MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT ON

HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) SELF-SERVICE

CIVIL SERVICE COMMISSION

October 2007

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

191-0596-03F

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 can be accessed at:
http://audgen.michigan.gov

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

October 12, 2007

Mr. Bryan J. Waldman, Chair
and
Mr. James D. Farrell, State Personnel Director
Civil Service Commission
Capitol Commons Center
Lansing, Michigan

Ms. Lisa Webb Sharpe, Director
Department of Management and Budget
Lewis Cass Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Waldman, Mr. Farrell, Ms. Webb Sharpe, and Ms. Takai:

This is our report on our follow-up of the 3 material findings (Findings 1 through 3) and 3 corresponding recommendations reported in the performance audit of Human Resources Management Network (HRMN) Self-Service, Department of Civil Service. That audit report was issued and distributed in July 2004; however, additional copies are available on request or at <http://www.audgen.michigan.gov>. Subsequent to our original audit, Executive Order No. 2007-30 abolished the Department of Civil Service and transferred the Civil Service Commission, as an autonomous entity, to the Department of Management and Budget.

Our follow-up disclosed that the Civil Service Commission, in conjunction with the Department of Information Technology, had partially complied with the 3 recommendations.

If you have any questions, please call me or Scott M. Strong, C.P.A., C.I.A., Deputy Auditor General.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

HUMAN RESOURCES MANAGEMENT NETWORK (HRMN)

SELF-SERVICE

CIVIL SERVICE COMMISSION

FOLLOW-UP REPORT

HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) SELF-SERVICE CIVIL SERVICE COMMISSION FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material findings and corresponding recommendations and the agency's preliminary response as reported in our performance audit report of Human Resources Management Network (HRMN) Self-Service, Department of Civil Service (DCS) (19-596-03), which was issued and distributed in July 2004. That audit report included 3 material conditions (Findings 1 through 3) and 4 other reportable conditions.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Civil Service Commission (CSC), in conjunction with the Department of Information Technology (DIT), has taken appropriate corrective measures in response to the 3 material findings and 3 corresponding recommendations.

BACKGROUND

Self-Service is a component of 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.

In December 2002, Executive Order No. 2002-19 established the executive direction and management of HRMN Self-Service in DCS and allowed DCS to enter into a service level agreement with DIT.

In August 2007, subsequent to our original audit, Executive Order No. 2007-30 abolished DCS and transferred CSC, as an autonomous entity, to the Department of Management and Budget.

SCOPE

Our fieldwork was performed from April through June 2007. We interviewed employees from CSC and DIT to determine the status of compliance with our audit recommendations. We reviewed policies and procedures related to State personnel data security, HRMN Self-Service access and password controls, and Web application security.

FOLLOW-UP RESULTS

EFFECTIVENESS OF SECURITY OVER HRMN SELF-SERVICE

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2004:

1. State Personnel Data Security

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 DIT will take actions as appropriate based on the recommended evaluation.

FOLLOW-UP CONCLUSION

We concluded that CSC had partially complied with this recommendation. Specifically, our follow-up disclosed:

a. CSC had not formally identified its responsibilities or developed an action plan to respond to employee identity theft. However, CSC informed us that it has developed informal policies and procedures identifying its responsibilities and action plan to respond to employee identity theft and is working toward formally documenting them.

b. CSC had not documented a formalized risk assessment process to evaluate, on a periodic basis, the risk of providing confidential data over the Internet. In addition, CSC had not developed policies and procedures or assigned responsibility for conducting risk assessments. However, CSC has incorporated an informal risk identification and mitigation process into its system development process. Also, CSC conducts monthly meetings with DIT to discuss security concerns.

c. CSC implemented security banners to expressly prohibit unauthorized access to HRMN Self-Service.

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2004:

2. HRMN Self-Service Access and Password Controls

RECOMMENDATION

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

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.

FOLLOW-UP CONCLUSION

We concluded that CSC had partially complied with this recommendation. Specifically, our follow-up disclosed:

a. CSC discontinued the use of the personal identification number process to request and obtain passwords. CSC implemented a secret identifying name process that, in conjunction with other required personal data, allows a user to securely request that a password notification be sent to his/her home address.

b. CSC had not fully implemented strong access and password security controls as recommended by Department of Management and Budget Administrative Guide procedures. However, CSC had prevented the display of passwords during entry, required the use of special characters within the password composition, stored passwords in an encrypted format, and transferred passwords in an encrypted format between its systems. Also, CSC informed us that it is continuing to work with the software vendor to address strengthening the software related to password controls.

c. CSC assessed the risks associated with the accessibility of information needed to change HRMN Self-Service passwords. CSC worked with the agencies responsible for issuing employee identification cards to remove the display of confidential employee information.

d. CSC improved the security of password notifications by changing the password notification process. CSC sends password notifications only to an employee's home address instead of e-mailing password notifications to an unsecured e-mail account.

e. CSC did not fully ensure that HRMN Self-Service authentication protects against certain security vulnerabilities. However, CSC has developed a risk mitigation plan for these security vulnerabilities.

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2004:

3. 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.

FOLLOW-UP CONCLUSION

We concluded that CSC had partially complied with this recommendation. CSC and DIT had developed and implemented some security controls over the HRMN Web application. However, CSC should continue to work with DIT and the software vendor to improve Web application security. Specifically, our follow-up disclosed:

a. CSC did not fully secure the HRMN Web application. Although CSC securely configured some parts of the Web application, CSC did not address all of the weaknesses noted in the audit. However, CSC informed us that it is working with the software vendor to address these weaknesses.

b. DIT implemented intrusion detection monitoring tools and reviewed system logs as part of its Statewide security process, including monitoring of the HRMN Web application.

c. DIT conducted periodic vulnerability scans of the State's network to comply with procurement card industry standards. These vulnerability scans included scans of the HRMN Web application.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN · OFFICE of the AUDITOR GENERAL ·