Information Security Officer at 202-566-0304, if you have any questions or need additional information.

Attachment
cc: Linda Travers
Mark Day
Myra Galbreath
George Bonina
Robin Gonzalez
John Gibson

Physical Access

Contractor Access Badges

OEI agrees with the finding that 29 badges were identified as contractor temporary badges not assigned to a specific individual. The NCC developed a procedure for issuing contractor temporary badges as a result of a prior audit finding that the data center had too many people with permanent access. Consequently, NCC issues contractor temporary badges for personnel whose data center access frequency is less than three times per week.

OEI disagrees with the finding that these contractor temporary badges have no names associated with the badges. Unescorted temporary badges are only assigned if the individual's name appears on a predefined controlled access list, maintained in the data center. As each temporary badge is issued, the individual's name is entered in a visitor access control log.

OEI disagrees with the finding that the temporary badges are not kept in EPA facilities. All badges are maintained at the NCC.

OEI disagrees with the finding that there is no formal process for identifying the contractor using the badge. The formal process for issuing and documenting temporary badges is in place as described above.

OEI disagrees with the finding that contractors do not identify specific individuals to support the NCC in cases of each emergency, and that the NCC issues generic access badges to the contractor companies rather than to specific individuals. Any contractor who does not currently have a permanently issued badge or whose name does not exist on the pre-defined access control list is required to have an escort during their presence in the data center. Each of these individuals must be identified by the vendor prior to their arrival.

OEI disagrees with recommendation (1); given the existence of the current process that explicitly associates all badges and access to the NCC with individual identification.

OEI agrees with recommendation (2) to conduct more frequent reviews of contractor access to the data center.

NCC Data Center Door Alarm

OEI agrees with this recommendation.

Local Alternate Processing Site Access

OEI will work with OARM to assess the risks, costs and benefits to make a risk-based decision on additional controls.

Service Continuity/Contingency Planning

Completion of the BIA

OTOP conducted training on contingency planning at the 2004 Security and Operations Conference. Staff from OTOP's Technology and Information Security Staff (TISS) provide support to system owners on an ongoing basis.

Since there is already a well-documented EPA requirement to conduct BIAs, the recommendation to document that requirement (18) is not necessary.

The recommendation to conduct additional training on contingency planning (17) is not necessary due to the clarity of the NIST document, OEI's supplemental guidance, the prior training conducted by OTOP and the availability of TISS support to program offices.

OEI agrees with the recommendation that the NCC conduct a BIA (19).

OEI disagrees with the recommendation to conduct a forum with EPA program offices leadership to update/modify current contingency planning and business continuity processes (19). This audit contains no finding that would be addressed through this recommendation.

Application Contingency Plan Weaknesses

OEI Response

Most of the recommendations appear to be based on an incorrect conclusion that problems with individual system contingency plans are the result of a systemic problem with the Agency-wide contingency planning program. As noted above, it appears that the auditors were not aware of the Agency procedures and guidance on contingency planning. OEI believes that it is inappropriate to place the responsibility for correcting deficiencies in program office system contingency plans on the OTOP Director. Placing this responsibility on the OTOP Director is in contradiction to FISMA which places the responsibility for system security on program officials for systems under their control. Therefore, OEI believes that recommendations (24) and (26) thru (30) should be directed to the Assistant Administrator of the appropriate office.

OEI believes that the recommendation to analyze all contingency plan test results, adjust contingency plans and send a "lessons learned" report to senior management (25) is unnecessary because there is nothing in the audit findings to support a conclusion that there is a systemic problem to be addressed through this recommendation. Also, consistent with FISMA, analyzing test results and adjusting plans is the responsibility of the program officials.

For reasons noted above, OEI disagrees with the recommendation to provide consistent training to all EPA application owners (20).

It is not clear why the recommendation to establish monitoring procedures to ensure that application contingency plans are tested at least once every year or more often (21) is included since the findings identify only one plan that may not have been tested. This recommendation is also unnecessary because OEI already has such a procedure in place. OEI uses the ASSERT system to track the status of contingency plan testing. This percentage of systems with tested contingency plans is measured on the E-gov scorecard of the President's Management Agenda as

well as an OMB performance measure that is reported quarterly to OMB. For the FY 2005 Annual FISMA report to OMB, EPA reported that 97% of the Agency's major applications and general support systems had tested contingency plans. OIG auditors have access to ASSERT and can verify this information.

OEI agrees with recommendations (22) and (23).

Authorization to Move Tapes to Alternate Storage Facility

OEI Response:

OEI will document procedures to authorize movement of backup tapes from NCC to a local storage facility.

Environmental Controls

OEI Response:

OEI agrees with recommendation (32) to address the risks of food and drinks in the NCC data center.

OEI will work with OARM to assess the risks, costs and benefits to make a risk-based decision on additional controls (33).

OARM Response:

OARM will respond directly to the IG in a separate document.

Appendix E
Office of Administration and Resources Management

Draft Report Response from the Office of Administration and Resources Management at RTP (OARM)

October 25, 2005

MEMORANDUM

SUBJECT: OARM Response to Draft Audit Report: Audit of Information System Service Contingency\Continuity and Physical Access Controls of EPA's Financial and Mixed-Financial Systems that Reside at Research Triangle Park
Assignment/Project No: 2004-001383

FROM: William G. Laxton, Director /s/
Office of Administration and Resources Management, RTP (C604-02)

TO: Vincent Campbell, Auditor/Project Officer
Office of Inspector General (2421T)

The enclosed report addresses the recommendations identified in the original audit report for OARM-RTP action. Our reply addresses each recommendation for Chapters 2 and 3. The point of contact for Chapter 2, *Physical Access,* is Sam Pagan, (919) 541-5001; for Chapter 3, *Service Continuity/Contingency Planning*, the contact point is Alex Montilla (919) 541-0324.

Attachment

Chapter 1: Overview

No findings or recommendations requiring OARM lead

Chapter 2: Physical Access

With regard to: Evacuation Re-Entry:

Recommendation 8: Coordinate the implementation of detailed policies and procedures regarding the reentry of staff to the campus and buildings after an event that would trigger an emergency evacuation. *(from page 5 of draft report)*		Response: Procedures are currently being written requiring all employees to badge in upon reentry into the buildings after an emergency evacuation.
Recommendation 9: Provide additional security training to employees/contractors addressing good physical security practices; such as challenging persons whom are attempting to enter the building without an EPA badge. *(from page 5 of draft report)*		Response: Employees at RTP have been reminded of these procedures through various all hands memos informing them of a heightened security posture and asking them to not allow others to piggyback in to the building once one person badges through a door. We will continue to inform our employees of these procedures through other means of communication.

With regard to: RTP Computer Room Visitor Identification:

Recommendation 10: Coordinate with the applicable program offices to consistently enforce policies and procedures that would require all visitors entering the computer room in building C, to sign a visitor log which should be maintained and kept on file. *(from page 6 of draft report)*		Response: On 21 July 2005 OARM posted access logs in each of the four computer rooms (C160, C131, C240 and N147) to include the main distribution facility (C160A). The policy was disseminated to system administrators via email directing that all visitors escorted into server rooms and the MDF sign in and out of the rooms accordingly. Escorts are required to record their identification badge number by each of their visitor's information.
Recommendation 11: Ensure the consistent enforcement of policies and procedures that would require all visitors entering the silo room at the local storage facility to sign a visitor log which should be maintained and kept on file. *(from page 6 of draft report)*		Response: Though this recommendation is made to OARM, the silo room in question is operated by the NCC. This recommendation should be addressed by OEI-OTOP. OARM has coordinated this finding with the appropriate NCC personnel and has provided an electronic copy of its computer room access log

		accordingly. OARM security will coordinate with the Director of OTOP to establish a procedure that would require everyone entering the silo room to sign a visitor log.

With regard to: Campus Visitor Identification:

Recommendation 12: Issue guidance to remind the security guards at RTP campus entrances to inspect the identification of all vehicles and individuals entering the campus. *(from page 7 of draft report)*		Response: Security into the RTP campus is based on a two tiered system. The first tier is a preliminary check at the gates. This check makes sure that each vehicle entering the RTP campus has an authorized vehicle pass. Visitors are issued a one day vehicle pass upon presenting proper identification. A more thorough security check is conducted during our second tier check. Each visitor is checked at the entrance to each of our main buildings. Visitors must go through a magnetometer and show proper identification prior to gaining entrance to our buildings.
Recommendation 13: Ensure that guards check that the removable parking passes correspond to the appropriate vehicle/individual. *(from page 7 of draft report)*		Response: Our main security check is conducted at the entrance to each one of our buildings and not at the gates. The main reason is that the RTP campus has a very porous perimeter. The gates are the principle way to get into the campus but there are many ways to enter through the wooded areas surrounding the campus. Because of this, we conduct our personnel security checks at the entrance to our buildings. Delivery trucks are stopped by bollards and another security gate inside the main campus. This gate is also manned by a security guard. Delivery trucks are not allowed through the bollards until positive identification of the driver and the program expecting the delivery is made.
Recommendation 14: Ensure that procedures are consistently followed for verifying visitor identification. *(from page 7 of draft report)*		Response: Various checks have been conducted during conferences held at RTP to assure the correct visitor procedures are followed.
Recommendation 15: Coordinate with other RTP program office to provide additional security training to employees/contractors addressing good physical practices; such as		Response: Coordination has been done via various all hands memos informing them of a heightened security posture and asking them to not allow others to "piggyback" into the

challenging persons whom are attempting to enter the building without a RTP badge. *(from page 7 of draft report)*		building once one person badges through a door. We will continue to inform our employees of these procedures through other means of communication.

With regard to the alternate processing site:

Recommendation 16: We recommend that the Director of OTOP and Director of OARM at RTP coordinate to develop a strategic plan to deploy security controls at the alternate processing site facility in the event of an emergency. Alternatively, the Director OTOP and the Director of OARM should coordinate to accept the security risk of the facility, and document the risk in the facility security risk assessment. *(from page 8 of draft report)*		Response: The Physical Security Assessment of the Research Triangle Park's (RTP) Main Campus Facility done in 2004 identified the local processing site facility as a "LOW Threat Level Facility". Based on this finding, we decided to mitigate this risk by including some of these corrections in a future lease agreement. Additionally, we decided to "accept the risk" of not having a visitor control system in place. One of the many functions done at local processing site is the initial drop-off of all incoming mail and packages into our facilities. These items are then x-rayed at the warehouse before they are delivered to our other facilities by our contractor. Furthermore, deliveries to the local processing site are made by different companies and drivers each day. We chose to accept this risk in order to protect our main facilities from vulnerabilities from unknown deliveries.

Chapter 3: Service Continuity/Contingency Planning

With regard to: Environmental Controls:

Recommendation 33: Install the equipment to implement necessary detective and preventive controls such as the identification of shut off valves for plumbing lines and water sprinklers, installation of water detection equipment, and the development of water emergency procedures that deal with plumbing line leakage and premature water release from sprinklers. Alternatively, compensating controls and related procedures, such as periodic monitoring of the computer room by security guards, should be implemented. *(from*		Response: In FY 2004 OARM installed water detection sensors in all computer rooms (C160, C131, C240 and N147) as well as the main distribution facility (C160A). Materials have been purchased and procedures are in place to drape plastic over the computer cabinets in each server room should there be a water emergency. OARM has installed a redundant Storage Area Network that performs synchronous mirroring between appliances in Building C and the NCC. OARM has offered this service to OCFO and the other campus program offices as a means of

page 16 of draft report)		mitigating this water incident vulnerability. The OARM LAN Manager monitors the computer rooms through physical inspection of each area. He tracks UPS Load, Humidity Levels and Temperature as well as looks for leaks in ceiling tile. The O&M contractor is advised of any water present beneath the raised floors and advises the OARM LAN Manager accordingly. The OARM LAN Manager does not recommend that Security Guards (contractors) be allowed into computer rooms or the MDF unescorted. OIG (Cheryl Reid) visited computer rooms in building C to verify that water detectors are in fact installed beneath the raised floor. She has seen the detectors that have been installed and to the best of our knowledge we have satisfied that portion of the recommendation. She recommended that procedures be posted in each room outlining our response actions to a water leak incident. We have submitted and received 5 poster boards containing such procedures for each computer room. Furthermore, we have submitted the work order to identify the shut off valves for the water sprinklers and plumbing lines. The O&M contractor (CHI) is responsible for those systems and would shut off the appropriate valves in the event of any water leaks. Finally, we provided OIG (Cheryl Reid) a copy of reports substantiating our periodic monitoring (weekly) of each computer room. The report substantiates our response that the computer rooms are being actively monitored. In short, we have water detectors in each computer room, we have posted compensating procedures, as well as, perform active monitoring of the computer rooms.

Appendix F
Office of Research and Development

Draft Report Responses from the Office of Research and Development (ORD)

November 4, 2005

MEMORANDUM

SUBJECT: ORD Response to Draft OIG Report, Audit of Information System Service Contingency/Continuity and Physical Access Controls of EPA's Financial and Mixed-Financial Systems that Reside at Research Triangle Park, No. 2004-001383

FROM: George Gray ***/s/ Lek Kadeli for***
Assistant Administrator (8101R)

TO: Rudolph M. Brevard
Acting Director, Business Systems Audits (2421T)

Purpose

The purpose of this memorandum is to provide the Office of Research and Development's (ORD) comments on the subject draft OIG report.

Background/Discussion

The draft report dated September 13, 2005, noted several areas which needed improvement. ORD took a proactive approach and immediate action to remedy those areas. Specifically, the ORD Management Information System (OMIS) Contingency Plan (attached) was revised as follows: (1) Appendix A, Personnel Contact List, was updated to include all business, home, and cell phone numbers; and (2) Appendix D, Disaster Recovery Testing, was added to include the type of test, test date, and the result. The revised OMIS Contingency Plan, dated September 26, 2005, was provided to the Office of Environmental Information on October 3, 2005 and to your staff on October 14, 2005.

It should be noted that the OMIS Contingency Plan clearly states that the database is exported nightly from Research Triangle Park, NC to our backup servers in Washington, DC. If the contingency plan is put into effect, the Washington, DC servers would be converted to our

production servers. We have successfully tested this Plan with the procedures outlined in Appendix C and documented it in Appendix D: Disaster Recovery Testing.

Detailed comments are attached that we believe will sharpen the quality and accuracy of the draft report. Should you or your staff have questions or require further information, please have them contact Cheryl Varkalis at 202-564-6688.

Attachments (2)

cc: Lek Kadeli
Jack Puzak
Alice Sabatini
Amy Battaglia
Jorge Rangel
Tom Tracy
John Sykes
Cheryl Varkalis

ORD Comments
on
OIG Draft Audit Report
Audit of Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems located at the Environmental Protection Agency's (EPA's) Research Triangle Park Campus

1. On page 12 , paragraph 2, line 1, the draft report states:

"In reviewing the Office of Research and Development Management Information System (OMIS) contingency plan, we noted that the call tree within the contingency plan contains only business phone numbers for essential personnel, and does not include the information that should be relayed to critical personnel. In addition, we noted that the recovery operations sections of the contingency plan does not adequately document the steps necessary to restore operations, and it does not appear that the contingency plan has been tested."

RESPONSE: We request this paragraph be deleted from the report, or the report adjusted to reflect actions already taken by ORD.

Discussion: Appendix A: Personnel Contact List, has been updated to include all business, home, and cell phone numbers. The steps necessary to restore operations are contained in Appendix C: OMIS Technical Disaster Recovery Procedures, which details all of the steps necessary to restore operations. This has been tested and noted in OMIS Contingency Plan Appendix D: Disaster Recovery Testing.

2. On page 14, Recommendation 29, the draft report states:

"We recommend that the Director of OTOP work collaboratively with the Office of Research and Development to revisit:

29) OMIS contingency plan and ensure that the call tree within the contingency plan contains home phone numbers and cell phone numbers for essential personnel, and it also contains the key information that should be relayed to critical personnel. Further, the OMIS contingency plan should document the steps necessary to restore operations, and should also be tested on a regular basis."

RESPONSE: We request this paragraph be deleted from the report, or the report adjusted to reflect actions already taken by ORD.

Discussion: Section 3.3, Activation, of the OMIS Contingency Plan, states the key information that is relayed to critical personnel. The steps to restore operations are documented in Appendix C. OMIS Disaster Recovery Testing is included in Appendix D. The most recent test was performed in August 2005; testing will be performed on an annual basis.

3. On page 21, Appendix B, item 6, the draft report states:

"OMIS is comprised of six independent modules. Only the Integrated Resource Management System (IRMS) and the Laboratory Implementation Plan (LIP) interface with IFMS. The real-time interfaces are used to electronically transmit transactions (commitment and reprogramming) to IFMS. Extract files are created after the nightly IFMS close to bring down to IRMS the approvals/disapprovals of the reprogramming transactions as well as the operating plan, commitments, obligations, and expenditures from the Suballowance Spending Control Inquiry Table (SASP) and General Ledger tables.

RESPONSE: We request the following change to this portion of the draft report:

OMIS is comprised of five independent modules. Only the Integrated Resource Management System (IRMS) interfaces with IFMS. The real-time interfaces are used to electronically transmit transactions (commitment and reprogramming) to IFMS. Extract files are created after the nightly IFMS close to bring down to IRMS the approvals/disapprovals of the reprogramming transactions as well as the operating plan, commitments, obligations, and expenditures from the Suballowance Spending Control Inquiry Table (SASP) and General Ledger tables.

Discussion: The Laboratory Implementation Plan (LIP) has been retired and is no longer in production. Thus, there are only five independent modules. References to the LIP should be removed.

Appendix G
Office of Solid Waste and Emergency Response

Draft Report Response from the Office of Solid Waste and Emergency Response (OSWER)

November 11, 2005

MEMORANDUM

SUBJECT**:** OSWER Response to Draft Audit Report "Audit of Information System Service Contingency\Continuity and Physical Access Controls of EPA's Financial and Mixed-Financial Systems that Reside at Research Triangle Park"
Assignment/Project No: 2004-001383

FROM**:** Barry N. Breen/s/
Deputy Assistant Administrator

TO: Rudolph M. Brevard
Acting Director, Business Systems Audits
Office of Inspector General

Thank you for the opportunity to respond to the draft audit report on Information System Service Contingency and Physical Access Controls. We appreciate your efforts to hold informational meetings to ensure clarity of your findings and recommendations and to give us an opportunity to recommend revisions. Our comment on the OIG recommendation is as follows:

OIG Recommendation

We recommend that the Director of OTOP work collaboratively with the Office of Solid Waste and Emergency Response to revisit CERCLIS contingency plans and ensure that it identifies critical resources; ensure that the recovery test addresses all elements of application recovery; and ensure that contracts are in place for the restoration of the application.

OSWER Response

We agree with the Office of Environmental Information's (OEI) October 21, 2005 response regarding the recommendation. Over the past year, the Office of Superfund Remediation and Technology Innovation (OSRTI) has worked closely with RTP to centralize the CERCLIS Regional databases. Since then, the Contingency Plan for CERCLIS has been revised. Furthermore, a coordinated effort with RTP has taken place to perform a table-top review of the

CERCLIS application. This review was conducted in September 2005. In complying with Agency standards, OSRTI has used the two NIST documents which focus specifically on COOP Guidance. The first Document is 800-84 Guide to Single-Organization IT Exercises describes the procedures for the table-top review. The second guide, NIST 800-34, Contingency Planning Guide for Information Technology Systems describes in detail how to write a COOP Plan.

Please feel free to contact Robert King at 703.603.8792 or William Bushee at 703.603.8963, if you have any questions or need additional information.

Appendix H
Office of the Chief Financial Officer

Draft Report Response from the Office of the Chief Financial Officer (OCFO)

October 13, 2005

MEMORANDUM

SUBJECT: Office of the Chief Financial Officer (OCFO) Response to the Office of Inspector General's (OIG) Information Technology Position Paper #2 – Internal Control – Compliance with Federal Guidelines, Fiscal Year 2005 Financial Statement Audit

FROM: Michael W. S. Ryan
Deputy Chief Financial Officer /s/

TO: Rudy Brevard
Acting Director, Business Systems Audits

We appreciate the opportunity to provide written comments on the subject Position Paper. The OCFO remains firmly committed to securing its systems and data in a cost effective manner and in accordance with Federal guidance, EPA policy, and best practices.

If you or your staff have any questions or need additional information concerning our response to the subject Position Paper, contact Krista Mainess, Director of the Office of Program Management, at 202-564-5903.

cc: Paul Curtis, OIG
Bill Samuel, OIG

OIG recommendations and corresponding OCFO responses are as follows:

OIG Recommendation #1: Responsible office directors provide training to all application owners on the importance of developing, maintaining, and testing contingency plans in accordance with EPA and NIST guidelines and ensure the plans clearly define necessary recovery steps for each application.

OCFO Response to Recommendation #1:
In accordance with EPA requirements, OCFO mandates role-based training for employees with significant security responsibilities, which includes application owners. In addition, beginning in December 2005, the OCFO will conduct quarterly IT Security Council meetings for application owners.

OIG Recommendation #2: Director, Office of Budget revise the BAS contingency plan to contain (1) complete contact information for key personnel and (2) alternate processing and return to normal operations procedures.

OCFO Response to Recommendation #2:
We will include additional contact information for key personnel in the BAS contingency plan. The full record of contact information will include the individual's team position, name, home, work, and pager numbers, and e-mail address. In addition, we will clearly state the procedures for alternate processing and returning to normal operations.

OIG Recommendation #3: Director, Office of Financial Services revise the CPS contingency plan to identify critical recovery requirements and alternate processing procedures.

OCFO Response to Recommendation #3:
The critical recovery requirements and alternate processing procedures for CPS are provided in the NCC/CPS Critical Applications Disaster Recovery Plan (Sixth Edition, Revision 6-5), dated February 18, 2005.

We are providing the following document references for your consideration.

- Critical Hardware: Appendix C
- Critical Software: Appendix D
- Telecommunications: Section 4.6.9.2
- Facilities: Section 5.0

OIG Recommendation #4: Director, Office of Financial Services (OFS) revise contingency plan for People Plus to (1) contain primary and secondary personnel information consistent with the Critical Applications Disaster Recovery Plan and (2) clearly describe which plan takes precedence during the recovery process.

OCFO Response to Recommendation #4:
The primary and secondary contacts for PeoplePlus are contained in both the OCFO COOP and Critical Applications Disaster Recovery Plan. The OCFO COOP takes affect if a failure occurs

in the DC area, in accordance with the Agency's overall contingency plan. On the other hand, the Critical Applications Disaster Recovery Plan takes affect if a failure occurs at RTP. We will ensure the PPL contingency plan clearly states the order of precedence between itself and the Critical Applications Disaster Recovery Plan.

OIG Recommendation #5: Director, Office of Financial Management (OFM) revise contingency plans, for all of their applications not subscribing to the NCC DRS plan (e.g. Financial Data Warehouse), in accordance with relevant Federal and EPA criteria and best practices.

OCFO Response to Recommendation #5:
We are in the process of subscribing to the NCC Disaster Recovery Service for the Financial Data Warehouse. In addition, we will revise the contingency plan for SCORPIOS in accordance with relevant Federal and EPA criteria and best practices.