



U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

September 30, 2005

MEMORANDUM FOR GAIL T. LOVELACE
CHIEF PEOPLE OFFICER (C)

FROM: GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

SUBJECT: STRATEGIC CHALLENGES FOR GSA'S
COMPREHENSIVE HUMAN RESOURCES
INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

The attached subject audit report presents the results of our review of GSA's human resources system--CHRIS. We met with you and your staff on August 25, 2005 to discuss our assessment of the managerial, operational, and technical controls for CHRIS and we also held a follow-up telephone conference on September 7, 2005 with your staff to obtain input on the draft report. Generally, you have concurred with our findings and recommendations for improving CHRIS, and have noted improvement actions underway. This report includes a Management Response section, which summarizes your written comments to the draft report and a copy of the comments you've provided is included in Appendix B.

In accordance with GSA Order ADM P 2030.2C, a time-phased action plan to specifically address the report recommendations and the Management Decision Record is required within 60 days of the report date. The time-phased action plan and completed Section B of the Management Decision Record should be submitted to the Assistant Inspector General for Auditing (JA), with a copy to the Audit Follow-up and Evaluation Branch (BECA).

It is important that the final actions and all management decisions responding to the report be completed within 12 months of the audit report issue date. Otherwise, the Office of Inspector General must identify in its Semiannual Report to Congress the matters on which final actions have not been completed within this timeframe. As such, to the maximum extent possible, your time-phased action plan should schedule actions to be completed within 12 months of the report issue date. To help us improve our customer service, we have attached a Customer Satisfaction Survey developed to obtain feedback regarding how the report and related audit services meet customer expectations. We request that the primary user of this report complete the questionnaire and return it to the Director, Audit Operations Staff (JAO) in the envelope provided. I appreciate the courtesies and assistance provided by you and your staff during our review. Should you have any questions, or if you would like to discuss any aspect of the report in greater detail, please contact me or Donna Peterson-Jones, Audit Manager, on (703) 308-1223.

Attachments

241 18th Street S., CS4, Suite 607, Arlington, VA 22202-3402

Federal Recycling Program



Printed on Recycled Paper

Audit Report

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

September 30, 2005

**Office of Inspector General
General Services Administration**



Office of Audits



U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 30, 2005

Reply to: Deputy Assistant Inspector General for
Attn of: Information Technology Audits (JA-T)

To: Gail T. Lovelace
Chief People Officer (C)

Subject: Strategic Challenges for GSA's Comprehensive
Human Resources Integrated System (CHRIS)
Report Number A040142/O/T/F05025

This report presents the results of our review of the Comprehensive Human Resources Integrated System (CHRIS). CHRIS is the General Services Administration's (GSA) web-based Human Resources (HR) system, which is based on the Oracle Federal HR commercial-off-the-shelf product and customized to support a range of HR and reporting functions intended to meet the needs of GSA and its customers.

Our review of CHRIS found that the original intent for CHRIS to provide a comprehensive, integrated HR system, GSA's strategic efforts with the system have been impeded by user reluctance to use the system and the availability of duplicative system functionality provided by other GSA systems. A post-implementation review to fully assess how well the system is meeting all user requirements has not yet been completed and with a changing environment driven by the Human Resources Information System (HRIS) component of e-Government, GSA has faced challenges in marketing CHRIS to new customers. Due to an insufficient customer base, CHRIS is not recovering costs or the revenue originally expected. With ongoing decisions regarding the selection of HR Line of Business systems, GSA faces critical management decisions regarding the future of CHRIS. Several areas of system security risk that could lead to system vulnerabilities or unnecessary risk were also identified through our annual review as part of our responsibilities under the Federal Information Security Management Act. Key security components for CHRIS had not been fully addressed including a final certification and accreditation of system controls and completion of required security documents. We also identified specific technical control vulnerabilities for the CHRIS Oracle database that, if exploited, could compromise the confidentiality, integrity, and availability of the system. Management attention aimed at improving managerial, operational, and technical controls is needed to ensure success with this important system. Written comments provided by your office have been included in their entirety in Appendix B.

I wish to express my appreciation to all of your staff and other persons who cooperated during the audit. If you have any questions, please contact me or Gwendolyn McGowan, the Deputy Assistant Inspector General for Information Technology Audits, on 703-308-1223.


Donna P. Peterson-Jones

Audit Manager
Information Technology Audit Office (JA-T)

241 18th Street S., CS4, Suite 607, Arlington, VA 22202-3402

Federal Recycling Program



Printed on Recycled Paper

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

TABLE OF CONTENTS

	<u>PAGE</u>
EXECUTIVE SUMMARY	i
Purpose	i
Background.....	i
Results-in-Brief	i
Recommendations	ii
Management Response	iii
INTRODUCTION	1
Objectives, Scope, and Methodology	1
RESULTS OF AUDIT.....	3
Some System Requirements May Not Be Fully Realized with CHRIS	3
Expected Benefits Not Realized for CHRIS Due to Insufficient Customer Base	5
Improved System Security Controls Needed	8
Key Components of Security Have Not Been Addressed with Certification and Accreditation of System Controls	8
Background Checks for Contractors Not Completed	9
Improvements Needed in Oracle Database Security.....	9
Recommendations	10
Management Response	11
Internal Controls	11

APPENDICES

KEY EVENTS IN CHRIS LIFECYCLEA-1
GSA CPO's RESPONSE TO DRAFT AUDIT REPORTB-1
REPORT DISTRIBUTIONC-1

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

EXECUTIVE SUMMARY

Purpose

The General Services Administration's (GSA) Comprehensive Human Resources Integrated System (CHRIS) is a web-based Human Resources (HR) Information Technology (IT) system based on the Oracle Federal HR commercial-off-the-shelf product and customized to support a range of HR and reporting functions intended to meet the needs of GSA and its customers. Our overall audit objectives were to determine whether: (1) GSA's CHRIS provides the needed functionality, security, and other controls for system operations to ensure the data's integrity and reliability; (2) the Office of the Chief People Officer (OCPO) has processes in place to improve system functionality and usability; and (3) CHRIS is financially beneficial to GSA. If not, what actions are needed to improve CHRIS?

Background

The CHRIS solution was first deployed through a client-server environment in August 2000 to provide HR systems support to GSA employees and approximately 8,600 external customers from the National Archives and Records Administration, the Equal Employment Opportunity Commission, the National Credit Union Administration, and Presidential Boards and Commissions that were previously supported by the legacy Personnel Information Resources System. While GSA's OCPO had the immediate requirement to service its own employees and existing customers with CHRIS, the growth of cross-servicing revenues became part of the organization's mission. In December 2001, the OCPO implemented new technology to provide web-based access to the CHRIS system over GSA's network. In September 2004 the OCPO provided all GSA employees with web-based electronic access to their own personal information within CHRIS. A timeline of key events relating to CHRIS is provided in Appendix A-1.

Results-in-Brief

CHRIS was deployed by the OCPO to provide important online capabilities and improve GSA and other Federal organizations' processes for human resources. Though the original intent for CHRIS was to provide a comprehensive, integrated HR system, GSA's strategic efforts with the system have been impeded by user reluctance to use the system and the availability of duplicative system functionality provided by other GSA systems. Since the system was introduced in August 2000 a post-implementation review to fully assess how well the system is meeting user requirements has not been completed. As a result, some requirements for the HR system such as those established by the Joint Financial Management Improvement Program may not be adequately supported with CHRIS. With a changing environment driven by the Human Resources Information System (HRIS) component of e-Government, GSA has also faced challenges in marketing CHRIS. Due to an insufficient customer base, CHRIS is not recovering costs or the revenue originally expected. System lifecycle costs have increased from an initial estimate of \$34 million to an estimated \$54

million without a projected quantifiable recovery of investment. With ongoing decisions regarding the selection of HR Line of Business systems, GSA must make critical management decisions regarding the future of CHRIS, including whether to: (1) retain the system and expand the customer base to offset costs; (2) offer CHRIS as a service provider under HRIS; or (3) sell CHRIS and discontinue GSA's management role with the system. Several areas of system security risk that could lead to system vulnerabilities or unnecessary risk were assessed through our FY 2004 review of GSA's IT Security Program required by the Federal Information Security Management Act. Key security components for CHRIS have not been fully addressed including the certification and accreditation of system controls and completion of required security documents. Background checks for contractors with access to CHRIS are also needed. During our review we also identified technical control vulnerabilities for the CHRIS Oracle database that, if exploited, may compromise the confidentiality, integrity, and availability of the system¹. Specific steps taken at this critical juncture could better ensure that GSA's strategic business objectives and all user needs are met with the CHRIS system.

Recommendations

We recommend that the GSA Chief People Officer:

- (1) Conduct a post-implementation review in accordance with the Office of Management and Budget's Circular A-130 and GSA's August 2002 IT Capital Planning And Investment Guide, to:
 - a. Validate estimated benefits and costs for CHRIS;
 - b. Evaluate CHRIS to ensure positive return on investment; and
 - c. Ensure that the system meets organizational and user needs.
- (2) Complete an alternatives analysis to fully consider the costs and benefits for the options of:
 - a. Keeping the system and expanding the customer base to offset costs; or
 - b. Offering CHRIS as a service provider under HRIS; or
 - c. Selling the system and discontinuing GSA's management role with CHRIS.
- (3) Ensure that adequate security controls are in place to manage risks with CHRIS by:
 - a. Completing the system certification and accreditation process for CHRIS including updating required system security documentation.
 - b. Prioritizing necessary background checks for contractor staff as required by the GSA IT Security Policy and implementing compensating controls until this process is completed.
 - c. Carefully assessing the Oracle database vulnerabilities and applying technical solutions to reduce associated risks.

¹ Specific results for our review of the CHRIS Oracle database were provided separately to the OCPO on July 20, 2005, due to the sensitive nature of the information reported.

Management Response

We met with the Chief People Officer (CPO) and Office of the Chief People Officer (OCPO) personnel to discuss the results of our review and to identify any areas in the draft report that may require revisions. They generally concurred with the findings and two of the three recommendations as presented in the report. Written comments provided by the CPO indicate that OCPO will take actions aimed at addressing the identified areas of risk in the report. Specifically, they identified ongoing or planned management actions toward: (1) conducting a formal post-implementation review for CHRIS to better assess whether the system effectively and efficiently meets user needs as well as JFMIP and HR system requirements, and (2) continuing to enhance CHRIS security controls including another system certification and accreditation and completing background checks on contractors.

The CPO did not agree with the recommendation to complete an alternatives analysis to fully consider the costs and benefits for the options of: (1) keeping the system and expanding the customer base to offset costs; or (2) offering CHRIS as a service provider under HRIS; or (3) selling the system and discontinuing GSA's management role with CHRIS. The CPO stated "an analysis was completed in 2003 and in 2005 the Office of the CPO and the Office of the Chief Financial Officer (CFO) decided that it would be in GSA's best interest to offer CHRIS and the Payroll Accounting Reporting (PAR) system, in combination, as the core of an HR Line of Business (LoB) Shared Service Center solution. A business case (OMB Exhibit 300) was submitted to OMB earlier this month as part of the FY 2007 budget formulation process. The offices of the CPO and CFO will work together to develop a more complete business model to support this plan." While the decision to continue CHRIS as a service provider under HRIS is an option that we recommended be considered, a more complete business model should clarify how alternatives were considered.

A copy of the management comments is provided in its entirety in Appendix B.

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

INTRODUCTION

The Comprehensive Human Resources Integrated System (CHRIS), a tool used by the General Services Administration (GSA) and its customer agencies to administer the careers of their Federal employees, provides a range of Human Resources (HR) services and information. The CHRIS system was based on the Oracle Federal HR commercial-off-the-shelf database product and the system has been customized for GSA and other Federal agency customers' use. CHRIS was first deployed to HR offices through a client-server environment in August 2000. In December 2001, the Office of the Chief People Officer implemented new technology to provide browser-based access over GSA's network by bringing the application to the users' desktops. A timeline of key events relating to CHRIS is provided in Appendix A-1.

Objectives, Scope, and Methodology

Our overall audit objectives were to determine whether: (1) GSA's CHRIS provides the needed functionality, security, and other controls for system operations to ensure the data's integrity and reliability; (2) the Office of the Chief People Officer (OCPO) has processes in place to improve system functionality and usability; and (3) CHRIS is financially beneficial to GSA. If not, what actions are needed to improve CHRIS? Our review focused on CHRIS project management, system and user requirements, security, system controls, and interfaces. We analyzed key documentation, including the Security Plan, Contingency Plan, Configuration Management Plan, User Manual, data dictionary, and documentation for interfaces, certification and accreditation, and security testing and evaluation. We also assessed the original 1999 business plan for CHRIS, the 2001 Gartner, Inc. pricing study, the 2001 Chief People Officer Technology Initiative, the 2003 International Business Machines study of strategic alternatives for CHRIS, pilot efforts for additional CHRIS modules; existing and planned system functionality; reconciliation of CHRIS' costs with Pegasys, GSA's financial system of record; and GSA operations as well as agreements with other Federal agencies for their use of CHRIS. We met with key officials in the OCPO, including the OCPO's Chief Information Officer (CIO), system administrators, and security officials. We interviewed system users in the National Capital Region, the Mid-Atlantic Region (Region 3), the Office of Inspector General Human Resources Offices, the Agency Liaison Division in the National Capital Region, and the OCPO's Consolidated Processing Center in GSA's Heartland Region (Region 6). CHRIS was concurrently reviewed and incorporated in the Fiscal Year (FY) 2004 review of GSA's Information Technology (IT) Security Program required by the Federal Information Security Management Act (FISMA). During the timeframes of this audit our office issued two separate reports on CHRIS security, with detailed results for our FISMA technical control tests for CHRIS: FY 2004 Office of Inspector General Information Security Review of the Comprehensive Human Resources Integrated System, Report Number A040179/O/T/F05006, dated January 11, 2005, and Security Vulnerabilities with the Comprehensive Human Resources Integrated System (CHRIS) Oracle Database, Report Number A040142/O/T/F05021 dated July 20, 2005.

We considered applicable regulations, policies, and guidance for HR systems, including: the GSA Information Technology Security Policy, CIO P 2100.1B, November 2004; Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003; Changes in GSA Organization, ADM 5440.577, December 5, 2003; the GSA Privacy Act Program, CPO 1878.1, October 27, 2003; Conducting Privacy Impact Assessments in GSA, CPO 1878.2, May 28, 2004; the GSA CIO's Capital Planning and IT Investment Guide, February 2000; the GSA CIO's Order on GSA Information Technology (IT) Capital Planning and Investment Control, CIO 2135.1, June 11, 2002; the GSA CIO's IT Capital Planning & Investment Control Guide, August 2002; the Systems Development Life Cycle Policy Handbook, CIO P 2140.2, April 20, 2004; the GSA Office of the Chief People Officer's Human Capital Strategic Plan (2002-2007); the Chief Human Capital Officers Act of 2002; the Federal Information Security Management Act of 2002; the Office of Management and Budget (OMB) Circular A-130 with its Appendices III and IV, Revised November 30, 2000; OMB Circular A-127, revised July 23, 1993; the Joint Financial Management Improvement Program's (JFMIP's) Human Resources and Payroll Systems Requirements, JFMIP SR-99-5, April 1999; the General Accounting Office's (GAO's)² Human Resources and Payroll Systems Requirements: Checklist for Reviewing Systems Under the Federal Financial Management Improvement Act, GAO/AIMD-00-21.2.3, March 2000; GAO's Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999; the National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998; NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, Revised June 2004; NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, January 2002; NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002; and the GSA CIO's IT procedural guides on certification and accreditation, security test and evaluation, contingency and configuration management plans, risk assessments, access control, password generation and protection, and security incident handling.

We performed our audit work in GSA's Central Office, the National Capital Region, the Mid-Atlantic Region (Region 3), and the Heartland Region (Region 6) between February 2004 and January 2005 in accordance with generally accepted government auditing standards.

² Effective July 7, 2004, the GAO's legal name was changed to the Government Accountability Office.

RESULTS OF AUDIT

The Comprehensive Human Resources Integrated System (CHRIS) was deployed by the Office of the Chief People Officer (OCPO) to provide important online capabilities and improve human resources (HR) processes for the General Services Administration (GSA) and its Federal agency customers; however, current costs and benefits for the system need to be carefully considered given the changing environment for Federal HR systems. Though the original intent for CHRIS was to provide a comprehensive, integrated HR system, GSA's strategic efforts with the system have been impeded by user reluctance to use the system and duplicative system functionality provided by other GSA systems. Some requirements for the HR system such as those established by the Joint Financial Management Improvement Program (JFMIP) may not be fully realized with CHRIS and since the system was introduced in August 2000 a post-implementation review to determine how well the system is meeting user requirements has not been completed. With a changing environment driven by the Human Resources Information System (HRIS) component of e-Government, GSA has faced challenges in marketing CHRIS. The system currently has an insufficient customer base and is not recovering costs or the revenue originally expected. CHRIS system lifecycle costs have also increased from an initial estimate of \$34 million to an estimated \$54 million through Fiscal Year (FY) 2006 without projecting a quantifiable recovery of investment. With ongoing decisions regarding the selection of HR Line of Business systems, GSA faces critical decisions including whether to: (1) retain the system and expand the customer base to offset costs; (2) offer CHRIS as a service provider under HRIS; or (3) sell CHRIS and discontinue GSA's management role with the system. Several areas of system security risk that could lead to system vulnerabilities or unnecessary risk were assessed through our FY 2004 Federal Information Security Management Act (FISMA) audit and actions are needed to ensure that adequate system controls are in place and operating as intended. Key security components for CHRIS have not been fully addressed including the certification and accreditation of system controls and completion of required security documents. Background checks for contractors with access to CHRIS are also needed. During our review we identified specific technical control vulnerabilities for the CHRIS Oracle database that, if exploited, may compromise the confidentiality, integrity, and availability of the system³. Taking steps to improve managerial, operational, and technical controls at this critical juncture will better ensure that GSA's strategic business objectives and all user needs are met with the CHRIS system.

Some System Requirements May Not Be Fully Realized with CHRIS

Although CHRIS development staff is currently making strides by improving system functionality and usability and improving communication with its customers, the original intent of providing a comprehensive HR solution with CHRIS that would support and empower GSA's HR professionals, managers, and employees has not been fully realized. CHRIS has encountered user dissatisfaction and system redundancy challenges, and some benchmark system requirements established by JFMIP⁴ may not be met with CHRIS. Further, a post-

³ Specific results for our review of the CHRIS Oracle database were provided separately to the OCPO on July 20, 2005, due to the sensitive nature of the information reported.

⁴ JFMIP's Human Resources and Payroll Systems Requirements, JFMIP SR-99-5, April 1999.

implementation review has not been performed for CHRIS to ensure that it meets all GSA, external customer, and other requirements⁵ for Federal HR systems.

While GSA was still using the legacy Personnel Information Resources System, the OCPO consolidated its HR-related activities to the Consolidated Processing Center (CPC) in Kansas City. The CHRIS Division Director stated that over the years, there has been a reluctance of the user community to fully utilize CHRIS and to provide adequate requirements to the system development staff, specifically around screen layouts and business process definition. The Oracle Federal HR solution, a commercial-off-the-shelf product that serves as the foundation for the CHRIS application, was not stable or well suited for the GSA user community as delivered. CHRIS was originally designed to meet the needs of regional HR offices in a distributed environment and was deployed with interim reports and a cumbersome user interface. As a result, CHRIS was initially met with dissatisfaction from the user community. Additionally, a dichotomy resulted since the intent of GSA's technical direction with CHRIS was to facilitate local transaction processing while the procedural direction was to perform HR transactions centrally with the CPC. However, the technical and procedural direction did not meet the needs of all the regions. As a result, we found that at least one regional office developed Lotus Notes applications to provide reports, communicate employee change requests to the CPC, and create new employee positions, in some cases bypassing HR functionality provided by CHRIS and supplementing the system with alternative Lotus Notes solutions. While CHRIS has the technical capability to be a comprehensive integrated human resources system, the system's functional capabilities are duplicated in other GSA systems. Further, some modules that provide specific HR functionality have not been implemented for CHRIS since the functionality exists in other GSA systems, including the Electronic Time and Attendance Management System, GSAJOBS, Thrift Savings Plan, and Employee Express.

To assess CHRIS capabilities in the area of system requirements, we relied on a checklist developed by the Government Accountability Office for reviewing specific benchmarks established by JFMIP. The checklist describes sets of functionality necessary to support enterprise-wide lines of business and to reduce redundancy and increase effectiveness and efficiency. We used this checklist as a guide, but did not apply it to the GSA's entire human resources system nor did we determine whether CHRIS substantially complies with all requirements for human resources systems. Our analysis found that some system requirements have been met with the system and others have not been fully met. JFMIP requirements stress the importance of electronic personnel files to reduce the operational burden of maintaining paper personnel files. However, according to one Regional Human Resources Division, discrepancies between the CHRIS database and paper employee files have lessened the degree of confidence in CHRIS' data integrity. In an attempt to improve the integrity of data maintained by CHRIS, the OCPO implemented employee read-only web access on September 30, 2004.

The GSA Chief Information Officer's February 2000 Capital Planning and Information Technology (IT) Investment Control Guide; June 2002 Order on IT Capital Planning and Investment Control; August 2002 IT Capital Planning and Investment Control Guide; April 2004

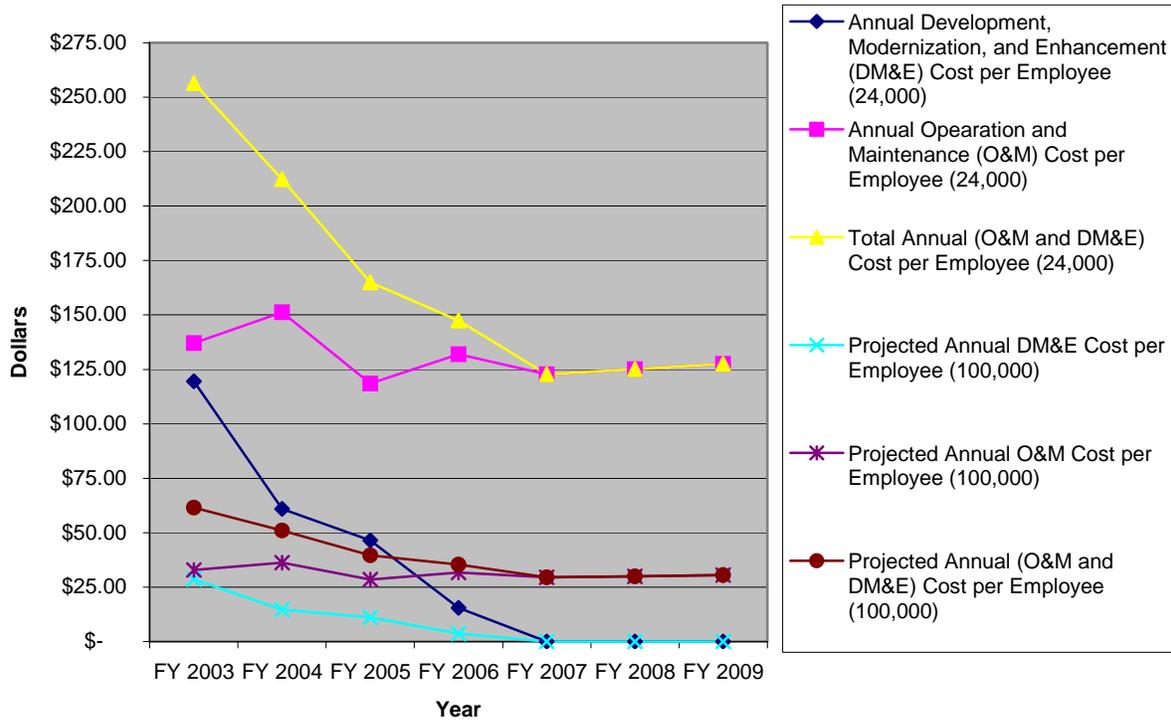
⁵ On December 1, 2004 JFMIP responsibilities were transferred to the Chief Financial Officers Council and the Office of Federal Financial Management (OFFM), and all system guidance issued by JFMIP is transferred to OFFM and remains in effect until modified.

System Development Life Cycle Policy Handbook, as well as the Office of Management and Budget's (OMB) November 2000 Circular A-130 with its Appendix IV all specify that a post-implementation review of the system should be performed. The objectives of such a review should include validating estimated benefits and costs, documenting effective management practices for broader use and lessons learned, and redesigning oversight mechanisms and performance levels to incorporate acquired knowledge. According to the Director and a management analyst in the CHRIS Division, a post-implementation review of CHRIS has not yet been carried out. Such a review would help GSA to better assess whether the system effectively and efficiently meets all user needs as well as JFMIP and HR system requirements, and would thus ensure long-term success for this very important system.

Expected Benefits Not Realized for CHRIS Due to Insufficient Customer Base

CHRIS has not yet realized an operating surplus from cross-servicing arrangements, nor reached a break-even business volume. In 2001, Gartner Inc. reported that competing Federal HR processing providers were charging their customers between \$98.35 to \$165 per employee and recommended that GSA establish an initial price point of \$100 per employee. However, GSA's per employee operations and maintenance (O&M) costs for CHRIS for FY 2001 were \$257, which prevented GSA from profiting at a competitive price near-term. Based on a growth estimate of 44,142 employees to be serviced through CHRIS by FY 2003, Gartner Inc. projected a shortfall of less than \$1 million in FY 2001 and \$543,000 in FY 2002, with a surplus of \$440,000 projected in FY 2003. However, as of FY 2005, CHRIS provided support for only 12,820 GSA and 10,622 cross-serviced employees, and thus the system is well below the projected customer base. The CHRIS system services the following external customers: National Archives and Records Administration, National Credit Union Administration, the Office of Personnel Management, the Railroad Retirement Board, the Export/Import Bank, and GSA's Agency Liaison Division that handles approximately 30 independent agencies, Presidential Boards, and Commissions throughout the government. GSA has not realized expected benefits from CHRIS cross-servicing arrangements, since pricing is insufficient to recover GSA's cost of providing HR services. Figure 1 conveys the actual annual cost for CHRIS per cross-serviced employee over a six-year period. The graph depicts annual employee costs strictly for development, modernization, and enhancement (DM&E) for CHRIS as well for the aggregate costs of DM&E, and operation and maintenance support with the system.

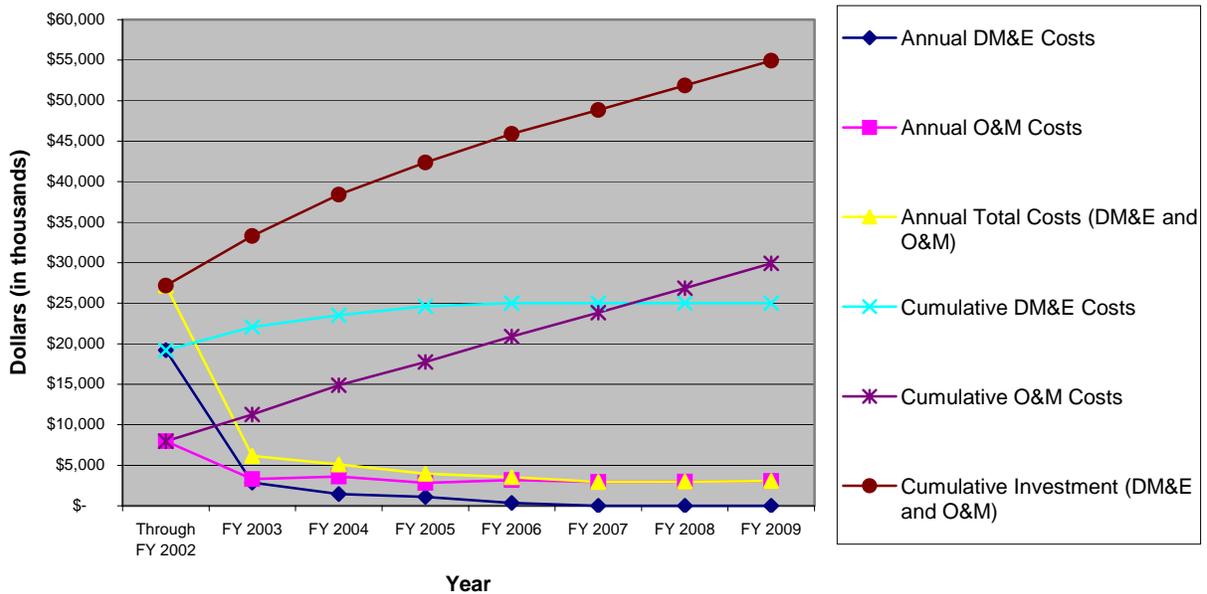
Figure 1: Annual CHRIS Costs Per Employee



This cost data shows that the customer base for CHRIS has not grown as anticipated, or as needed, to recover the investment for the system. CHRIS' external customers' fees have remained at \$100 per employee, however, since these fees exclude offsetting collections, including Oracle licensing and support, GSA must subsidize the system expenses. For example, actual O&M costs for CHRIS for FY 2004 were approximately \$151 per employee per year, so GSA essentially subsidized \$51 per every cross-serviced employee for that fiscal year. Current cost per employee estimates are based on an approximate cross-serviced customer base of 24,000. However, projected estimates are based on 100,000 cross-serviced employees.

Without projecting a quantifiable recovery of investment, CHRIS system lifecycle costs have also increased from an initial estimate of \$34 million to an estimated \$54 million in FY 2006. Figure 2 depicts growing lifecycle cost estimates reported for CHRIS. However, because available estimates do not include costs for development, modernization, and enhancement beyond FY 2006, the actual cost of CHRIS could be higher than projected.

Figure 2: CHRIS Lifecycle Cost Analysis



According to the CHRIS Division Director, the low customer base has occurred, in part, because marketing efforts have been restricted until the national standards for HR systems have been established. The changing environment for Federal HR systems has made it difficult for the OCPO to effectively market CHRIS to new customers. Current electronic Government (e-Gov) projects include one related to improving the Federal HR process by establishing easy to use, cost effective, standardized, integrated, e-HR/Payroll services to support the mission and employees of the Federal Government. The Office of Personnel Management (OPM) was given lead responsibility for these projects, and GSA is supporting this effort as a partner to OPM. The GSA payroll office was chosen by OPM/OMB as one of the four payroll service providers for the Executive Branch. The overall goal of these HR/Payroll e-Gov initiatives is to reduce the number of human resources and payroll systems in use throughout the Executive Branch. This requires an integration process with existing HR processes that has already begun with payroll systems and for HR systems. OPM has recently announced the new HRIS component of e-Government (HR Line of Business) initiative, and GSA intends to continue to be an HR service provider for other Federal agencies. However, due to the alignment of the Federal agencies with the four payroll providers, GSA has acquired only a few small agencies to provide payroll support, which could further limit the customer base for the system.

The OCPO has offered CHRIS, with its Oracle HR, to OMB as a possible system solution to be delivered by service providers with the HR Line of Business. A thorough post-implementation review is needed to document implementation experiences, recommend system enhancements, and provide guidance for considering options for the CHRIS system. The OCPO continues to enhance CHRIS and plans to keep its existing software enhancement commitments, such as Oracle upgrades, patches, module activation, and minor fixes, scheduled in 2005 and 2006. GSA must decide whether to: (1) keep the system and expand the customer base to offset costs; (2) offer CHRIS as a service provider under HRIS; or (3) sell the system and discontinue GSA's management role with CHRIS. Regardless of whether CHRIS is selected as an application suitable for the HR Line of

Business, critical decisions regarding CHRIS operations should be addressed promptly to minimize potential financial losses.

Improved System Security Controls Needed

During this audit several weaknesses with CHRIS' security controls that could lead to system vulnerabilities or unnecessary risks were identified and have been previously brought to management's attention for prompt correction. Our FY 2004 FISMA review⁶ identified specific security weaknesses including results from system vulnerability scans. With FISMA we identified specific risks for CHRIS, and since our review steps have been taken to address concerns related to budgeting for security costs and tracking known security risks for CHRIS. However, although CHRIS security controls were conditionally certified by the Office of the Chief Information Officer (OCIO) in February 2003, key security processes were not complete for CHRIS. Four conditions stipulated with the CHRIS Certification and Accreditation (C&A) were: (1) completion of the CHRIS Contingency Plan; (2) completion of the CHRIS Configuration Management Plan; (3) correction or mitigation of the technical findings from the Risk Assessment and System Test and Evaluation Report; and (4) implementation of a formal auditing and monitoring program to detect problems and misuse of OCPO resources. These conditions have been reported by the OCPO as completed, but a final, unconditional accreditation letter has not been issued for CHRIS. Further, system security C&A documents that we reviewed for CHRIS did not address all security controls as required by the GSA IT Security Program. At the time of our review, we found that background checks had not yet been completed for contractors hosting the system and providing system administration support to CHRIS before being granted access to the system. Finally, we also found that the CHRIS database has a number of vulnerabilities that, if exploited, may compromise the confidentiality, integrity and availability of the CHRIS system. Because CHRIS contains highly sensitive and valuable information that may be exposed to undue risk, the OCPO should take additional steps to more comprehensively address the management, operational, and technical security controls for the system.

Key Components of Security Have Not Been Addressed with Certification and Accreditation of System Controls

Several components of CHRIS security have not been addressed through the C&A process as required in the GSA IT Security Program and require management attention to manage the risks associated with changing technology, system enhancement, the growth of malicious software, and other threats. The Accreditation letter for CHRIS stipulates continued operation with the four conditions that were to be met no later than September 30, 2003: (1) completion of the CHRIS Contingency Plan; (2) completion of the CHRIS Configuration Management Plan; (3) correction or mitigation of the technical findings from the Risk Assessment and System Test and Evaluation Report; and (4) implementation of a formal auditing and monitoring program to detect problems and misuse of OCPO resources. Although these conditions have been reported as met, a final, unconditional accreditation letter has not yet been issued. Further, we found that CHRIS security documentation did not always meet requirements. While a Contingency Plan

⁶ FY 2004 Office of Inspector General Information Security Review of the Comprehensive Human Resources Integrated System, Report Number A040179/O/T/F05006, January 11, 2005.

had been completed for the system during our review, the Contingency Plan did not include procedures and frequency for testing backup tapes, procedures for performing damage assessments, and procedures for terminating contingency operations. The system Risk Assessment did not include a business impact analysis or identify the system's mission, processes, and interfaces, and described controls that should be used rather than those that are currently in place. The CHRIS Security Plan did not address recommendations made in the system Risk Assessment and did not include procedures for system and application timeout handling, review of database management system logs, external/internal handling of media, and use of integrity verification programs to look for evidence of data tampering, errors, and omissions. CHRIS security officials have updated the system Security Plan to include procedures for implementation of a formal auditing and monitoring program to detect problems and misuse of OCPO resources.

[Sensitive information regarding Oracle features has been removed here.]

As a result, CHRIS and its sensitive and valuable information may be exposed to undue risk if the OCPO does not take steps to more comprehensively address potential system threats and vulnerabilities and issue a final, unconditional certification and accreditation letter.

Background Checks for Contractors Not Completed

Contractors developing functional enhancements for CHRIS and providing routine maintenance support for the system have not received required background checks before being granted access to the system and its sensitive data, as required by the GSA IT Security Policy. The CHRIS Security Plan identified that aggregate sensitivity for data is medium-high due to the amount of private information located within the environment because employee access to and use of CHRIS' data affects GSA's mission and operations. Further, efficiency of service and confidentiality, integrity, and availability concerns remain that could impact HR activities. GSA's IT Security Policy requires that contractors who design, operate, test, maintain, and/or monitor GSA systems shall be required to have at least a background investigation consisting of a National Agency Check and Inquiries Credit before being granted access to GSA systems or data. At the time of our review of CHRIS, one development contractor's background check had been resubmitted and two other contractors' background checks had been requested but not completed. During the exit conference, the OCPO reported that the problem with background checks for CHRIS contractor personnel has been addressed except for one newly hired contractor, who has no access to the production system. The development contract for CHRIS requires compliance with the Privacy Act "and applicable agency rules and regulations," but does not specify a deadline for completion of background checks. Without required background checks for CHRIS contractor personnel, compensating controls, such as criminal record checks, monitoring of detailed audits logs, and obtaining the contractor's internal background investigation and employment history record, should be implemented.

Improvements Needed in Oracle Database Security

We found specific vulnerabilities in the CHRIS database that, if exploited, may compromise the confidentiality, integrity, and availability of the system. The CHRIS database contains sensitive

personnel data, such as social security numbers, which could be used for identity theft if compromised. An Oracle hardening guide was not in place to assist CHRIS database administrators with guidance on the configuration of a secure Oracle database, until after our review. In the absence of this guidance, our assessment was based on the recommendations of the IT Governance Institute's Oracle Database Security, Audit and Control Features⁷.

[Examples of vulnerabilities have been removed due to their sensitive nature.]

Careful attention to these conditions is necessary to manage the risks associated with changing technology, system enhancement, the growth of malicious software, and other threats that CHRIS faces. Detailed information as to the specific results of our review of the CHRIS Oracle database⁸ were provided to the OCPO separately due to the sensitive and technical nature of the information reported.

Recommendations

We recommend that the GSA Chief People Officer:

- (1) Conduct a post-implementation review in accordance with the Office of Management and Budget's Circular A-130 and GSA's August 2002 IT Capital Planning And Investment Guide, to:
 - a. Validate estimated benefits and costs for CHRIS;
 - b. Evaluate CHRIS to ensure positive return on investment; and
 - c. Ensure that the system meets organizational and user needs.

- (2) Complete an alternatives analysis to fully consider the costs and benefits for the options of:
 - a. Keeping the system and expanding the customer base to offset costs; or
 - b. Offering CHRIS as a service provider under HRIS; or
 - c. Selling the system and discontinuing GSA's management role with CHRIS.

- (3) Ensure that adequate security controls are in place to manage risks with CHRIS by:
 - a. Completing the system certification and accreditation process for CHRIS including updating required system security documentation.
 - b. Prioritizing necessary background checks for contractor staff as required by the GSA IT Security Policy and implementing compensating controls until this process is completed.
 - c. Carefully assessing the Oracle database vulnerabilities and applying technical solutions to reduce associated risks.

⁷ PriceWaterhouseCoopers, Inc. produced Oracle Database Security, Audit and Control Features, published by the IT Governance Institute in 2004, with assistance from many industry security experts.

⁸ Security Vulnerabilities with the Comprehensive Human Resources Integrated System (CHRIS) Oracle Database, Report Number A040142/O/T/F05021, July 20, 2005.

Management Response

We met with the Chief People Officer (CPO) and Office of the Chief People Officer (OCPO) personnel to discuss the results of our review and to identify any areas in the draft report that may require revisions. They generally concurred with the findings and two of the three recommendations as presented in the report. Written comments provided by the CPO indicate that OCPO will take actions aimed at addressing the identified areas of risk in the report. Specifically, they identified ongoing or planned management actions toward: (1) conducting a formal post-implementation review for CHRIS to better assess whether the system effectively and efficiently meets user needs as well as JFMIP and HR system requirements, and (2) continuing to enhance CHRIS security controls including another system certification and accreditation and completing background checks on contractors.

The CPO did not agree with the recommendation to complete an alternatives analysis to fully consider the costs and benefits for the options of: (1) keeping the system and expanding the customer base to offset costs; or (2) offering CHRIS as a service provider under HRIS; or (3) selling the system and discontinuing GSA's management role with CHRIS. The CPO stated "an analysis was completed in 2003 and in 2005 the Office of the CPO and the Office of the Chief Financial Officer (CFO) decided that it would be in GSA's best interest to offer CHRIS and the Payroll Accounting Reporting (PAR) system, in combination, as the core of an HR Line of Business (LoB) Shared Service Center solution. A business case (OMB Exhibit 300) was submitted to OMB earlier this month as part of the FY 2007 budget formulation process. The offices of the CPO and CFO will work together to develop a more complete business model to support this plan." While the decision to continue CHRIS as a service provider under HRIS is an option that we recommended be considered, a more complete business model should clarify how alternatives were considered.

A copy of the management comments is provided in its entirety in Appendix B.

Internal Controls

As discussed in the Objectives, Scope, and Methodology section of this report, our audit objectives were to answer the following questions: (1) does GSA's CHRIS solution provide the needed functionality, security, and other controls for system operations to ensure the data's integrity and reliability; (2) does the OCPO have processes in place to improve system functionality and usability; (3) is CHRIS financially beneficial to GSA; and (4) if not, what actions are needed to improve CHRIS? We focused our review on selected modules within CHRIS, management controls, operational controls, access controls, as well as the addition of new functionality within CHRIS. The Results of Audit and Recommendations sections of this report state in detail the need to strengthen specific managerial and technical controls with CHRIS. Our review did not include a detailed analysis of all controls or capabilities within CHRIS or overall controls provided within the OCPO.

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

KEY EVENTS IN CHRIS LIFECYCLE

<u>Date</u>	<u>CHRIS Event</u>
September 1, 1996	Investment in CHRIS Initiated.
Late 1999	Business plan for CHRIS issued.
August 2000	Phase 1 of CHRIS Implemented.
October 12, 2001	Gartner study on pricing for CHRIS issued.
December 17, 2001	Phase 2 of CHRIS Implemented.
February 2002	CHRIS was implemented for its Federal customer agencies.
November 14, 2002	Access Control Directive for CHRIS issued.
December 20, 2002	Risk Assessment for CHRIS issued.
February 20, 2003	System Security Plan for CHRIS issued.
February 20, 2003	System Test and Evaluation Report for CHRIS issued.
February 26, 2003	Security Certification and Accreditation for CHRIS issued.
March 31, 2003	Contingency Plan for CHRIS released.
July 29, 2003	Contingency Plan for CHRIS modified.
September 8, 2003	IBM study of CHRIS strategic options issued.
June 18, 2004	Patch Management Process document for CHRIS issued.
September 30, 2004	CHRIS Personal View now operational.
November 20, 2004	Contingency Plan for CHRIS revised.

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

GSA CPO's RESPONSE TO DRAFT AUDIT REPORT



GSA Office of the Chief People Officer

SEP 30 2005

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: GAIL T. LOVELACE *Gail T. Lovelace*
CHIEF PEOPLE OFFICER (C)

SUBJECT: Management Response to Draft Audit Report
Strategic Challenges for GSA's CHRIS System
Report Number A040142

The Office of the Chief People Officer generally agrees with the findings contained in the draft audit report, and agrees with two of the three recommendations. This management response addresses the specific recommendations contained in the draft report, and provides additional information.

Recommendations

- (1) Conduct a post-implementation review in accordance with the Office of Management and Budget's Circular A-130 and GSA's August 2002 IT Capital Planning And Investment Guide, to:
 - a. Validate estimated benefits and costs for CHRIS;
 - b. Evaluate CHRIS to ensure positive return on investment; and
 - c. Ensure that the system meets organizational and user needs.
- (2) Complete an alternatives analysis to fully consider the costs and benefits for the options of:
 - a. Keeping the system and expanding the customer base to offset costs; or
 - b. Offering CHRIS as a service provider under HRIS; or
 - c. Selling the system and discontinuing GSA's management role with CHRIS.
- (3) Ensure that adequate security controls are in place to manage risks with CHRIS by:
 - a. Completing the system certification and accreditation process for CHRIS including updating required system security documentation.
 - b. Prioritizing necessary background checks for contractor staff as required by the GSA IT Security Policy and implementing compensating controls until this process is completed.
 - c. Carefully assessing the Oracle database vulnerabilities and applying technical solutions to reduce associated risks.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Management Response to Recommendations

1. We agree that conducting a formal post-implementation review of CHRIS, in accordance with the Office of Management and Budget's Circular A-130 and GSA's August 2002 IT Capital Planning and Investment Guide, would help GSA to better assess whether the system effectively and efficiently meets user needs as well as JFMIP and HR system requirements, and would thus ensure long-term success for this system.
2. We do not agree that another alternatives analysis should be completed. Such an analysis was completed in 2003 with the assistance of IBM. In the spring of 2005, the Office of the CPO and the Office of the Chief Financial Officer (CFO) decided that it would be in GSA's best interest to offer CHRIS and the Payroll Accounting Reporting (PAR) system, in combination, as the core of an HR Line of Business (LoB) Shared Service Center solution. A business case (OMB Exhibit 300) was submitted to OMB earlier this month as part of the FY2007 budget formulation process. The offices of the CPO and CFO will work together to develop a more complete business model to support this plan.
3. We agree that we should continue to enhance CHRIS security controls. CHRIS will undergo another system certification and accreditation in 2006, and we will update all required system security documentation. All background checks for contractor staff have now been completed with the exception of one recent hire, and this person has recently submitted the necessary security paperwork. The contractor, whose security clearance is pending, does not have access to production or sensitive data. Oracle database vulnerabilities identified during the audit are currently being addressed by the system administrator and database administrator. This is an on-going activity, and we work closely with Oracle to ensure that, in the future, quarterly security updates and patches are installed.

General Comments

The report says that "GSA's strategic efforts with the system have been impeded by user reluctance to use the system and the availability of duplicative system functionality provided by other GSA systems." Several legacy, home grown systems were already in place prior to the implementation of CHRIS, and a few others were created during the early stages of CHRIS when CHRIS could not yet provide needed functionality. As these legacy systems are replaced by CHRIS, or otherwise reach the end of their lifecycle, they are systematically being retired.

The report says that "GSA has also faced challenges in marketing CHRIS. Due to an insufficient customer base, CHRIS is not recovering costs or the revenue originally expected." GSA made a conscious decision to stop marketing CHRIS, and to curtail bringing on additional clients, until the impact of HR LOB on the Federal HR community and the CHRIS system could be determined. GSA has recently decided to become an HR LOB Shared Service Center, using the CHRIS and PAR systems, and plans to expand the customer base to offset costs.

The report says that "CHRIS has encountered user dissatisfaction." This is true in the early days of any new IT system. Many early CHRIS users experienced growing pains while the Oracle product was being federalized, and may still have a residual negative perception of CHRIS. However, current CHRIS users have expressed a high degree of user satisfaction. Our internal and external clients have recently requested additional products and services as a result of positive experiences. We will be implementing a new customer survey to identify and monitor user satisfaction.

The report says that "According to one Regional Human Resources Division, discrepancies between the CHRIS database and paper employee files have lessened the degree of confidence in CHRIS' data integrity." Some of this problem is a carry-over from GSA's previous HR system. Over the past two years, the Consolidated Processing Center has compared key data in paper Official Personnel Folders (OPFs) to data in CHRIS. Discrepancies have been identified and corrected. New CHRIS data input has been fully-synchronized with paper records since 2000. GSA will work with OPM to convert the pre-CHRIS paper files into an electronic format, in accordance with the Enterprise HR Initiative (EHRI).

The report says, "Due to the alignment of the Federal agencies with the four payroll providers, GSA has acquired only a few small agencies to provide payroll support, which could further limit the customer base for the system." Oracle has recently built an interface between the Oracle Federal HR Application and USDA's National Finance Center, the largest HR LOB Shared Service Center. We believe that GSA can take advantage of this new payroll interface to attract larger agencies, and further expand our customer base.

The Background section of the report refers to the legacy "Personnel Information Reporting System." The correct name of this legacy system is the "Personnel Information Resources System"

STRATEGIC CHALLENGES FOR
GSA'S COMPREHENSIVE HUMAN
RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A040142/O/T/F05025

REPORT DISTRIBUTION

	<u>Copies</u>
Chief People Officer (C)	3
Director, Office of Information Management, Office of the Chief People Officer (CI)	1
Director, CHRIS Division, Office of the Chief People Officer (CID)	1
Chief Information Officer (I)	2
Regional Administrator (WA)	1
Regional Administrator (3A)	1
Regional Administrator (6A)	1
Audit Follow-up and Evaluation Branch (BECA)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Administration and Data Systems Staff (JAS)	1
Regional Inspector General for Auditing (JA-W)	1
Assistant Inspector General for Investigations (JI)	1
Regional Inspector General for Investigations (JI-W)	1
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F)	1
Deputy Assistant Inspector General for Acquisition Audits (JA-A)	1