OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

PeoplePlus Security Controls Need Improvement

Report No. 2005-P-00019

July 28, 2005

Report Contributors: Rudolph M. Brevard
Corey Costango
Warren Brooks
William Coker

Abbreviations

EPA	Environmental Protection Agency
HR	Human Resources
IT	Information Technology
NACIC	National Agency Check with Inquiries and Credit
OARM	Office of Administration and Resources Management
OCFO	Office of the Chief Financial Officer
OFS	Office of Financial Services
OHR	Office of Human Resources
OIG	Office of Inspector General
PAR	Personnel action request
PPL	PeoplePlus
TOPOs	Task Order Project Officers

2005-P-00019
July 28, 2005

U.S. Environmental Protection Agency
Office of Inspector General

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

Our objectives were to determine whether: (1) the Environmental Protection Agency (EPA) adequately configured PeoplePlus' application security and technical infrastructure to protect the confidentiality, integrity, and availability of system data; and (2) implemented controls were working as intended.

Background

PeoplePlus is the EPA's new integrated human resources (HR), benefits, payroll, and time and labor system that is managed jointly by the Office of the Chief Financial Officer (OCFO) and the Office of Administration and Resources Management (OARM). Both HR and payroll data are processed to comply with Federal, State, and EPA reporting requirements.

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/2005/20050728-2005-P-00019.pdf

PeoplePlus Security Controls Need Improvement

What We Found

Our review identified three significant issues in the security administration of PeoplePlus (PPL). First, the Agency had not followed prescribed procedures for managing user access privileges, monitoring changes in employee responsibilities, and processing system access requests. Second, EPA did not verify or conduct the required National Agency Check with Inquiries and Credit background screenings for 45 percent (10 of 22) of contractor personnel with PPL access. Third, EPA implemented PPL without adequately implementing security controls for two key processes. Specifically, OCFO had not properly secured default user IDs and did not adequately separate incompatible duties performed by the Security Administrator.

What We Recommend

We recommend the Directors of EPA's Office of Financial Services (OFS) and Office of Human Resources (OHR) take 13 actions to improve PPL security controls. These recommendations address areas where EPA could improve user access management and contractor background screening procedures. These recommendations include: (1) reinforcing the requirements to follow prescribed policies and procedures; (2) providing a training program to increase awareness and ability to perform security duties; (3) evaluating the need for system development contractors to have access to the production environment; and (4) establishing a milestone date to complete contractor background screening. We recommend that EPA evaluate all default user IDs to secure them, and assign Security Administrators' responsibilities in a manner that provides adequate separation of incompatible duties. EPA concurred with all of our recommendations and provided a plan of action to address concerns.

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

OFFICE OF
INSPECTOR GENERAL

July 28, 2005

MEMORANDUM

SUBJECT: PeoplePlus Security Controls Need Improvement
Report No. 2005-P-00019

FROM: Rudolph M. Brevard, Acting Director /s/
Business Systems Audits

TO: Charles E. Johnson
Chief Financial Officer

Luis A. Luna
Assistant Administrator for
Administration and Resources Management

This is our final report on the PeoplePlus security controls audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe problems the OIG has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, 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.

Action Required

The Action Officials do not have to provide a response to this report. The Agency's response to the draft report contained an adequate corrective action plan with milestone dates to implement the plan. 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 have any questions regarding this report, please contact me at (202) 566-0893.

Table of Contents

Chapter 1
Introduction

Purpose

Our objectives were to determine whether: (1) the Environmental Protection Agency (EPA) adequately configured PeoplePlus' application security and technical infrastructure to protect the confidentiality, integrity, and availability of system data; and (2) implemented controls were working as intended.

Background

PeoplePlus (PPL) is the EPA's new integrated human resources (HR), benefits, payroll, and time and labor system that is managed jointly by the Office of the Chief Financial Officer (OCFO) and Office of Administration and Resources Management (OARM). The system processes the data to comply with Federal, State, and EPA reporting requirements.

As both the HR and payroll system, PPL contains confidential personnel information, such as names, addresses, Social Security numbers, and employee IDs. In this regard, EPA classified PPL's data sensitivity level as high for confidentiality, integrity, and availability because:

- The Privacy Act requires protection of the personnel information in the system;
- Miscalculation of payroll and entitlements could occur due to inaccurate or erroneously modified data; and
- Unavailability of data would adversely affect the Agency's ability to make financial payments, address benefits issues, or meet internal reporting requirements.

EPA established policies to guide its employees and contractors on controlling and securing access to the PPL system, as well as the network and other Agency information resources. OCFO developed procedures for online access to the system. OCFO also developed the PPL Security Plan, which details the managerial, operational, and technical controls for securing PPL. Likewise, EPA created a network security policy that establishes controls to ensure a secure network infrastructure. The Agency's Information Security Manual sets forth requirements for securing information resources in accordance with EPA and Federal policies. Appendix A contains a summary of key Agency policies.

Scope and Methodology

We conducted this audit from November 2004 to April 2005 at EPA Headquarters in Washington, DC. We interviewed Agency personnel and contractors responsible for processing HR and payroll transactions and securing the application. We reviewed Agency policies, procedures, reports, and forms used to grant users system access and enforce system security. We conducted system walkthroughs of user functionality and selected a judgmental sample of functional users within the Office of Financial Services (OFS) and the Office of Human Resources (OHR) to evaluate their system access. Functional users are EPA employees or contractors that have special access to PeoplePlus in order to process human resources, time keeping, or payroll transactions; or perform system security maintenance. This audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

Results in Brief

Program offices had not followed prescribed procedures to limit employees' system access, monitor changes in employees' system needs, process system access requests, or conduct background screenings on contractors. We identified the following additional weaknesses: (1) program offices did not develop procedures to carry out their assigned system responsibilities, and (2) personnel required additional training to perform their assigned duties. Without restricting user access to the minimal set of privileges necessary, users could circumvent the organizational security policy in order to expose the Agency to attacks or damage the information technology (IT) infrastructure.

Furthermore, EPA implemented PPL without adequately implementing security controls for two key system maintenance processes. OCFO had not properly secured default user IDs shipped with the system. A user ID is a number or name, which is unique to a particular PeoplePlus user. Furthermore, OCFO had not separated incompatible duties performed by the Security Administrator. During system development, EPA did not conduct an analysis to: (1) determine which default accounts were necessary to operate the system, (2) develop a strategy to mitigate the risks associated with prepackaged default accounts, and (3) design controls to ensure one person could not authorize or approve system changes without detection. EPA places itself at greater risk because an employee could use the IDs or incompatible duties to bypass implemented controls without detection and undermine the integrity of the data processed through the system.

We made 13 recommendations to improve PPL security controls. EPA concurred with all of our recommendations and provided a plan of action to address concerns. We included EPA's complete response as Appendix B.

Chapter 2
Further Steps Needed to Improve User Account Management

EPA did not effectively manage PPL user system access. Specifically, OCFO and OARM had not followed prescribed procedures for managing user access privileges, monitoring changes in employee system access needs, or granting users access consistent with requests. This occurred because Agency personnel did not conduct required tasks, such as: (1) verifying employee access requests to assigned responsibilities, (2) reviewing user access needs on a quarterly basis, (3) monitoring the changes in employee duties, and (4) maintaining documentation to support access to the system. This led to excessive – unnecessary or incompatible – system access, which could allow users to circumvent implemented security controls and increases the likelihood that errors or wrongful acts go undetected.

Managing Access Privileges

PPL functional users received more system access than necessary to perform their job responsibilities. Several employees had system access privileges that gave them the capability to perform unnecessary or incompatible functions. For example:

- OCFO employees, whose access should have been limited to entering data, had the ability to approve data as well. Specifically, two OCFO employees within the Payroll Management section could calculate and confirm pay sheets in addition to the ability to review and approve these same payroll transactions. In addition, one of these employees had access that allowed that person to perform incompatible time-keeping and approving functions. With this access, the employee could record hours worked, and verify and approve data on employee time sheets. We also noted that approximately 44 other employees had access to these same incompatible time-keeping and approving functions. However, we did not verify to what extent these other employees were using this access.

- OARM gave a user system access to critical HR functions, with the ability to input personnel action requests (PARs); although the employee only needed the ability to generate reports.

- Several system development contractors have functional user roles (a specific set of rights and privileges) within the production environment. These roles provide the contractors with the ability to process general

payroll transactions, update employee pay records, and review and approve individual payroll transactions. The contractors also have the ability to record and approve hours worked on employee time sheets, process PAR transactions, and manage employee records.

Monitoring Changes in System Access

EPA did not remove system access after users either transferred to other offices or were assigned different job responsibilities. These employees retained their previous system access privileges, although they did not need the access for their current duties. For instance:

- OCFO had not requested the removal of full system access for a contractor recently assigned to other duties. Although the contractor needed elevated access during system validation, the office took no action to reduce the contractor's access once EPA placed PPL into production.

- The OCFO Payroll Supervisor, with access to key payroll processing functions, transferred to the Office of Research and Development in November 2004. However, neither office took action to ensure the employee's system access was consistent with their duties; although Agency policy requires this analysis. In addition, OCFO had not updated system access privileges for the current Payroll Supervisor, who transferred from the Systems Planning and Integration Staff group.

Processing Access Requests

EPA had not correctly processed user access request forms for 79 percent (11 of 14) of the users in our sample. Although EPA granted functional users system access to key HR and payroll functions, we found Security Administrators did not maintain or process system access documentation in accordance with prescribed procedures. We selected a sample of 14 functional users to validate whether EPA processed access requests according to prescribed policies. As indicated in Table 1, EPA granted system access in accordance with prescribed policies 21 percent of the time. For the remainder of the users, EPA granted system access either without adequately prepared (unavailable or unsigned) documentation or inconsistent with the requests.

Table 1 - Analysis of PeoplePlus System Access Forms

Access Granted:	Number	Percent
With Adequate Documentation	3	21
Without Adequate Documentation	7	50
Inconsistent with Requests	4	29
Total	14	100

Online Security Policy Enforcement and System Access Definitions Are Ineffective

EPA has not managed user accounts effectively because personnel did not follow existing security policies and system access user roles were not adequately developed.

Although OCFO provided broad overarching guidance for securing the PPL system, program offices carry out these responsibilities inconsistently. As a result, personnel did not conduct required tasks such as: (1) verifying employee access requests to assigned responsibilities; (2) reviewing user access needs quarterly; (3) monitoring the changes in employee duties; and (4) maintaining documentation to support access to the system.

EPA's analysis of user access requirements to develop system access roles was inadequate. In many cases, we found EPA developed system access roles based on the employee duties in the separate HR and Payroll systems as opposed to the access needed for the new combined system. In addition, EPA developed generic system access roles to perform a series of related tasks and then gave employees this access regardless of whether they performed those duties.

Inconsistent compliance with security guidance and inadequate user role development led to excessive user access privileges. Although EPA implemented procedures to monitor payroll processing, an employee with excessive privileges could inappropriately change payments to individuals if the review procedures are not followed or enforced. In addition, excessive access provides employees with unnecessary opportunities to circumvent system security and sets the stage for situations where errors or wrongful acts could go undetected.

Recommendations

We recommend the Director of the Office of Financial Services:

2-1 Conduct and document an analysis of functional user system access requirements to create appropriate roles that restrict employee access to necessary functionality.

2-2 Assign all current system users to the appropriate roles.

We recommend the Directors of the Office of Human Resources and the Office of Financial Services:

2-3 Develop and publish a joint policy memorandum to all staff reinforcing established policies and procedures outlined in the PPL Security Plan and Online Access Guide.

2-4 Develop and implement a strategy to increase managers' awareness of security responsibilities assigned to their employees.

2-5 Provide in-depth training for the assigned PPL Access Coordinators and Security Administrators. Establish milestone dates when all PPL Access Coordinators and Security Administrators will complete the training.

2-6 Establish milestone dates when offices will implement the required quarterly reviews of user system access.

2-7 Conduct and document an evaluation of system access needs for system development contractors with access to the production environment. Establish, document, and implement controls to limit and monitor contractor access.

Agency Comments and OIG Evaluation

The Directors of both OFS and OHR concurred with our seven recommendations to improve PPL user account management. The Agency has completed some analysis of functional user roles and completion dates for corrective actions to address our remaining recommendations. The corrective actions planned are appropriate and will adequately address the recommendations.

Chapter 3
Improvements Needed in Contractor Background Screening Process

EPA did not ensure that contractors obtained an appropriate background check before granting them access to PPL. Our review indicated that offices granted contractors access to the system without verifying whether contractor personnel had the required National Agency Check with Inquiries and Credit (NACIC). These weaknesses occurred because the Agency did not follow the procedures outlined in the online access policy. These weaknesses in basic controls have the potential to undermine an essential part of the system's security.

EPA Did Not Follow Contractor Background Screening Procedures

EPA did not ensure contractors obtained the required background check before granting them access to PPL. We reviewed the background check status for all OCFO and OARM contractors with system access. We found that for 10 of 22 contractors (45 percent), the program offices authorized access to the system without verifying the contractor had completed the Agency-required NACIC background check.

These weaknesses occurred because neither program office followed the procedures outlined in the online access policy. Specifically, we found that the Task Order Project Officers (TOPOs), responsible for authorizing and requesting system access, needed additional training on EPA-prescribed contractor background screening procedures. In addition, OARM did not establish procedures to follow up on requested background screening checks for contractors given temporary system access.

Because intentional and unintentional employee actions are the primary cause of disruptions of information system integrity and operation, security controls should provide reasonable assurance that systems are safeguarded. Although not infallible, background checks serve as a basic control to determine whether contractors are suitable to have access to sensitive Agency information. These checks are an integral part of an overall system of controls to protect the confidentiality, integrity, and availability of information systems.

Furthermore, while authorizing temporary system access is sometimes necessary, offices should use it sparingly and monitor it to maintain internal controls. By not implementing processes to follow up and promptly remove the access when no longer required, management places EPA in greater risk that unscrupulous individuals could undermine the integrity of the system.

Recommendations

We recommend that the Directors of the Office of the Human Resources and the Office of Financial Services:

3-1 Develop, implement, and document a formal training program for the personnel responsible for requesting and approving contractor personnel access to PPL. Ensure that all TOPOs receive the training.

3-2 Develop, implement, and document specific procedures for processing contractor personnel background screening requests.

3-3 Develop and implement a monitoring process for contractors granted temporary access to PPL.

3-4 Establish a milestone date to complete NACIC security screenings for all contractor personnel with system access.

Agency Comments and OIG Evaluation

The Directors of both OFS and OHR concurred with our four recommendations to improve the contractor background screening process. The Agency has completed all NACIC security screenings for the contractor personnel we identified in the report as not having a verified background check. The Agency established target dates for addressing our remaining recommendations. The corrective actions planned are appropriate and will adequately address the recommendations.

Chapter 4
Improvements Needed for Default User IDs and Security Administrator Duties

EPA implemented PPL without adequately developing security controls for default user IDs and adequately separating incompatible duties performed by the Security Administrator. By not controlling special access accounts and adequately separating duties, a person could bypass implemented controls without detection and undermine the integrity of the data.

Default User IDs Not Secured

EPA has not secured default user IDs, which allow users to by-pass security controls. Default user IDs are of two types: "Super User IDs" and "User IDs." Super User IDs have unrestricted access to the system. User IDs provide unlimited access for specific application modules, such as HR or Payroll. Our review disclosed that 7 of 9 (78 percent) IDs listed in a Security Administrator account were default user IDs. Although the Security Administrator changed the account passwords and locked some accounts, we found three of the default user IDs were still active.

Like many enterprise resource planning applications, PPL comes with multiple default user IDs with passwords set to commonly known factory settings. The manufacturer delivered the PPL software to EPA with default user IDs and passwords. According to industry security best practices, the Agency should have appropriately secured the default user IDs and passwords, by: (1) locking, (2) removing, or (3) changing them as part of the system implementation process. Immediate and proper identification and maintenance of these IDs, especially Super User IDs, are vital to the security of the application. With knowledge of the system's configuration and access to EPA's network, a person could use a default user ID to exploit PPL.

Although EPA developed a system security plan and provided broad overarching security guidance, we found that key security documents were either not prepared or unavailable for review. Specifically, EPA had not prepared an analysis of the design and assignment of permissions and roles within the system. In this regard, EPA had not documented which default IDs were necessary for the system to process HR and payroll transactions or the remediation actions necessary to secure those accounts not needed.

Security Administrator Performs Incompatible Duties

Our analysis determined that one Security Administrator had system access and responsibilities for three incompatible, critical security functions. These functions should be separate to ensure that no one person has complete control over the implementation of program changes without detection. A Security Administrator responsible for implementing user roles could inadvertently or deliberately obtain access to PPL functions that are not in accordance with management policies. Specifically, this particular Security Administrator was responsible for:

- Creation and maintenance of roles and permission lists;
- Migration of roles and permission lists into the production stage; and
- Creation and maintenance of user profiles.

The performance of incompatible duties is a common security concern, but is further heightened when an employee with control over the system performs the duties. The Security Administrators are one of the pillars of an effectively implemented system of controls. Because of this, EPA places itself at greater risk when a Security Administrator performs incompatible duties that are vital to the underlying security of the application. In addition, the potential exists that system changes could occur and go undetected which could undermine the controls management must rely upon for the integrity of the information processed by the system.

As previously stated, EPA had not adequately described the design and assignment of permission lists and roles within the system. Furthermore, EPA had not: (1) analyzed Security Administrator responsibilities to ensure one employee was not performing incompatible duties, (2) assigned duties between the two Security Administrators, and (3) provided sufficient training to security personnel to perform these duties.

Recommendations

We recommend that the Director of the Office of Financial Services:

4-1 Conduct and document an analysis of default user IDs to determine the necessity for each default account and deactivate default user IDs as appropriate.

4-2 Conduct and document an analysis of Security Administrator responsibilities and assign duties in a manner that provides adequate separation of duties.

Agency Comments and OIG Evaluation

The Director of OFS concurred with our two recommendations to review the status of default user IDs and to analyze Security Administrator responsibilities for adequate separation of duties. The Agency has completed an analysis of default user IDs and has planned a completion date for conducting and documenting a thorough analysis of Security Administrator responsibilities. The corrective action planned is appropriate and will adequately address the remaining recommendation.

Appendix A

Agency Criteria

Office of Financial Management, Policy Announcement No. 04-01, Policies and Procedures for Online Access to EPA's Integrated Human Resources, Benefits, Payroll, Time and Labor Management System-PeoplePlus, provides procedures for online access to the system. In addition, the Policy provides procedures for requesting and changing user IDs, passwords, and access; security training for PPL access coordinators and users; and responsibilities of individuals with system access. Specifically, Security Administrators are responsible for verifying that requested access is limited to the performance of a user's assigned responsibilities, monitoring adherence to the policies and procedures contained in this Policy, and conducting an annual review of system online security functions. The Agency should monitor any changes to authorized users' employment status or changes in the duties affecting their access, conduct quarterly reviews of user access needs to ensure only those authorized functions that are required to perform their current duties are retained in their security profiles, and retaining copies of the user access request forms. The Policy also identifies maintaining and ensuring adequate segregation of duties as a vital procedure for controlling access to the system. Additionally, program offices are required to ensure contractor personnel have, at a minimum, a NACIC background screening before granting access to PPL.

Office of Chief Financial Officer/Office of Administration Resources Management, PeoplePlus (PPL) Security Plan, details the managerial, operational, and technical controls for securing the PPL system. This document describes personnel security requirements as well as the requirements for segregation of duties and minimal privileges. The Security Administrators are responsible for reviewing the requests to provide reasonable assurance that unnecessary privileges are not granted. In addition, the Security Administrators are responsible for reviewing access lists quarterly to verify that users continue to need access. User access must be restricted to the minimum necessary to perform the job. At a minimum, any contractor support must pass the NACIC background check before gaining access to PPL.

EPA Order No. 2195.1 A4, Network Security Policy, establishes basic controls to ensure a secure network infrastructure. It specifies that: (1) access authorizations and controls must follow the principles of "need-to-know," "need-to-perform," and "least privilege" in relation to functional requirements; (2) access authorizations must be documented; and (3) authorizations and associated authentication methods must be periodically reviewed, tested, and verified. In addition, the Policy specifies that network procedures, standards, and operating practices for implementation of this policy are consistent with National Institute for Standards and Technology requirements, and documented industry standards and best practices.

EPA's Information Security Manual sets forth requirements and guidance for securing Agency information resources in accordance with EPA and Federal security policies and mandates. Specifically, the policy lists requirements for personnel screening, logical access controls, and establishing proper segregation of duties.

Appendix B

Agency Response to Draft Report

July 20, 2005

MEMORANDUM

SUBJECT: PeoplePlus Security Controls Audit Report

FROM: Milton Brown, Director /s/
Office of Financial Services (2734R)

Rafael DeLeon, Director /s/
Office of Human Resources (3610A)

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

We thank you for the opportunity to review and provide comments on the PeoplePlus (PPL) Security Controls Draft Audit Report (Assignment No. 2005-00342). The Office of Financial Services (OFS) and the Office of Human Resources (OHR) support the specific audit objectives: "to determine whether: (1) the Environmental Protection Agency (EPA) adequately configured People Plus application security and technical infrastructure to protect the confidentiality, integrity, and availability of system data; and (2) implemented controls were working as intended." Based on already planned actions and the audit findings, we will continue to improve security policies, training, and general oversight of PPL security. In addition, OFS will work with users and payroll staff to address concerns and implement improved compliance of the system.

The report identifies issues with controls that it claims are commonly bypassed and lacking in management oversight. The report implies that problems are commonplace and places the Agency at substantial risk. We believe this is subject to interpretation and is overstated. Management in the Office of the Chief Financial Officer (OCFO) and the Office of Administration and Resources Management (OARM) take the integrity and privacy of employees' personnel and payroll data very seriously, and our staffs understand the importance of maintaining data integrity.

The report also states that actions that might be allowed by users with excessive privileges could create system compromises "without detection". As was provided in earlier draft responses, all payroll actions are audited, and if a supervisor or security administrator

caused inappropriate or adverse actions to occur, full audit records are available to the Agency payroll audit team. In no case does any action go undetected.

In addition, the report implies that security role development and role/default account management were haphazard and lacking in attention to detail. The report does not reflect the amount of attention placed on security controls. While these areas need to be reviewed and updated now that the system is in full production, OFS spent considerable time and attention establishing and working on these areas prior to implementation.

Attached is our response to your recommendations presented to us in the draft audit report. We again appreciate the opportunity to work through the issues and we appreciate your consideration of our comments on the audit.

If you have any questions or require additional information or clarification concerning our response, please contact Sheila Bullock, Office of Financial Services on (202) 564-5202 and Brenda Daly, Office of Human Resources on (202) 564-6290.

Attachment

cc: Raffael Stein 2734R
Janice Kern 2734R
Jayna Alexander 2734R
Carline Ransom 2734R
Sheila Bullock 2734R
Corey Costango 2421T
Warren Brooks 2421T
William Coker 2421T
Mike Hamlin 3631M
Jeuli Bartenstein 3631M
Brenda Daly 3631M
Dennis Nolan 2733R
Richard Bennett 2733R
Joseph L. Dillon 2731A
Krista Mainess 2710A
Larry Burnham 2710A

Attachment

Responses to Recommendations

No.	Recommendation	Concur / Non-Concur	Responsible Office	Planned Completion Date	Comments
We recommend the Director of the Office of Financial Services:					
2-1	Conduct and document an analysis of functional user system access requirements to create appropriate roles that restrict employee access to necessary functionality.	Concur	OFS	06/30/2005 07/31/2005 08/31/2005 08/31/2005	We have performed an analysis of functional user system access requirements to create appropriate roles associated with job functionality. Payroll roles were completed as of 6/30/05. The Help Desk roles will be completed by 7/31/05 and Time & Labor roles will be completed by 8/31/05. All roles will be documented by 08/31/05.
2-2	Assign all current system users to the appropriate roles.	Concur	OFS	08/31/2005	All current system users will be assigned to appropriate roles. In addition, those anomalies identified in the IG Report has been corrected. We will continue to monitor security access to ensure that these inconsistencies do not occur again.
We recommend the Directors of the Office of the Human Resources and the Office of Financial Services:					
2-3	Develop and publish a joint policy memorandum to all staff reinforcing	Concur	OFS/OHR	08/31/2005	OFS and OHR will work together to develop and publish a joint policy memorandum to re-emphasize to staff the

	established policies and procedures outlined in the PPL Security Plan and Online Access Guide.				importance of the guidance provided in the PPL Security Plan and Policy Announcement 04-01 (Policies and Procedures for On-Line Access to EPA's Integrated Human Resources, Benefits, Payroll, Time and Labor Management System-PeoplePlus).
2-4	Develop and implement a strategy to increase managers' awareness of security responsibilities assigned to their employees.	Concur	OFS/OHR	08/31/2005	OFS and OHR are working together to develop and implement a strategy to increase managers' awareness of the PPL security responsibilities assigned to their employees. Implementation of this strategy is scheduled to begin on 07/29/05. We will include this in the PPL manager training planned for August.
2-5	Provide in-depth training for the assigned PPL Access Coordinators and Security Administrators. Establish milestone dates when all PPL Access Coordinators and Security Administrators will complete the training.	Concur	OFS/OHR	08/31/2005 Completed Completed Completed Completed Completed Completed	We are in the process of providing in-depth training for the PPL Access Coordinators. The Security Administrators will also be provided training as appropriate. Please note the completed training for the OFS and OHR Security Administrators. *OFS Security Administrator* - PeopleSoft Security Training version 8.12 September 10-12, 2002 - PeopleSoft Security Training July 12-14, 2005 *OHR Security*

					Administrator - PeopleSoft Security Training version 8.12 April 27, 2002 - PeopleSoft Security Training version 8.4 March 2, 2004 - Attended IT Security and Operations conference May 17-21, 2004 - Attended IT Security and Operations conference (ISO) April 11-14, 2005
2-6	Establish milestone dates when offices will implement the required quarterly reviews of user system access.	Concur	OFS/OHR	08/31/2005	The required quarterly reviews will be conducted for contractors and functional users. In addition, quarterly reminders of the policy and procedures for maintaining PPL access will be provided to the PPL Access Coordinators. The milestone dates for quarterly reviews and reminders are: September 20, 2005 June 30, 2006 December 31, 2005 September 20, 2006 March 31, 2006 December 31, 2006
2-7	Conduct and document an evaluation of system access needs for system development contractors with access to the production	Concur	OFS/OHR	07/31/2005 07/31/2005	OFS and OHR will conduct and document an evaluation of system access needs for system contractors. We will also establish, document, and implement controls to ensure

	environment. Establish, document, and implement controls to ensure contractor access is limited and monitored.				contractor access is limited and based on current responsibilities. Please note that controls exist today to monitor and track contractor access through the audit log. (Currently this function is performed biweekly.) This will formalize our procedures.
3-1	Develop, implement, and document a formal training program for the personnel responsible for requesting and approving contractor personnel access to PPL. Ensure that all Task Order Project Officers (TOPO) receive the training.	Concur	OFS/OHR	08/31/2005	OFS and OHR will develop, implement, and document a formal training plan for the personnel responsible for requesting and approving contractor personnel access to PPL. In addition, we will ensure that the TOPOs receive training.
3-2	Develop, implement, and document specific procedures for processing contractor personnel background screening requests.	Concur	OFS/OHR	On-Going	OFS and OHR will document and continue to implement specific Agency procedures such as the SF-85 process, and the OF-306 process, as well as the funding procedures necessary to complete these tasks.
3-3	Develop and implement a monitoring process for contractors granted temporary access to PPL.	Concur	OHR	10/2005	It is OHR's responsibility to implement the Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The Policy requires that EPA's non-

					Federal workers undergo Federally-sponsored background checks before being issued smart cards that will permit access to our facilities and information systems. EPA's implementation plan has been submitted to the Office of Management and Budget (OMB), with implementation expected in October. We believe that our efforts will result in a comprehensive Agency program for non-Federal worker background checks consistent with HSPD-12. Also, we will implement a monitoring process which will perform periodic checks on the status of the NACICs for all contractors that have been granted temporary access to PeoplePlus.
3-4	Establish a milestone date to complete documented NACIC security screenings for all contractor personnel with system access.	Concur	OHR	Completed	As of 06/30/2005, OFS and OHR completed all NACIC security screenings for all contractor personnel with system access (See Chapter 3 of Audit Report). We feel that the need for key milestones are no longer relevant due to the fact that we are following the EPA Information Security Manual 2195A1, 1999 Edition, page 68, which states: "The NACIC screening must occur prior to providing contractor personnel with access to

					EPA systems. Contractor personnel must submit required background investigation documentation within ten (10) days after initiation of contract. To avoid unnecessary delays, new contractor personnel may begin work while the OPM screening is in progress, provided contractor personnel have already completed pre-screening requirements by their employer." We will develop a process to monitor the status of the NACIC.
We recommend that the Director of the Office of Financial Services:					
4-1	Conduct and document an analysis of default user IDs to determine the necessity for each default account and deactivate default user IDs as appropriate.	Concur	OFS	Completed	On 06/23/05, we conducted and documented an analysis of default user IDs to determine the necessity for each default account (See Chapter 4 of Audit Report). Based on the analysis it was determined that three IDs were not locked and of the three, we locked two and the passwords were changed. The third user ID could not be locked because it is used to create User Accounts. However, the access was restricted to the Security Administrator in a different name. In addition, the Default User IDs passwords will be changed quarterly – every 90 days.
4-2	Conduct and document an analysis of Security	Concur	OFS/OHR	07/31/2005	OFS will conduct and document a thorough analysis of Security

	Administrator responsibilities and assign duties in a manner that provides adequate separation of duties.				Administrator responsibilities and assign duties in a manner that provides adequate separation of duties. Please note that the Security Administrator is a special and complex case. Any user with super user privilege presents separation of duties and trust issues in any production system environment with sensitive or financial data.

Appendix C

Distribution

Office of the Administrator
Director, Office of Financial Services
Director, Office of Human Resources
Audit Coordinator, Office of the Chief Financial Officer
Audit Coordinator, Office of Administration and Resources Management
Director, Technical 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
Inspector General