

# Office of Inspector General

---

U.S. Department of Labor

Office of Information Technology Audits

## Government Information Security Reform Act (GISRA) Evaluation of PeoplePower HRMS Application

### Final Report

This review was performed by KPMG LLP under contract to the Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

/s/

JOHN J. GETEK

Assistant Inspector General for Audit

**Report Number: 23-01-013-07-001**

**Date Issued: September 28, 2001**

# Table of Contents

<u>Section</u>	<u>Page</u>
<b><u>EXECUTIVE SUMMARY.....</u></b>	<b><u>1</u></b>
POSITIVE SECURITY CONTROL OBSERVATIONS .....	1
SECURITY CONTROL ISSUES .....	1
<i>High Risk Control Issues</i> .....	<i>1</i>
<i>Medium Risk Control Issues</i> .....	<i>1</i>
OASAM MANAGEMENT RESPONSE .....	2
CONCLUSION.....	2
<b><u>INTRODUCTION.....</u></b>	<b><u>3</u></b>
BACKGROUND.....	3
<i>Department of Labor</i> .....	<i>3</i>
<i>Office of the Assistant Secretary for Administration and Management</i> .....	<i>3</i>
<i>Office of Chief Information Officer</i> .....	<i>3</i>
<i>PeoplePower</i> .....	<i>3</i>
OBJECTIVES .....	3
SCOPE AND METHODOLOGY.....	4
<b><u>FINDINGS AND RECOMMENDATIONS.....</u></b>	<b><u>4</u></b>
HIGH RISK CONTROL ISSUES .....	5
MEDIUM RISK CONTROL ISSUES .....	11
<b><u>ACRONYMS.....</u></b>	<b><u>18</u></b>
<b><u>Appendix 1.....</u></b>	<b><u>19</u></b>

## **EXECUTIVE SUMMARY**

The Department of Labor's (DOL) Office of Inspector General (OIG), engaged KPMG to perform independent evaluation services in accordance with the Government Information Security Reform Act (GISRA). KPMG performed its evaluation over the Office of the Assistant Secretary for Administration and Management (OASAM) PeoplePower Human Resources Management System (HRMS) that encompasses PAR processing, Payroll, and Benefits<sup>1</sup> and runs in the PeoplePower (i.e., PeopleSoft®) General Support System<sup>2</sup> environment. The evaluation was conducted from June 20, 2001 through August 09, 2001, at the DOL headquarters in Washington, DC.

KPMG's objectives were 1) to determine OASAM's response to the Office of Management and Budget (OMB) M-01-24 Memorandum, Reporting Instructions for the Government Information Security Act, and 2) report any material weaknesses found as a result of our evaluation.

### **Positive Security Control Observations**

As implemented by OASAM in the context of the PeoplePower HRMS application, DOL's security program appears to:

- Feature most of the components identified in the NIST Self-Assessment Guide.
- Be reasonably integrated in to OASAM business processes.
- Except as noted below, operate with sufficient effectiveness to provide reasonable, but not absolute assurance over the confidentiality, integrity, and availability of information handled by the Personnel/Benefit applications.
- Be adequately resourced and supported by senior management.

In addition, PeoplePower is being implemented using a proprietary Implementation methodology that appears to adequately address GISRA control objectives.

### **Security Control Issues**

However, we note that PeoplePower does not exist in isolation from the rest of the OASAM/DOL IT environment. Security and assurance at the PeoplePower HRMS application level are directly or indirectly impacted by weaknesses in the OASAM environment generally, and in the backbone network specifically. In this context, we identified 10 control findings during our evaluation that OASAM and PeoplePower must address to satisfy basic PeoplePower application security and assurance requirements. They are categorized as high and moderate risk security control issues.

The high and moderate control issues that directly or indirectly impact PeoplePower HRMS application are presented below.

#### ***High Risk Control Issues***

1. PeoplePower does not follow the DOL Systems Development Life Cycle processes.
2. PeoplePower has not developed or tested a Disaster Recovery Plan.
3. PeoplePower does not have a formal Incident Response Plan.
4. PeoplePower Operational Procedures do not fully implement controls articulated in the Computer Security Handbook.
5. PeoplePower has not been formally certified or accredited.

#### ***Medium Risk Control Issues***

6. While PeoplePower users are required to sign PeoplePower system-level rules of behavior, there are no

---

<sup>1</sup> As defined in OMB Circular A-130, Appendix III

<sup>2</sup> *ibid*

- corresponding network rules of behavior.
7. PeoplePower user access rights are not reviewed annually to determine if system access is commensurate with job responsibilities.
  8. An application controls review has not been performed on PeoplePower applications.
  9. PeoplePower audits, program reviews and security reviews do not follow a consistent methodology or employ the same measures of performance.
  10. PeoplePower does not follow formalized termination procedures for employees (LAN access, etc).

### **OASAM Management Response**

We issued a Tentative Findings and Recommendations (TFAR) document to OASAM's PeoplePower program Management on August 24, 2001. The acting PeoplePower Team Director reviewed and had no comment on any of the evaluation's tentative findings.

In response to the draft, OASAM's management generally concurred with the finding and recommendations and identified actions taken and planned that address the recommendations. OASAM's comments to the draft are summarized under the "Management Comments" section for each finding. OASAM's complete response to the draft report is included in its entirety as Appendix 1 to the report.

### **Conclusion**

The actions taken and planned by OASAM, when fully implemented, should satisfy the intent of the recommendations. Additionally, we provided comments and/or conclusions under the "Conclusion" section for each of the findings.

# INTRODUCTION

## Background

### *Department of Labor*

DOL is responsible for the administration and enforcement of Federal statutes relating to the American workplace and the U.S. workforce. The legal and regulatory framework created by these statutes is implemented through a broad range of workplace programs that affect employers and employees. DOL activities include programs to protect workers' wages, improve workplace health and safety, regulate employment and pension rights, promote equal employment opportunity, and administer job training, unemployment insurance, and workers' compensation programs. In addition, DOL is charged with strengthening free collective bargaining, and collecting, analyzing, and publishing labor and economic statistics. DOL is headquartered in the Frances Perkins Building, 200 Constitution Avenue NW, Washington, D.C. (FPB).

### *Office of the Assistant Secretary for Administration and Management*

Within DOL, OASAM serves as the Secretary's principal advisor for DOL administration and management. In this capacity, OASAM directs the development, implementation, review, and evaluation of DOL-wide administrative and management policies and programs. This includes DOL's IT plans and programs.

### *Office of Chief Information Officer*

OASAM manages the DOL IT program through its Office of Chief Information Officer (OCIO), headed by the Chief Information Officer (CIO). The CIO position was established in 1997 pursuant to guidance contained Section 5125<sup>3</sup> of the Information Technology Management Reform Act (ITMRA). While the OCIO is a component organization within OASAM, the CIO reports directly to the Secretary.

### *PeoplePower*

One of DOL's strategic IT goals is to increase integration of DOL IT systems and extend access to automated services implement information resources in such a way that they improve economy, efficiency, and effectiveness in departmental IT operations. A phased implementation of an integrated HRMS application is viewed as an enabler of this goal; the PeoplePower (human resources) application represents a keystone activity in achieving this end. Currently, the HRMS application is used to support customary employee payroll and benefits functions throughout DOL. The applications are hosted on SUN and NT servers; these servers are located at DOL headquarters at the FPB. Network connectivity is provided across DOL's Employee Computer Network (ECN). ECN consists of 22 TCP/IP-based LAN segments in the FPB and LAN segments in each of the 10 OASAM Regional offices. PeoplePower users can access PeoplePower applications and services across the ECN from any DOL PC-based desktop computers that has the proper client software loaded using a standardized graphical user interface; currently, approximately 440 people have been granted PeoplePower access.

## Objectives

The objective of the evaluation was to determine: OASAM's response to the Office of Management and Budget (OMB) M-01-24 Memorandum, Reporting Instructions for the Government Information Security Act and report any material weaknesses found as a result of our evaluation.

---

<sup>3</sup> ITMRA Section 5125 amends 44 U.S.C. § 3506 that governs the coordination of Federal information policy. The amendment establishes the authority for the position of CIO in all Federal agencies.

## Scope and Methodology

In accordance with the GISRA, the DOL OIG contracted KPMG to serve as the OIG's independent evaluator of OASAM's PeoplePower HRMS application. The evaluation was conducted at DOL headquarters in Washington, DC from June 20, 2001 through August 09, 2001.

KPMG conducted the evaluation using guidance from the National Institute of Standards and Technology's (NIST) Self-Assessment Guide for Information Technology Systems and the Federal Information System Controls Audit Manual (FISCAM). This guidance was used to reply to the Office of Management and Budget (OMB) M-01-24 Memorandum, Reporting Instructions for the Government Information Security Act.

Our review was performed in four phases: (1) Planning; (2) Arranging for the review with OASAM and PeoplePower management and staff; (3) Testing and interviewing; and (4) Report writing.

The planning phase was designed to ensure that team members understood the OASAM's security program as they relate to PeoplePower applications. Arranging the review included contacting OASAM and PeoplePower representatives and agreeing on the timing of detailed survey and testing procedures.

Testing and interviews included: Interviews with key OASAM, CIO, HR and PeoplePower managers and staff; reviews of key reports, tables and related documentation; and security administration policies and practices.

The report-writing phase entailed drafting a compliance report, providing a draft copy to the OIG, CIO and PeoplePower management for review, and preparing and issuing the final report.

## FINDINGS AND RECOMMENDATIONS

The following section describes the findings and recommendations that have been identified during the GISRA Evaluation fieldwork on the OASAM PeoplePower HRMS. Each finding includes a description of the condition, the cause of the condition, the criteria against which the condition was identified (e.g., NIST, GAO, OMB, etc.), the potential effects, and a recommendation to address the condition. Additionally, the related OMB requirement is referenced in order to facilitate the OIG reporting requirement process.

We have identified ten conditions as they relate to the OMB Reporting Requirements. Five of the conditions have been classified as "High Risk Control Issues" and five "Moderate Risk Control Issues."

**High Risk Control Issues:** The identified condition could result in a decline in public confidence in DOL or substantially impair the organization's ability to execute its core business functions (including payroll and benefits functions), or compromise the confidentiality, integrity or availability of system and information resources.

**Medium Risk Control Issues:** The identified condition could result in damage to DOL's reputation, cause a reduction in organizational efficiency or effectiveness, or place at hazard the confidentiality, integrity or availability of system and information resources.

A description of the high and medium risk control issues follows:

**High Risk Control Issues**

**Number of Findings: 5**

References	Finding and Recommendation
<p><b>Finding #1;</b> OMB Reporting Requirement(s) IIB5, IIB6, IIB10</p>	<p><b>Condition:</b> PeoplePower does not follow the DOL Systems Development Life Cycle methodology.</p> <p><b>Cause:</b></p> <ul style="list-style-type: none"> <li>▪ The DOL SDLC and Change Control Board have not been fully implemented.</li> <li>▪ Lack of formalization and integration of Best Practices Implementation policy into systems development.</li> <li>▪ No formal review of system development processes.</li> </ul> <p><b>Criteria:</b> <u>NIST Special Pub 800-14</u>: “Security, like other aspects of an IT system, is best managed if planned for <i>throughout</i> the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/ acquisition, implementation, operation, and disposal.... Organizations should ensure that security activities are accomplished during each of the phases.... From a security point of view, configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications.”</p> <p><b>Effect:</b></p> <ul style="list-style-type: none"> <li>▪ Potential to develop systems with functional and security weaknesses.</li> <li>▪ Potentially higher development and/or management costs due to inefficient systems design, requirement to re-design or modify systems/functionality.</li> </ul> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head:</p> <ul style="list-style-type: none"> <li>▪ Integrate formal SDLC processes into the PeoplePower implementation methodology; increase management oversight of SDLC it at every phase of systems development to ensure all efforts are in compliance with DOL standards.</li> <li>▪ Formalize all Change Control Board documentation.</li> </ul> <p><b>Management Comments:</b> In the first quarter of Fiscal Year (FY) 2002, the People Power team will compare the current life cycle practices for the system to the DOL System Development Life Cycle (SDLC) methodology, identify gaps, and develop an appropriate action plan to conform with the DOL SDLC methodology.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #2;</b> OMB Reporting Requirement(s) IIB5, IIB6, IIB12</p>	<p><b>Condition:</b> PeoplePower has not developed or tested a Formal Disaster Recovery Plan, as highlighted in the Computer Security Handbook.</p> <p><b>Cause:</b></p> <ul style="list-style-type: none"> <li>▪ OASAM has developed, but not implemented, a formal Disaster Recovery Plan.</li> <li>▪ Lack of centralized responsibility to complete and test this plan according to regulations.</li> </ul> <p><b>Criteria:</b> <u>NIST Special Pub 800-14</u>: “Contingency planning directly supports an organization's goal of continued operations. Organizations should practice contingency planning because it makes good business sense.”</p> <p><b>Effect:</b></p> <ul style="list-style-type: none"> <li>▪ Potential for substantial degradation in public service, inability to execute core business processes in the event of an emergency or natural disaster.</li> <li>▪ Potential loss of public confidence in DOL.</li> </ul> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head:</p> <ul style="list-style-type: none"> <li>▪ Integrate the PeoplePower application into the overall OASAM Disaster Recovery Plan.</li> <li>▪ Implement and test a PeoplePower and OASAM disaster recovery plan that takes into account Department and other federal agency plans. Prioritize this plan as critical; schedule formal completion and test dates.</li> <li>▪ OASAM management monitor progress to ensure plan completion and test in accordance with schedule.</li> </ul> <p><b>Management Comments:</b> The People Power team has prepared preliminary plans for disaster recovery. By the end of the second quarter of FY 2002, the People Power team will adjust its disaster recovery plan to comport with OASAM’s strategy, as outlined in the Business Operations Center’s (BOC) agency-level recovery plan and the Information Technology Center’s (ITC) network and communications recovery plans.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #3;</b> OMB Reporting Requirement(s) IIB6, IIB8</p>	<p><b>Condition:</b> PeoplePower does not have a formal Incident Response Plan.</p> <p><b>Cause:</b> OASAM is in the process of developing an updated formal Incident Response Capability. However, at the time of our review, Formal Incident Response Procedures did not exist.</p> <p><b>Criteria:</b> <u>NIST Special Pubs 800-14 and 800-3</u>: “An organization should address computer security incidents by developing an incident handling capability.” “A CSIRC provides computer security efforts with the capability to respond to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities, in an efficient and timely manner. A CSIRC further promotes increased security awareness of computer security-related risks so that agencies are better prepared and protected.”</p> <p><b>Effect:</b> PeoplePower and OASAM management ability to proactively manage system risk substantially reduced.</p> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head develop and implement a formal incident response capability within PeoplePower and OASAM in accordance with NIST Special Pub 800-3 guidance; ensure proper duty separation is maintained to protect the integrity of the incident response capability.</p> <p><b>Management Comments:</b> The Information Technology Center has a formal Incident Response Plan that comports with the Department’s Computer Security Handbook and the plan feeds into the overall Incident Response and Reporting Procedures of the Department. The ITC Incident Response Plan will be used to manage all OASAM systems. OASAM’s Computer Security Officer will train the People Power team on the procedures by November 1, 2001.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable</p>

References	Finding and Recommendation
<p><b>Finding #4;</b> OMB Reporting Requirement(s) IIB5, IIB6</p>	<p><b>Condition:</b> PeoplePower Operational Procedures do not fully implement procedures and controls articulated in the Computer Security Handbook.</p> <p><b>Cause:</b> No measures of performance exist to ensure these controls highlighted in the Computer Security Handbook are incorporated at the application level. Additionally, The Agency lacks implementation of major components articulated in the Computer Security handbook.</p> <p><b>Criteria:</b> <u>NIST Special Pub 800-18</u>: “Organizations should have the following three different types of policy: Program, Issue-Specific, and System Specific. (Some organizations may refer to these types with other names such as directives, procedures, or plans.)... All three types of policy should be...supported by Management. <i>Without management support, the policy will become an empty token of management's "commitment" to security.</i>” [Italics in original]</p> <p><b>Effect:</b> Potential for compromise of systems, applications and information due to inadequate security controls implementation.</p> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head and PeoplePower management conduct an internal review to determine where gaps exist between policies and procedural implementation. Develop a plan to mitigate risks and close gaps.</p> <p><b>Management Comments:</b> The People Power team will conduct an internal review to compare current procedures and controls with the Computer Security Handbook to determine where gaps exist between policies and procedural implementation. A plan of action will be developed to mitigate risks and close the gaps by the end of FY 2002.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #5;</b> OMB Reporting Requirement(s) IIB5, IIB6</p>	<p><b>Condition:</b> PeoplePower has not been formally certified or accredited.</p> <p><b>Cause:</b> Formal Accreditation Procedures are not being followed in the Proprietary Implementation Methodology. Additionally, OASAM has not developed formal Certification and Accreditation Procedures.</p> <p><b>Criteria:</b> <u>NIST Special Pub 800-18</u>: “During implementation, the system is tested and installed or fielded. The following items should be considered during this phase:...” Security Testing. System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system.... Accreditation. System security accreditation is the formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk.</p> <p><b>Effect:</b></p> <ul style="list-style-type: none"> <li>▪ OASAM management has not formally accepted information security risk.</li> <li>▪ Risk assessments have focused on the project financial risk, but not on application security risk.</li> </ul> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head:</p> <ul style="list-style-type: none"> <li>▪ Develop and implement FIPS-102 based standard procedures for conducting certification and accreditation on all future system/application implementations.</li> <li>▪ Conduct accreditation and certification on existing PeoplePower applications in accordance established procedures.</li> <li>▪ Formally designate appropriate qualified DOL personnel to serve in Certification Authority (CA) and Designated Approval Authority (DAA) roles.</li> </ul> <p><b>Management Comments:</b> In accordance with the Department of Labor Manual Series Chapter 9, Information Technology, the People Power team will promptly obtain interim approval to operate for the Assistant Secretary for Administration and Management. Once formal certification and accreditation procedures are issued by the Office of the Chief Information Officer (OCIO), the People Power team will complete the process with due diligence.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions.</p>

**Medium Risk Control Issues**

**Number of Findings: 5**

References	Finding and Recommendation
<p><b>Finding #6;</b> OMB Reporting Requirement(s) IIB5, IIB6</p>	<p><b>Condition:</b></p> <p>While PeoplePower users are required to sign People-Power system-level rules of behavior, there are no corresponding network rules of behavior.</p> <p><b>Cause:</b></p> <ul style="list-style-type: none"> <li>▪ Inadequate management controls.</li> <li>▪ Lack of procedure and ownership of this duty- enforcement.</li> </ul> <p><b>Criteria:</b></p> <p><u>NIST Special Pubs 800-14 and 800-18</u>: “A set of rules of behavior must be established for each system.”</p> <p>“The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries.”</p> <p><b>Effect:</b></p> <p>Users may misuse the network for personal or inappropriate access.</p> <p><b>Recommended Corrective Action:</b></p> <p>We recommend that the Agency Head:</p> <ul style="list-style-type: none"> <li>▪ Require all current employees to sign a formal Rules of Behavior document; maintain signed copies in individual’s personnel records.</li> <li>▪ Require all current contract workers to sign a formal Rules of Behavior document; maintain signed copies with the COTR.</li> <li>▪ Ensure all new employees and contractors sign a formal Rules of Behavior document; maintain signed copies as recommended above.</li> </ul> <p><b>Management Comments:</b></p> <p>The Department’s Appropriate Use Policy is the overarching guidance in this area and applies to all employees and DOL contractors. In addition, the People Power team has addressed the rules of behavior, especially as it pertains to security and the privacy of the People Power system. All users, whether Department of Labor employees or contractors, must sign this agreement before any access is given. Absence further guidance fro the OIG, we consider this finding resolved.</p> <p><b>Conclusion:</b></p> <p>The PeoplePower users have signed an agreement for use of the application, however, the PeoplePower management has not ensured that users are appropriately aware and understand the rules of behavior associated with using the network which supports the PeoplePower application. The OIG does not consider this resolved. Resolution is dependent upon PeoplePower management working with OASAM to ensure all PeoplePower users are appropriately aware of the Appropriate Use policy.</p>

References	Finding and Recommendation
<p><b>Finding #7;</b> OMB Reporting Requirement(s) IIB5, IIB6</p>	<p><b>Condition:</b> PeoplePower user and contractor access rights are not reviewed annually to determine if system access is commensurate with job responsibilities.</p> <p><b>Cause:</b> Inadequate management, HR controls.</p> <p><b>Criteria:</b> <u>NIST Special Pub 800-18</u>: “Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. The following should be considered:  User Account Management. Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.  Audit and Management Reviews. It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.”</p> <p><b>Effect:</b></p> <ul style="list-style-type: none"> <li>▪ Potential for ‘access creep’ as employees are promoted or change jobs within OASAM/DOL.</li> <li>▪ Potential disclosure of sensitive information by contractor personnel.</li> </ul> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head develop and implement formal standard procedures for:</p> <ul style="list-style-type: none"> <li>▪ Granting contractor access.</li> <li>▪ Annual user account and access rights review and revalidation.</li> <li>▪ Terminating employees under friendly and hostile circumstances.</li> </ul> <p><b>Management Comments:</b> The People Power team is currently implementing a software solution that automates the provisioning of user accounts through the use of a workflow-based engine. Access360 Inc., manufactures the software solution called “enRole.” This tool will facilitate access management and aid in annual reviews of every type of user account for the People Power system. It is scheduled to be on-line at the end of CY 2001 phasing the implementation into the beginning of CY 2002.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #8;</b> OMB Reporting Requirement(s) IIB5, IIB6, IIB11</p>	<p><b>Condition:</b> An application controls review has not been performed on PeoplePower applications.</p> <p><b>Cause:</b> No formal methodology was used to review PeoplePower application.</p> <p><b>Criteria:</b> <u>NIST Special Pubs 800-18 and 800-12</u>: “Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management requires the analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action. Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one.”</p> <p><b>Effect:</b> Lacking a clear understanding of application-level information assurance risks OASAM and PeoplePower managers are less able to accurately gauge and proactively manage the risk to PeoplePower using cost-effective controls.</p> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head perform an applications control review in accordance with NIST, DOL, and GAO guidance.</p> <p><b>Management Comments:</b> Consistent with DOL practice, the People Power team will complete an application controls review in accordance with the National Institute of Standards and Technology Special Publication 800, and General Accounting Office’s Federal Information System Audit Control Manual. The controls review will be completed by the end of the second quarter of FY 2002.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #9;</b> OMB Reporting Requirement(s) IIB5, IIB6, IIB11</p>	<p><b>Condition:</b> PeoplePower audits, program reviews and security reviews do not follow a consistent methodology or employ the same measures of performance.</p> <p><b>Cause:</b> OASAM audits, program reviews and security reviews do not follow a consistent methodology or employ the same measures of performance.</p> <p><b>Criteria:</b> <u>NIST Special Pubs 800-18 and 800-12</u>: Risk assessment must produce a meaningful output that reflects what is truly important to the organization. The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls.” “How the boundary, scope, and [risk assessment] methodology are defined will have major consequences in terms of (1) the total amount of effort spent on risk management and (2) the type and usefulness of the assessment's results.</p> <p><b>Effect:</b> Although OASAM has had a number of audits and reviews performed within the last three years, several different methodologies have been used. Lacking a clear methodology yields an inconsistent result, making it more difficult for OASAM and PeoplePower managers to accurately gauge and proactively manage the risk to PeoplePower using cost-effective controls.</p> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head develop a regular schedule of systems and applications risk/controls reviews that will yield a consistent result, enabling more effective risk management and problem tracking.</p> <p><b>Management Comments:</b> The People Power team will participate in the structured in-progress quarterly review process managed by the Office of the Chief Information Officer for any development, modernization, or enhancement activities. Additionally, a post implementation review will be completed by the Department’s Technical Review Board using the Department’s Post Implementation Review Methodology for the People Power releases already in production. The Post implementation reviews will be completed by the end of April 2002.</p> <p><b>Conclusion:</b> The actions planned by People Power management are responsive to the issue identified and, when fully implemented, should satisfy the intent of the recommended corrective actions. Additionally, the target dates provided for the actions appear reasonable.</p>

References	Finding and Recommendation
<p><b>Finding #10;</b> OMB Reporting Requirement(s) IIB5, IIB6</p>	<p><b>Condition:</b> PeoplePower does not have formalized termination procedures for employees (LAN access, etc)</p> <p><b>Cause:</b> Inadequate management, HR controls.</p> <p><b>Criteria:</b> <u>NIST Special Pub 800-18</u>: “Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. The following should be considered:  Friendly Termination. <i>Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing or transferring employees.</i>  Unfriendly Termination. <i>Given the potential for adverse consequences, organizations should do the following:</i></p> <ul style="list-style-type: none"> <li>▪ System access should be terminated as quickly as possible when an employee is leaving a position under less than friendly terms. If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.</li> <li>▪ When an employee notifies an organization of a resignation and it can be reasonably expected that it be on unfriendly terms, system access should be immediately terminated.</li> <li>▪ During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.</li> <li>▪ In some cases, physical removal from the offices may be necessary.”</li> </ul> <p><b>Effect:</b></p> <ul style="list-style-type: none"> <li>▪ Potential for adverse actions by disgruntled employees.</li> <li>▪ Potential for adverse actions by employees terminated for cause.</li> <li>▪ Potential for lost data through premature deletion of former employee’s accounts.</li> </ul> <p><b>Recommended Corrective Action:</b> We recommend that the Agency Head develop and implement formal standard procedures for terminating employees under friendly and hostile circumstances.</p> <p><b>Management Comments:</b> The Department uses a distributed model for handling information within the People Power system. There are fourteen (14) Personnel Offices that process across eight (8) major LAN networks run by the major agencies of the Department. Therefore, access to these LANs is the responsibility of the agencies which operate them. The agencies are also required to notify appropriate authorities of any terminations or dismissals.  As has been done in the past, a memorandum will be issued to remind agencies of their responsibility to notify appropriate authorities through current implemented procedures.</p> <p><b>Conclusion:</b> The action planned by People Power management is responsive to the issue identified, however OASAM should investigate other means to ensure communication of timely</p>

	and sensitive issues/information within the department.
--	---

## ACRONYMS

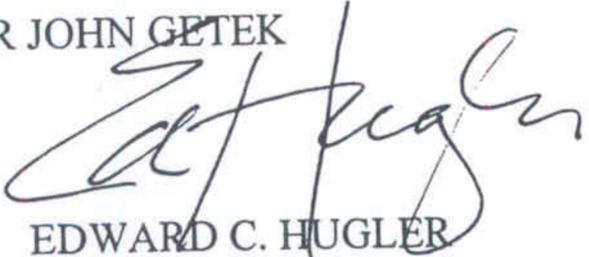
CA	Certification Authority
COTR	Contracting Officer's Technical Representative
CSIRC	Computer Security Incident Response Capability
DAA	Designated Approval Authority
DOL	Department of Labor
ECN	Employee Computer Network
FIPS PUB	Federal Information Processing Standards Publication
FISCAM	Federal Information System Controls Audit Manual
FPB	Frances Perkins Building
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSS	General Support System
HR	Human Resources
HRMS	Human Resource Management System
IRM	Information Resource Management
IT	Information Technology
ITMRA	Information Technology Management Reform Act
LAN	Local Area Network
MA	Major Application
NIST	National Institute of Standards and Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management Budget
PAR	Personnel Action Request
SDLC	Systems Development and Life Cycle



SEP 28 2001

MEMORANDUM FOR JOHN GETEK

FROM:

  
EDWARD C. HUGLER  
Deputy Assistant Secretary for Operations  
Administration and Management

SUBJECT:

Reply to Draft Audit Report No. 23-01-013-07-001;  
Government Information Security Reform Act (GISRA)  
Evaluation of People Power System.

The following responds to the findings in the Draft Audit Report. The positive general observations about the GISRA Evaluation of the People Power system are appreciated as this gives overall context to the report's findings.

The Draft Report also observes that the People Power system does not exist in isolation from the OASAM/DOL IT environment. The Draft Report highlights areas where closer coordination can be achieved within OASAM components to assure an integrated approach in handling security control issues.

### **High Priority Control Issues**

#### **Finding # 1- People Power does not follow the DOL System Development Life Cycle methodology.**

In the first quarter of Fiscal Year (FY) 2002, the People Power team will compare the current life cycle practices for the system to the DOL System Development Life Cycle (SDLC) methodology, identify any gaps, and develop an appropriate action plan to conform with the DOL SDLC methodology.

By way of background, the People Power system is based on PeopleSoft's Human Resource Management System, which is a Commercial-of-the-Shelf (COTS) System. The DOL People Power team followed a best practice-based implementation methodology that pre-dated the development and issuance of DOL's SDLC methodology. PeopleSoft provided the Department with two major releases of its current production version of the People Power software based on this methodology.

The People Power team developed its implementation methodology tailored to the life cycle of a large COTS-based system, developed with the help of its tier-one implementation partner, Price WaterHouse Coopers (PWC).

**Finding #2 – People Power has not developed or tested a Formal Disaster Recovery Plan, as highlighted in the Computer Security Handbook.**

The People Power team has prepared preliminary plans for disaster recovery. By the end of the second quarter of FY 2002, the People Power team will adjust its disaster recovery plan to comport with OASAM's strategy, as outlined in the Business Operations Center's (BOC) agency-level recovery plan and the Information Technology Center's (ITC) network and communications recovery plans.

**Finding #3 – People Power does not have a formal Incident Response Plan.**

The People Power team maintains system logs, and in accordance with the Department's Security Handbook, reviews these system logs and compares them to trends on a periodic basis. When unusual or suspicious activity is detected, the People Power team immediately notifies the OASAM Computer Security Officer.

OASAM's Computer Security Officer resides within the ITC, which has a formal Incident Response Plan that comports with the Department's Computer Security Handbook, and the plan feeds into the overall Incident Response and Reporting Procedures of the Department that is managed by the Office of the Chief Information Officer. The ITC's Incident Response and Reporting procedures will be used to manage all cyber-based incidents affecting OASAM systems. All system owner's in OASAM have received instructions on how to report any unusual activity or incidents to OASAM's Computer Security Officer for follow-on action. OASAM's Computer Security Officer will train the People Power team on the overall Incident Response and Reporting procedures by November 1, 2001. Absent further guidance from the OIG, we consider this finding resolved.

**Finding #4 – People Power Operational Procedures do not fully implement procedures and controls articulated in the Computer Security Handbook.**

The People Power Team has a Change Control Board (CCB) and documented procedures within its System Security Plan. The People Power CCB actively reviews and grants changes/modifications to the system. The CCB is made up of senior People Power team

members representing cross-functional disciplines. While the CCB provides a good vehicle for making these types of decisions, the People Power team does not follow consistent procedures for making changes to the system or consistent procedures for validating them in accordance with DOL Policies. The People Power team will conduct an internal review to compare current procedures and controls with the Computer Security Handbook to determine where gaps exist between policies and procedural implementation. A plan of action will be developed to mitigate risks and close the gaps by the end of FY 2002.

**Finding #5 – People Power has not been formally certified or accredited.**

In accordance with the Department of Labor Manual Series Chapter 9, Information Technology, the People Power team will promptly obtain interim approval to operate from the Office of Assistant Secretary for Administration and Management. Once formal certification and accreditation procedures are issued by the Office of the Chief Information Officer (OCIO), the People Power team will complete that process with due diligence.

**Medium Priority Control Issues**

**Finding #6 – While People Power users are required to sign People Power system-level rules of behavior, there are no corresponding network rules of behavior.**

The Department's Appropriate Use Policy is the overarching guidance in this area and applies to all employees and DOL contractors. In addition, the People Power team has addressed the rules of behavior, especially as it pertains to security and the privacy of the People Power system. All users, whether Department of Labor employees or contractors, must sign this agreement before any access is given. Absence further guidance from the OIG, we consider this finding resolved.

**Finding #7 - People Power user and contractor access rights are not reviewed annually to determine if system access is commensurate with job responsibilities.**

The People Power team is currently implementing a software solution that automates the provisioning of user accounts through the use of a workflow-based engine. Access360, Inc. manufactures the software solution called "enRole". This tool will facilitate access management and aid in annual reviews of every type of user account for the People

Power system. It is scheduled to be on-line at the end of CY 2001 phasing the implementation into the beginning CY 2002.

Within this implementation effort, the People Power team is working with other components of OASAM, including the Human Resource Center (HRC), to develop formal standard procedures for the People Power system to grant access to contractors and to terminate accounts of separating employees. This effort will be completed by the end of the third quarter of FY 2002.

**Finding #8 – An application controls review has not been performed on People Power application.**

In early CY 2001, the People Power team went through a Facilitated Risk Analysis Process (FRAP™) session. The FRAP session offered a formal methodology, facilitated by skilled security professionals, focused on specific People Power assets to aid in reducing or eliminating operational inefficiencies, and relied on the client's subject matter experts.

Consistent with DOL practice, the People Power team will complete an application controls review in accordance with the National Institute of Standards and Technology's Special Publication 800, and the General Accounting Office's Federal Information System Control Audit Manual. The controls review will be completed by the end of the second quarter of FY 2002.

**Finding #9 - People Power audits, program reviews, and security reviews do not follow a consistent methodology or employ the same measure of performance.**

The People Power team will participate in the structured in-progress quarterly review process managed by the Office of the Chief Information Officer for any development, modernization, or enhancement activities. Additionally, a post implementation review will be completed by the Department's Technical Review Board using the Department's Post Implementation Review Methodology for the People Power releases already in production. The post implementation reviews will be completed by the end of April 2002.

**Finding #10 - People Power does not have formalized termination procedures for**

**employees (LAN Access).**

The Department uses a distributed processing model for handling information within the People Power system. There are fourteen (14) Personnel Offices that process across eight (8) major LAN networks run by the major agencies of the Department. Therefore, access to these LANs is the responsibility of the agencies which operate them. The agencies are also required to notify appropriate authorities of any terminations or dismissals.

As has been done in the past, a memorandum will be issued to remind agencies of their responsibility to notify appropriate authorities through current implemented procedures.

cc: Pizzella, P  
Stepp, T  
Delaney, T