Audit Report

IMPROVED ACCESS CONTROLS COULD HELP PROTECT PERSONNEL INFORMATION WITHIN THE COMPREHENSIVE HUMAN RESOURCES INTEGRATED SYSTEM (CHRIS)
REPORT NUMBER A060246/O/T/F08013

September 8, 2008

Office of Inspector General
General Services Administration

Office of Audits

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 8, 2008

Reply to: Gwendolyn A. McGowan
Deputy Assistant Inspector General for Information Technology Audits (JA-T)

To: Gail T. Lovelace
Chief Human Capital Officer (C)

Subject: Improved Access Controls Could Help Protect Personnel Information within the Comprehensive Human Resources Integrated System (CHRIS)
Report Number A060246/O/T/F08013

This report presents the results of our audit of specific access controls implemented with the Comprehensive Human Resources Integrated System (CHRIS) and highlights our audit findings and recommendations to Office of the Chief Human Capital Officer (OCHCO) management for improving system access controls for CHRIS. We have coordinated closely throughout the audit with system officials on specific Information Technology (IT) security issues we identified. We presented detailed information in a briefing to the OCHCO on June 11, 2008, and a copy of those slides are included as Appendix A. Due to the sensitive information contained in the Appendix related to the results of our technical security control scans, only reports provided to the OCHCO and the Office of the Chief Information Officer (OCIO) contain Appendix A.

Background

The OCHCO deployed CHRIS, a customized version of Oracle's Federal Human Resources Management System (OFHR), in August 2000 to provide on-line capabilities through a client server environment and improve Human Resources (HR) processing. CHRIS is used to initiate, generate, and store personnel actions and provide HR data used to produce reports for GSA and its Federal customers to meet internal and external reporting requirements. Over the past seven years, CHRIS has undergone significant changes, including transitioning to providing users web-based access over GSA's network in December 2001, providing GSA Associates with web-based access to their own personnel information within the system in September 2004, and implementing award functionality in March 2006.

Objective, Scope, and Methodology

The object of this review was to determine: (1) if management, operational, and technical controls have been implemented within CHRIS to appropriately limit access to sensitive personnel information; (2) if not, what vulnerabilities exist that may allow improper or fraudulent activity; and (3) what compensating controls should be implemented to ensure that CHRIS access controls support the mission and goals of Agency Services and Staff Offices (S/SO)? We gathered information related to the implementation of access controls and analyzed key security documentation. We surveyed key Agency personnel and members of their staff, including the Chief Human Capital Officer (CHCO); OCHCO, Director, Office of Information Management; system security officials; and other OCHCO personnel responsible for developing, maintaining, and operating the system. We also interviewed representatives from other GSA S/SOs and Federal agencies that use the CHRIS system, including the National Archives and Records Administration (NARA) in College Park, Maryland and the National Credit Union Association (NCUA) in Alexandria, Virginia. Our review focused on users with Manager Self Service access for CHRIS and the sensitive HR information that can be obtained through CHRIS on-line. We used commercially available tools and agreed upon procedures to complete network security scanning, examine database configuration, and review web application security for CHRIS.

To assess managerial, operational, and technical controls for CHRIS, we relied on applicable statutes, regulations, policies, and operating procedures regarding the development, implementation, and testing of IT system access controls, such as: Office of Management and Budget (OMB) A-130, Appendix III, Security of Federal Automated Information Resources, November 28, 2000; the GSA IT Security Policy, CIO P 2100.1D, June 2007; the GSA Chief Information Officer's (CIO) IT procedural guides on certification and accreditation, security test and evaluation, configuration management plans, security incident handling, and managing enterprise risk; the Federal Information Security Management Act of 2002; OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006; and National Institute of Standards and Technology (NIST) special publications for securing Federal information systems. We conducted this performance audit work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The scope of our audit did not address overall functionality provided with CHRIS, training of users, or physical access controls. The review also did not assess the accuracy and integrity of the data the system maintains.

Highlights of Audit Findings

CHRIS is GSA's agency-wide automated HR management system. In implementing CHRIS, the OCHCO provided important on-line capabilities and improved HR processes for GSA Associates and employees of other Federal agencies that have contracted with GSA to use CHRIS. Our review identified several areas where improved access controls for CHRIS could help to better protect personnel information. We found that careful consideration of the system's functionality and controls is needed to better restrict access to certain personnel data. Overall, improved access controls would help to enforce "Least Privilege" requirements for CHRIS. Independent reviews of CHRIS audit logs could also help to address "Separation of Duties" control risks, and careful consideration of controls for system reporting capabilities would greatly assist in efforts to protect CHRIS data. Our review also found that prompt security enhancements could improve CHRIS. The OCHCO should take steps to strengthen access controls for CHRIS to (1) better ensure that personnel information is protected from unauthorized disclosure, access, and modification and (2) preserve authorized access restrictions.

Improved Access Controls Would Help to Enforce Least Privilege Requirements for CHRIS. GSA's CHRIS system has been designated as a moderate risk system that requires "Least Privilege" access to data and processes. Specifically, Least Privilege is a policy that requires that a system's user be given no more access than necessary to perform his or her official duties. Implementing Least Privilege effectively requires the (1) identification of specific tasks a user needs to be able to perform, (2) determination of the minimum set of privileges required to perform those tasks, and (3) restriction of the user to no more than those privileges needed to perform those specified tasks. Procedures provided by the GSA-CIO for system access control requires that Least Privilege be implemented for GSA's moderate risk systems. As such, only personnel with proper authorization and a "need-to-know" should be allowed access to data processed, handled, or stored within the CHRIS system. Further, CHRIS security documentation states that users are given the least amount of privileges or access needed to perform their duties. The Privacy Impact Assessment (PIA)[1] developed for CHRIS also provides information on access for the groups of users for the system and the amount of access each user group should have. The users in the "managers and supervisors" group are described in the PIA as having read-only access to their direct reports, with the ability to review limited personnel and benefit information as well as assignment position, education, training, and performance appraisal information for their employees. Our review found that managers and supervisors, through the "Manager Self Service" menu, can create, view, modify, and approve performance plans, appraisals, and awards for their direct employees. Managers and supervisors with "Manager Self Service" access can also issue awards and view award amounts and justifications for GSA employees from other S/SOs. Because the system does not restrict information that can be input into the award justification data field, supervisors are free to include project-specific or other information about individuals receiving awards. As such, award justifications within CHRIS can contain sensitive information about other GSA divisions and personnel activities.[2] However, award-related information could be used for unofficial purposes, and restricting access based on a "need-to-know" could help to better manage risk associated with unauthorized access under the Least Privilege policy.

CHRIS officials explained that the system was designed to delegate award authority and enable managers to recognize staff who may not be assigned to their office. Through discussions with seven managers from the Public Buildings Service (PBS), Federal Acquisition Service (FAS), and Staff Offices at GSA's Central Office, we found instances, however, where supervisors who issue awards were unaware that managers from other S/SOs had access to award information. Most managers we spoke with informed us that they would prefer that access to their employee award information be restricted to only those within their own organizations who have a need to access award information. We also found that Human Resources specialists from the National Archives and Records Administration (NARA) currently use a customized version of the CHRIS awards module to provide for restricted access to NARA award information. This capability provides NARA managers the ability to issue an award to an employee from another office without access to information on the award amounts and justifications input by another manager.

[1] A PIA addresses privacy issues associated with the collection and retention of sensitive information and examines the risks and effects of collecting, maintaining, and disseminating information in identifiable form.

[2] The two exceptions to this are Senior Executive Service employees and Office of Inspector General investigators.

In September 2005,[3] we recommended that the CHCO conduct a post-implementation review for CHRIS: (1) validate estimated benefits and costs for CHRIS, (2) evaluate CHRIS to ensure positive return on investment, and (3) ensure that the system meets organizational and user needs. Subsequently, during this audit, we were informed that the OCHCO planned to do an operational analysis in lieu of a post-implementation review. The OCHCO has since put completion of the operational analysis on-hold until a decision is made at GSA as to how to move forward, to either continue with CHRIS or move to a selected HR Shared Service Center (SSC). Given the access control weaknesses we have identified, we re-affirm the importance of completing a comprehensive assessment, including an evaluation of the controls implemented for and functionality provided with the system, to determine how well the system is meeting all user and management requirements and whether required controls, including provisions to enforce Least Privilege, are in place and operating as intended.

Ensuring Independent Reviews of CHRIS Audit Logs Could Help to Address Separation of Duties Control Risks. There is a potential conflict of interest when the same person who administers access control functions also administers audit functions for any system. Effective "Separation of Duties" is achieved by dividing responsibilities among two or more individuals or organizational roles to diminish the likelihood that errors and wrongful acts will go undetected, since the activities of one individual or group serve as a check on the activities of the other. Audit trails can also be used in concert with access controls to identify and provide information about users who are suspected of improper access to or modification of data (e.g., introducing errors into a database). When audit trails are activated for a system, comparisons can then be made between the actual changes made to records and what was expected. This practice can help management determine if errors were made by the user, by the system or application software, or by some other source. System resources should also be monitored to detect unauthorized activity and deviations from the access control policy, and verify the effectiveness of implemented security controls. NIST Special Publication 800-53 and the GSA IT Security Policy[4] require that the Agency's information systems enforce Separation of Duties requirements, including those between access control functions and auditing procedures. Our review found that, due to limited personnel resources for CHRIS, the OCHCO had not implemented Separation of Duties for system auditing and monitoring. While we recognize the challenges that limited resources place on organizations, we re-affirm the importance of implementing key controls to ensure that personnel information is adequately protected and that potential unauthorized activity within the CHRIS system is identified and investigated.

Careful Consideration of Controls for System Reporting Capabilities Is Needed to Protect Personnel Information. CHRIS relies on the Commercial-off-the-Shelf (COTS) product Business Objects, managed by PBS, for reporting. GSA, like other organizations, is becoming increasingly reliant on information system services that are implemented outside of the system's accreditation boundary, which are used by, but not a part of, the organizational information system. In general, the growing dependence on external service providers and new relationships being forged with those providers can present new and difficult challenges, especially in the area of information system security. However, the responsibility for adequately mitigating risk to

[3] Strategic Challenges for GSA's Comprehensive Human Resources Integrated System (CHRIS), Report Number A040142/O/T/F05025, September 30, 2005.
[4] GSA Order, CIO P 2100.1D, GSA Information Technology (IT) Security Policy, July 21, 2007.

agency-wide and customer HR operations and assets arising from the use of external information system services remains with the authorizing official for the system. Our review found that the OCHCO had not yet assessed controls for or risks associated with accessing CHRIS personnel information through the Business Objects reporting utility. NIST recommends that organizations that own and operate interconnected systems should establish a Memorandum of Understanding (MOU) that defines the responsibilities of both parties in establishing, operating, and securing an interconnection. An MOU between the OCHCO and the PBS OCIO for services supporting CHRIS access to the PBS Business Objects enterprise server software license and associated tools was established in March 2001. The MOU documents the number of users that will access the Business Objects software and that need computer-based training, as well as the cost to the OCHCO for those services for a two-year period. The details of the interconnection and the controls required for the protection of personnel information accessed through the Business Objects reporting utility, however, have not yet been established. For instance, key roles and responsibilities for securing the interconnection and CHRIS data for PBS and the OCHCO are not yet clear. The potential impact of this type of operating environment was highlighted on June 4, 2007 when an authorized CHRIS user from NARA inadvertently accessed and displayed employee records from all Agencies with information stored in the CHRIS database using the PBS Business Objects utility. Prompt action was taken by the OCHCO to identify the vulnerability and to make every attempt to avoid a reoccurrence. However, this security incident highlighted the need to have a complete MOU in place to adequately define roles and responsibilities for securing CHRIS data accessed through Business Objects and identify required controls to manage risks, including unauthorized or unintentional access to or disclosure of personnel information. To address this need, we believe it is important for the OCHCO to closely coordinate with PBS and establish a MOU that defines roles and responsibilities for securing CHRIS data for PBS and the OCHCO and that identifies security controls required to appropriately restrict personnel data provided with the Business Objects reporting utility.

Prompt Security Enhancements Could Improve CHRIS. We applied commercially available vulnerability assessment tools, manual techniques, and agreed upon procedures to test technical controls for CHRIS. Testing included reviewing web application security and examining database configuration. The tests identified opportunities to reduce risk to the CHRIS web application and database. We met with system security officials the end of May 2007 and conveyed the detailed results of our system security scanning. We also re-scanned the database in July 2007 after a system upgrade and discussed updated results with system security officials. Vulnerabilities identified with our scanning of the CHRIS Oracle database involve recording the actions taken by users in the database, including the activity of privileged users. These vulnerabilities could make it more difficult to detect when an attack occurs and to be able to analyze the attack after the fact. Automated scanning of the CHRIS web application identified possible SQL injections and instances where exceptions were not being appropriately handled, both of which could enable an attacker to exploit the vulnerability and gain unauthorized access to the database and its contents. Manual web application testing identified additional opportunities to harden the system, such as eliminating cross site scripting and delaying logins, to reduce risk. Specific vulnerabilities identified during our review are included in the briefing slides provided as Appendix A. Due to the sensitive nature of the information, only reports given to the OCHCO and OCIO contain this appendix. Taking specific steps to secure the CHRIS database and web application would reduce the likelihood that the system could be compromised due to known vulnerabilities, which could put personnel information and the CHRIS system at undue risk.

Recommendations

To better restrict access to personnel information, we recommend that the Chief Human Capital Officer:

1. Complete a comprehensive assessment, including an evaluation of access controls implemented for and functionality provided with the system, to determine if CHRIS has been implemented in accordance with user and management requirements and whether Least Privilege controls are in place and operating as intended.
2. Ensure independent reviews of CHRIS auditing and monitoring logs are completed.
3. Coordinate with PBS to establish a MOU that defines roles and responsibilities for securing CHRIS data for PBS and the OCHCO and identifies security controls required to protect personnel data viewed with the Business Objects reporting utility.
4. Address CHRIS technical vulnerabilities and ensure all known vulnerabilities are promptly recorded and mitigated.

Management Comments

The CHCO concurred with all audit findings and recommendations. A copy of the CHCO's comments is provided in its entirety as Appendix B.

Internal Controls

The objective of this review was to determine: (1) if management, operational, and technical controls have been implemented within CHRIS to appropriately limit access to sensitive personnel information; (2) if not, what vulnerabilities exist that may allow improper or fraudulent activity; and (3) what compensating controls should be implemented to ensure that the CHRIS access controls support the mission and goals of Agency Services and Staff Offices (S/SO)? This report states the need to strengthen specific access controls for CHRIS in order to better protect personnel information. This review did not address overall system functionality or physical access controls. We also did not assess the integrity or accuracy of the information maintained in the system.

I wish to express my appreciation to you and your staffs for your cooperation during the audit. If you have any questions, please contact me or Gwen McGowan, Deputy Assistant Inspector General for IT Audits, on 703-308-1223.

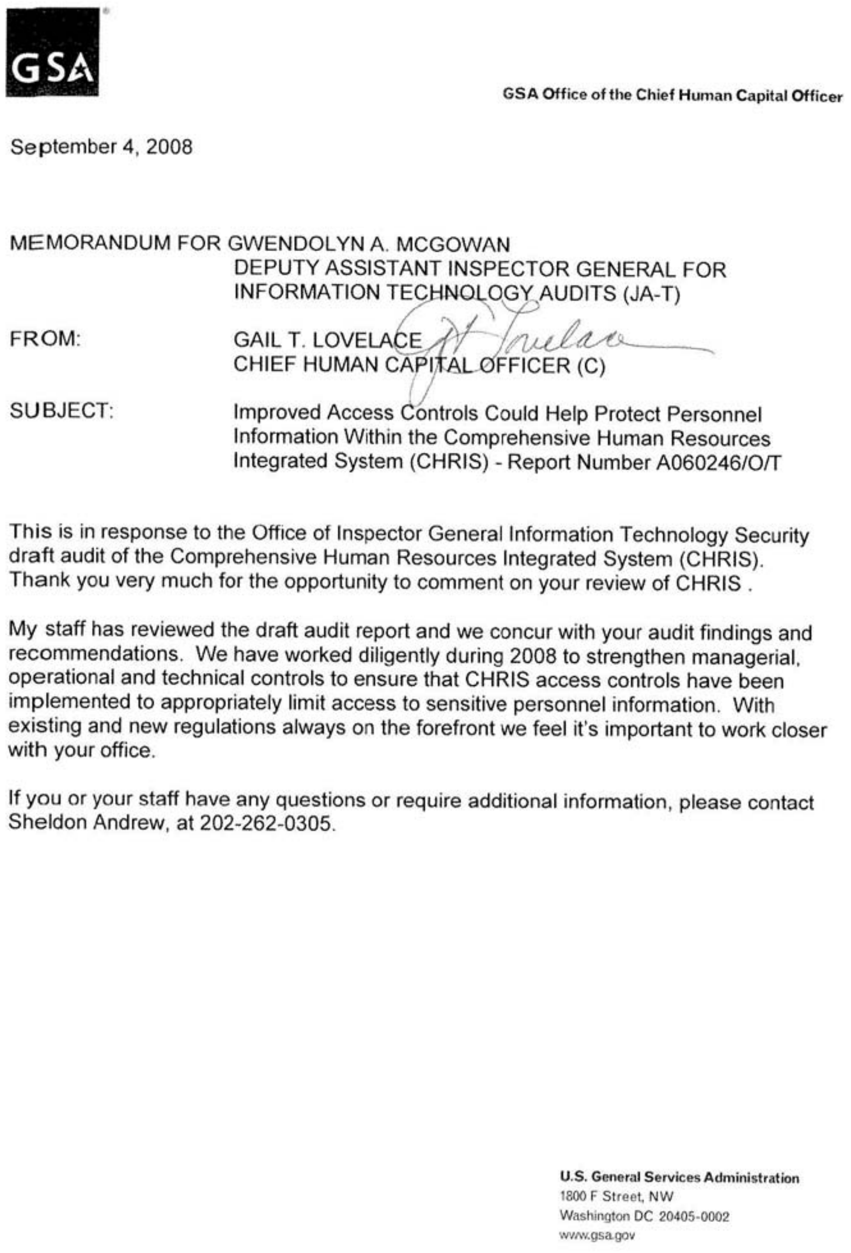
Jennifer M Klimes

Jennifer M. Klimes
Audit Manager, Information Technology Audit Office (JA-T)

APPENDIX A –BRIEFING SLIDES TO THE CHCO

Due to the sensitive nature of the information contained in this appendix, only reports provided to the Office of the Chief Human Capital Officer (OCHCO) and the Office of the Chief Information Officer contain a copy of the briefing slides used to present detailed information to the OCHCO on June 11, 2008. Requests for copies of these slides should be referred to Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits, or Jennifer Klimes, Audit Manager, on 703-308-1223.

APPENDIX B – GSA CHCO'S RESPONSE TO THE DRAFT REPORT



GSA

GSA Office of the Chief Human Capital Officer

September 4, 2008

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

FROM: GAIL T. LOVELACE
CHIEF HUMAN CAPITAL OFFICER (C)

SUBJECT: Improved Access Controls Could Help Protect Personnel Information Within the Comprehensive Human Resources Integrated System (CHRIS) - Report Number A060246/O/T

This is in response to the Office of Inspector General Information Technology Security draft audit of the Comprehensive Human Resources Integrated System (CHRIS). Thank you very much for the opportunity to comment on your review of CHRIS .

My staff has reviewed the draft audit report and we concur with your audit findings and recommendations. We have worked diligently during 2008 to strengthen managerial, operational and technical controls to ensure that CHRIS access controls have been implemented to appropriately limit access to sensitive personnel information. With existing and new regulations always on the forefront we feel it's important to work closer with your office.

If you or your staff have any questions or require additional information, please contact Sheldon Andrew, at 202-262-0305.

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

IMPROVED ACCESS CONTROLS
COULD HELP PROTECT PERSONNEL
INFORMATION WITHIN THE COMPREHENSIVE
HUMAN RESOURCES INTEGRATED
SYSTEM (CHRIS)
REPORT NUMBER A060246/O/T/F08013

APPENDIX C – REPORT DISTRIBUTION

	Copies
With Appendix A	
Chief Human Capital Officer, Office of the Chief Human Capital Officer (C)	3
Chief Information Officer, Office of the Chief Information Officer (I)	2
Without Appendix A	
Chief Information Officer, Public Buildings Service (PG)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Administration and Data System Staff (JAS)	1
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F)	1
Assistant Inspector General for Investigations (JI)	1
Internal Control and Audit Division (BEI)	1
Audit Liaison, Office of the Chief Human Capital Officer (C)	1