PERFORMANCE AUDIT

OF

HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) SELF-SERVICE

DEPARTMENT OF CIVIL SERVICE

July 2004

19-596-03

"...The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof."

– Article IV, Section 53 of the Michigan Constitution

Audit report information may be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit
Human Resources Management Network (HRMN) Self-Service
Department of Civil Service (DCS)

Report Number:
19-596-03

Released:
July 2004

HRMN Self-Service is the State's Web-based automated system used by State employees and human resource managers to view and maintain personnel information related to employee benefits, leave balances, pay warrant information and withholdings, and life events. HRMN Self-Service also enables human resource managers to track and maintain human resource reports.

Audit Objective:
To assess the effectiveness of security over HRMN Self-Service.

Audit Conclusion:
DCS did not completely establish effective security over HRMN Self-Service.

Material Conditions:
DCS did not sufficiently evaluate and minimize the risk of providing confidential State employee and dependent data over the Internet through HRMN Self-Service. Appropriate evaluation and risk assessment would minimize vulnerabilities to the State and to State employees resulting from unauthorized access. (Finding 1)

DCS did not completely establish effective access and password controls over HRMN Self-Service. Effective access and password controls minimize the possibility of unauthorized users obtaining access to HRMN Self-Service data. (Finding 2)

DCS had not developed and implemented sufficient Web application security controls. Without the implementation of sufficient Web application security controls, personnel data and Web application resources are vulnerable to intrusion or misuse. (Finding 3)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of general controls over HRMN Self-Service.

Audit Conclusion:
The Department of Information Technology's (DIT's) general controls over HRMN Self-Service were reasonably effective.

Reportable Conditions:
DIT had not established controls over the operating system configuration. The operating system should be installed with a minimal service configuration to reduce the risk of intrusion and the exploitation of well-known operating system vulnerabilties. (Finding 4)

DIT had not established complete operating system access controls. This could result in unauthorized modification, loss, or disclosure of confidential State employee data. (Finding 5)

DIT had not established complete physical security controls over HRMN Self-Service resources. Physical security controls help ensure that valuable system resources are safeguarded and that access is limited to individuals responsible for managing the system. (Finding 6)

DIT should strengthen controls over program changes to HRMN Self-Service. Program change controls help ensure that only authorized, tested, and approved program modifications are implemented and that access to and distribution of programs are carefully controlled. (Finding 7)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 7 findings and 7 corresponding recommendations. The agency preliminary response indicated that DCS and DIT agreed with the 3 recommendations and 4 findings, respectively, pertaining to their operations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

July 27, 2004

Ms. Susan Grimes Munsell, Chairperson
Civil Service Commission
and
Ms. Janet M. McClelland, Acting State Personnel Director
Department of Civil Service
Capitol Commons Center
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Ms. Munsell, Ms. McClelland, and Ms. Takai:

This is our report on the performance audit of Human Resources Management Network (HRMN) Self-Service, Department of Civil Service.

This report contains our report summary; description of system; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during the audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) SELF-SERVICE
DEPARTMENT OF CIVIL SERVICE

Description of System

Self-Service is a component of the Human Resources Management Network* (HRMN), the State's automated human resource, payroll, and employee benefits system. HRMN Self-Service* is a Web-based automated system used by State employees and human resource managers to view and maintain personnel information related to employee benefits, leave balances, pay warrant information and withholdings, and life events. HRMN Self-Service also enables human resource managers to track and maintain human resource reports. Employees and human resource managers gain access to HRMN Self-Service from the State of Michigan Intranet* or from the Internet*. HRMN Self-Service was implemented on the Intranet in March 2001 and over the Internet in December 2002.

Expected benefits of Self-Service to employees and human resource managers include:

a. A single source providing benefits information, job postings, and training options for employees to use in making informed choices.

b. Employee responsibility for executing transactions, resulting in fewer errors and shorter cycle times.

c. Employees accessing current information more conveniently.

d. Employees' increased appreciation and satisfaction as a result of having access to their own information.

e. Employee and human resource manager initiation of transactions and inquiries.

Expected benefits of Self-Service to agencies include:

(a) Cost-savings in the areas of printing, distribution, customer service, and inquiries.

(b) Improved accuracy and completeness of data.

(c) Reduction of tedious tasks and paperwork.

** See glossary at end of report for definition.*

(d) Improved timeliness and consistency of information.

(e) Enhanced ability for human resources to focus on adding strategic value.

Executive Order* No. 2002-13 transferred the administration of State employee benefit programs to the Department of Civil Service (DCS). In addition, Executive Order No. 2002-19 established the executive direction and management of HRMN in DCS and allowed DCS to enter into a service level agreement with the Department of Information Technology (DIT) or any other executive branch agency to provide infrastructure support for HRMN.

DCS contracted with a third-party vendor to design a solution for providing secure access to HRMN Self-Service, which was completed in April 2000. The State contracted with another third-party vendor to perform a security analysis of the HRMN Self-Service Web architecture prior to making Self-Service accessible over the Internet, which was completed in August 2002. The primary objective of the security analysis was to evaluate the proposed network and system architecture for security vulnerabilities and provide recommendations to mitigate any identified risks.

As of September 2003, the total number of HRMN Self-Service user codes and passwords was approximately 61,000. DCS required State employees to use HRMN Self-Service when employees made changes to their benefits in August and September 2003.

** See glossary at end of report for definition.*

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of Human Resources Management Network (HRMN) Self-Service, Department of Civil Service (DCS), had the following objectives:

1. To assess the effectiveness* of security over HRMN Self-Service.

2. To assess the effectiveness of general controls over HRMN Self-Service.

Audit Scope

Our audit scope was to examine the information processing and other records of Human Resources Management Network Self-Service. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of HRMN Self-Service's information technology and other records primarily for the period April 2002 through September 2003. Our audit fieldwork was performed between April and September 2003. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We collected background information about HRMN Self-Service. We obtained an understanding of the internal control* pertaining to security over HRMN Self-Service. We used the results of our review to determine the extent of our detailed analysis and testing.

** See glossary at end of report for definition.*

2. Detailed Analysis and Testing Phase

We performed an assessment of internal control pertaining to security over HRMN Self-Service and general controls over HRMN Self-Service. Specifically, we assessed:

a. Effectiveness of Security Over HRMN Self-Service:

(1) We assessed the effectiveness of controls over access to HRMN Self-Service.

(2) We evaluated the configuration of the HRMN Self-Service Web application software.

(3) We assessed the Department of Information Technology's (DIT's) procedures for monitoring the security and performance of HRMN Self-Service.

b. Effectiveness of General Controls Over HRMN Self-Service:

(1) We assessed the configuration of operating system* controls pertaining to HRMN Self-Service.

(2) We observed and assessed controls pertaining to physical security over HRMN Self-Service hardware.

(3) We examined procedures for making and implementing program changes to HRMN Self-Service Web application software.

(4) We evaluated the configuration of the firewalls* pertaining to HRMN Self-Service.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

** See glossary at end of report for definition.*

Agency Responses

Our audit report contains 7 findings and 7 corresponding recommendations. The agency preliminary response indicated that DCS and DIT agreed with the 3 recommendations and 4 findings, respectively, pertaining to their operations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require DCS to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF SECURITY OVER HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) SELF-SERVICE

COMMENT

Background: Security policies and procedures over Web application resources help ensure the protection of sensitive and confidential information. Effective controls, such as access controls, Web application configuration controls, and security controls, and performance monitoring are needed to protect State employee personnel information from disclosure or alteration. The absence of these controls could result in unauthorized access to personnel data.

Audit Objective: To assess the effectiveness of security over HRMN Self-Service.

Conclusion: The Department of Civil Service (DCS) did not completely establish effective security over HRMN Self-Service. Our assessment disclosed three material conditions* related to State personnel data security, HRMN Self-Service access and password controls, and Web application security (Findings 1 through 3).

During our audit fieldwork, we reported to DCS management the detailed results of our review. This report summarizes the material control conditions we identified and the recommendations we made.

FINDING

1. State Personnel Data Security

DCS did not sufficiently evaluate and minimize the risk of providing confidential State employee and dependent data over the Internet through HRMN Self-Service. Appropriate evaluation and risk assessment would minimize vulnerabilities to the State and to State employees resulting from unauthorized access.

Generally accepted system security principles (GASSP), promulgated by the International Information Security Foundation, recommend that security measures be appropriate to the value of the data and the threats to which the data is vulnerable. Also, the Freedom of Information Act (Sections 15.231 - 15.246 of the

** See glossary at end of report for definition.*

Michigan Compiled Laws) protects certain personnel and dependent data from disclosure.

Using the Internet to access State employee and dependent data heightens the need for additional security measures. Specific things that DCS should do to evaluate and minimize security risks include:

a. Identifying the State's responsibilities and developing an action plan to respond to employee or dependent identity theft.

b. Conducting a risk assessment to evaluate the risks of providing confidential data over the Internet.

c. Implementing security banners to expressly prohibit unauthorized access to HRMN Self-Service. Banners inform anyone accessing the system that only authorized users are allowed and that unauthorized access is forbidden. Banners would aid in prosecuting an intruder by helping to establish that the intruder was aware that he or she was trespassing.

RECOMMENDATION

We recommend that DCS sufficiently evaluate and minimize the risk of providing confidential State employee and dependent data over the Internet through HRMN Self-Service.

AGENCY PRELIMINARY RESPONSE

DCS agreed with the recommendation and will continue to identify and document the acceptable level of risk over confidential State personnel data. DCS informed us that it has added security banners to HRMN Self-Service expressly prohibiting unauthorized access. In addition, DCS and the Department of Information Technology (DIT) will take actions as appropriate based on the recommended evaluation.

FINDING

2. HRMN Self-Service Access and Password Controls

DCS did not completely establish effective access and password controls over HRMN Self-Service. Effective access and password controls minimize the possibility of unauthorized users obtaining access to HRMN Self-Service data.

Department of Management and Budget (DMB) Administrative Guide procedures 1310.02 and 1410.17 provide guidance and requirements to State departments for developing and implementing access and password controls. We noted:

a. DCS did not establish a secure process for employees to create and change their personal identification number (PIN).

b. DCS did not implement strong access and password security controls as recommended by DMB Administrative Guide procedures.

   After we brought this to management's attention, DCS implemented changes to resolve one weakness.

c. DCS did not sufficiently assess the risks associated with the accessibility of information needed to change HRMN Self-Service passwords.

d. DCS did not ensure the security of password notifications.

   After we brought this to management's attention, DCS implemented changes to improve controls over password notifications.

e. DCS did not sufficiently ensure that HRMN Self-Service authentication* protects against security vulnerabilities.

RECOMMENDATION

We recommend that DCS completely establish effective access and password controls over HRMN Self-Service.

** See glossary at end of report for definition.*

AGENCY PRELIMINARY RESPONSE

DCS agreed with the recommendation and informed us that it immediately implemented changes addressing effective access and password controls. In addition, DCS and DIT will continue to assess the system to ensure that it complies with evolving State security policies, procedures, and processes.

FINDING

3. Web Application Security

DCS had not developed and implemented sufficient Web application security controls. Without the implementation of sufficient Web application security controls, personnel data and Web application resources are vulnerable to intrusion or misuse.

The U.S. Federal Trade Commission recommends that all entities use the Open Web Application Security Project's (OWASP's) Top Ten Vulnerabilities list as the standard for Web application security. OWASP identifies the most serious vulnerabilities in Web security. OWASP states that a secure Web site includes both secure software and a secure configuration. The HRMN Self-Service Web application does not have the level of security suggested by OWASP for systems that are on the Internet. We noted:

a. DCS did not securely configure the HRMN Web application.

b. DCS did not completely implement monitoring tools for the Web application. DCS and DIT had developed and implemented some audit logs; however, DCS and DIT should enhance the logs to allow additional monitoring of the Web application.

c. DCS did not conduct periodic vulnerability scanning of the Web application. OWASP recommends that a vulnerability scanning tool be used at least monthly on a Web application to detect vulnerabilities in the Web application and operating system.

DCS and DIT had developed and implemented some security enhancements to HRMN Self-Service. However, DCS should continue to work with DIT and the software vendor to improve Web application security.

RECOMMENDATION

We recommend that DCS develop and implement additional Web application security controls.

AGENCY PRELIMINARY RESPONSE

DCS agreed with the recommendation. DCS and DIT informed us that they continue to review the HRMN Self-Service access control process and take appropriate actions to ensure that they meet State security policies, standards, and procedures.

EFFECTIVENESS OF GENERAL CONTROLS OVER HRMN SELF-SERVICE

COMMENT

Background: General controls are the policies and procedures that apply to a department's overall computer operations. The purpose of establishing general controls is to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued computer operations in case of unexpected interruptions. Although general controls are normally independent of individual computer applications, they provide the framework within which many different applications are processed. Therefore, weaknesses in general controls can adversely affect all of a department's automated information systems.

Audit Objective: To assess the effectiveness of general controls over HRMN Self-Service.

Conclusion: DIT's general controls over HRMN Self-Service were reasonably effective. However, we identified reportable conditions* related to operating system configuration, operating system access controls, physical security, and program change controls (Findings 4 through 7).

** See glossary at end of report for definition.*

FINDING

4. Operating System Configuration

DIT had not established controls over the operating system configuration. The operating system should be installed with a minimal service configuration to reduce the risk of intrusion and the exploitation of well-known operating system vulnerabilities.

In accordance with guidance provided by Carnegie Mellon Software Engineering Institute's CERT Coordination Center, a recognized security organization, only the essential operating system services should be enabled to enhance the operating system security.

Our review of 3 HRMN Self-Service file servers disclosed that DIT had installed many unnecessary services and had not properly secured configuration files. Many of these services have known exploits and vulnerabilities associated with them. Removing or disabling these services would reduce the risk that an unauthorized user could gain access to the system. A security analysis performed by a third-party vendor also recommended that some of these services be disabled.

In addition, DIT had not established policies and standards to support and describe how the operating systems have been and should be configured for 2 of the 3 file servers. Policies and standards should identify critical and sensitive operating system files and establish a baseline configuration for the files. Documenting and establishing a baseline configuration will help ensure that all systems are securely configured and will aid in the detection of unauthorized changes to the system.

RECOMMENDATION

We recommend that DIT establish controls over the operating system configuration.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding. DIT and DCS informed us that they will take action to establish stronger controls over network operating system configuration.

FINDING

5. Operating System Access Controls

DIT had not established complete operating system access controls. This could result in unauthorized modification, loss, or disclosure of confidential State employee data.

Access controls protect information and resources from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. Effective controls include granting access to data, program, and system files only to the extent necessary for individuals to perform their assigned duties. Our review of operating system access for 3 HRMN Self-Service file servers disclosed:

a. DIT did not restrict permissions for privileged accounts for 2 of the 3 file servers. DIT should restrict permissions to the privileged accounts to prevent unauthorized access to the operating system.

b. DIT did not use unique network administrator user codes for 2 of the 3 file servers. The use of unique user codes by the network administrators allows for accountability for changes to the operating system.

c. DIT did not establish access controls over server configuration files for all 3 file servers reviewed. A security analysis performed by a third-party vendor also recommended more restrictive access for 1 of the file servers. DIT immediately corrected the file access for 1 file after we brought it to DIT's attention. DIT should review configuration file access and modify those files with excessive rights.

d. DIT did not monitor the audit logs for 2 of the 3 file servers. In addition, DIT did not enable the audit logs to monitor for invalid access attempts for 2 of the 3 file servers. An important task in keeping a computer system secure is monitoring for unauthorized access, network administrator activity, and security related problems. Audit logs provide information about which systems have been attacked and compromised. Audit logs also provide useful information to monitor system performance and to track problems. After we brought this to management's attention, DIT activated audit logs on these file servers.

e. DIT did not require network administrators to periodically change their network passwords for 2 of the 3 file servers. DMB Administrative Guide procedure 1310.02 requires periodic changing of passwords. Changing passwords on a periodic basis helps to ensure password confidentiality and reduces the risk of unauthorized access to the system.

f. DIT did not automatically disconnect computer workstations or use password-protected screen savers after a reasonable period of inactivity for all 3 file servers reviewed. This could result in unauthorized system access if a workstation is left unattended. DMB Administrative Guide procedure 1310.02 requires that workstations automatically log off if left unattended for a specific period of time.

RECOMMENDATION

We recommend that DIT establish complete operating system access controls.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding. DIT and DCS informed us that they will take action to establish stronger controls over network operating system access controls.

FINDING

6. Physical Security

DIT had not established complete physical security controls over HRMN Self-Service resources. Physical security controls help ensure that valuable system resources are safeguarded and that access is limited to individuals responsible for managing the system.

Our review of physical security controls for 2 locations disclosed:

a. DIT did not establish procedures for the periodic review of the computer room access list at 1 of the 2 locations. DIT issued access cards to four individuals who did not need access to perform their job. In addition, another individual was issued two access cards. Access to the computer room should be limited to operations personnel. Periodically reviewing the computer room access list would help DIT ensure that access to the computer room is granted to only authorized individuals.

b. DIT did not have a process to track the assignment of temporary access cards issued at 1 of the 2 locations. Developing and implementing a process to track the assignment of temporary access cards would provide enhanced accountability over the cards and access to the computer room.

c. DIT did not prepare a disaster recovery plan for its computer room for 1 of the 2 locations. The plan should contain procedures for recovery from disaster, such as fire, tornado, or sabotage, and should identify the materials, personnel, equipment, and communication systems necessary to process HRMN Self-Service at another facility. Completing a disaster recovery plan may help reduce system downtime and aid in the recovery of data.

RECOMMENDATION

We recommend that DIT establish complete physical security controls over HRMN Self-Service resources.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding. DIT and DCS informed us that they will take action to strengthen physical security controls over HRMN Self-Service resources.

FINDING

7. Program Change Controls

DIT should strengthen controls over program changes to HRMN Self-Service. Program change controls help ensure that only authorized, tested, and approved program modifications are implemented and that access to and distribution of programs are carefully controlled.

Our review disclosed:

a. DIT did not maintain previous versions of HRMN Self-Service application and Web page source code on the network. Maintaining versions of programs is important in the event that a program needs to be restored because of errors in the current version.

b. DIT had not established HRMN Self-Service application and Web page version controls. As a result, DIT did not number its program versions and

maintain a history of program changes. Library control software would provide a mechanism for maintaining numbered program versions and provide a means for management to log and monitor when the source code was copied or changed.

c. DIT had not established strong access permissions on program files. DIT should review the file permissions and modify those with excessive rights.

RECOMMENDATION

We recommend that DIT strengthen controls over program changes to HRMN Self-Service.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding. DIT informed us that it has begun, and will continue, to develop and implement tools, processes, and procedures to improve controls over program changes to HRMN Self-Service.

GLOSSARY

Glossary of Acronyms and Terms

authentication	Verification of identity as a security measure. Passwords and digital signatures are forms of authentication.
DCS	Department of Civil Service.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.
effectiveness	Program success in achieving mission and goals.
executive order	An official pronouncement of the Governor provided for in Article V, Section 2 of the State Constitution.
firewall	A hardware and/or software boundary that prevents unauthorized users from accessing restricted files on a network. The part of the network that is not protected by the firewall is available to whoever logs on.
HRMN Self-Service	A component of HRMN. HRMN Self-Service is a Web-based automated system used by State employees and human resource managers to enable employees to maintain their own employee benefit and other personnel information.
Human Resources Management Network (HRMN)	The State's integrated human resources system that processes personnel, payroll, and employee benefits data for the Michigan Administrative Information Network Human Resources System (MAIN HRS).
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial

	reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding or agency assets against unauthorized acquisition, use, or disposition.
Internet	The worldwide information highway composed of thousands of interconnected computer networks.
Intranet	An internal local area network that may not be connected to the Internet, but which has similar functions. Some organizations set up worldwide Web servers on their own internal networks so employees have access to the organization's Web documents.
material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
operating system	The main control program of a computer that schedules tasks, manages storage, and handles communication with peripherals.
OWASP	Open Web Application Security Project.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.