MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY

DEPARTMENT OF MANAGEMENT AND BUDGET

August 2005

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

07-598-01F

"...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

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

August 2, 2005

Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Ms. Takai:

This is our report on our follow-up of the 3 material findings (Findings 1 through 3) and 4 related recommendations reported in the performance audit of Telecommunication Services and Enterprise Security, Department of Management and Budget. That audit report was issued and distributed in March 2002; however, additional copies are available on request or at <http://www.audgen.michigan.gov>. Subsequent to our original audit, Executive Order No. 2001-3 transferred the responsibility for all information technology services to the Department of Information Technology.

Our follow-up disclosed that the Department of Information Technology had complied with the 4 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

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY
DEPARTMENT OF MANAGEMENT AND BUDGET
FOLLOW-UP REPORT

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY DEPARTMENT OF MANAGEMENT AND BUDGET FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material findings and related recommendations and the agency's preliminary response as reported in our performance audit report of Telecommunication Services and Enterprise Security, Department of Management and Budget (DMB) (#0759801), which was issued and distributed in March 2002. That audit report contained 3 material findings (Findings 1 through 3) and 12 other reportable conditions.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Information Technology (DIT) had taken appropriate corrective measures in response to the 3 material findings and 4 related recommendations.

BACKGROUND

Subsequent to our original audit, Executive Order No. 2001-3 transferred the responsibility for all information technology services to DIT. The mission of DIT is to provide effective solutions, through skilled and valued employees, in its partnership with its clients. DIT is responsible for securing the State's data network, which is used for conducting State business and exchanging information among State agencies, State employees, citizens, and other stakeholders.

SCOPE

Our fieldwork was completed during April 2005. We interviewed network security personnel. We reviewed policies and procedures related to network security, vulnerability assessments and penetration testing, and the firewall rulebase. We tested DIT's compliance with selected policies and procedures.

FOLLOW-UP RESULTS

EFFECTIVENESS OF THE STATE'S DATA NETWORK

RECOMMENDATIONS AND RESPONSE AS REPORTED IN MARCH 2002:

1. Network Security Policy

RECOMMENDATIONS

We recommend that DMB ensure that the State's network security policy completely addresses important security issues.

We also recommend that DMB clearly define and assign responsibility for enforcement of the network security policy.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the recommendations. However, DMB believes that the State addresses security issues on a continuous basis as reflected in the number of employees assigned to oversee various security functions and through the active participation of the Enterprise Security Oversight Committee. DMB is finalizing the process of updating and implementing 20 Internet security standards. In addition, DMB informed us that implementation of the Michigan portal was accomplished without any security breaches because of the extensive security enhancements made between January and July 2001.

FOLLOW-UP CONCLUSION

We concluded that DIT had complied with these recommendations.

In regard to the first recommendation, DIT developed policies and procedures that help reduce the risk of unauthorized access and unauthorized disclosure of protected information as well as maintain resource accountability. DIT has expanded and strengthened its network policies and procedures over the firewall rulebase, Internet access, privacy, e-mail, Web page banners, passwords, network monitoring, and intrusion detection. Additionally, DIT developed policies and procedures for advancing technologies used by the State including wireless and virtual private network access.

In regard to the second recommendation, DIT has established a charter for Enterprise Security that gives it the authority to enforce the State's information technology security standards, including the authority to remove access to or to take possession of information technology resources.

RECOMMENDATION AND RESPONSE AS REPORTED IN MARCH 2002:

2. Vulnerability Assessment and Penetration Testing

RECOMMENDATION

We recommend that Enterprise Security conduct a risk assessment to determine the extent of and frequency for performing vulnerability assessments and penetration testing of the network perimeter.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the recommendation and informed us that it routinely conducts vulnerability scans of key network components and servers as part of the change management control process. DMB believes that its vulnerability scans have been effective in reducing its overall level of risk. In addition, DMB has worked with State agencies to provide them the tools they need to conduct agency risk assessments of their networks and services, while Enterprise Security has focused on information technology resources that have more of an enterprise mission. DMB informed us that this recommendation complements the actions it is taking and will be tempered only by the availability of resources.

FOLLOW-UP CONCLUSION

We concluded that DIT had complied with this recommendation.

DIT implemented Policy 100.15 (Risk Management), which created a framework for assessing infrastructure risks and identifying threats to the network. The policy requires an independent network vulnerability assessment to be conducted periodically to locate vulnerabilities as well as penetration testing to determine whether the vulnerabilities could be exploited.

DIT contracted with outside vendors to provide independent network vulnerability assessments to locate vulnerabilities of the network. In 2002, Enterprise Security

contracted with UNYSIS Enterprise Security Services to conduct an enterprise level security assessment identifying weaknesses and vulnerabilities in the State's network and supporting infrastructure. UNYSIS Enterprise Security Services provided a security related incident tracking database that identified threats to the State's network. Furthermore, in January 2005, Enterprise Security contracted with Eastern Michigan University to provide an analysis of risks that includes an enterprise-wide network-based vulnerability assessment. Also, DIT has received funds from the U.S. Department of Homeland Security for penetration testing and is moving forward with the testing to identify network vulnerabilities.

RECOMMENDATION AND RESPONSE AS REPORTED IN MARCH 2002:

3. Firewall Rulebase

RECOMMENDATION

We recommend that Telecommunication Services continue to configure its firewalls to increase the security of the State's data network.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the recommendation and informed us that it continues to configure its firewalls to increase the security of the State's data network. DMB informed us that, over the past 18 months, it has installed more robust firewalls, rules have been refined, rule additions for internal servers have been restricted, extranet firewalls have been added, and a demilitarized zone (DMZ) project for publicly accessible servers has been initiated.

FOLLOW-UP CONCLUSION

We concluded that DIT had complied with this recommendation.

DIT strengthened its controls over the firewall by developing DMB Administrative Guide procedure 1350.80 (Firewall and SOM-NET [State of Michigan Network] Perimeter Security Standard), which defines the management of the firewall rulebase. Procedure 1350.80 established a firewall rule request process that included a separation of duties requiring Enterprise Security to approve all firewall

rules and firewall rule changes that are implemented by Telecommunication Services. Enterprise Security further strengthened firewall rulebase controls by developing procedures for logging and periodic auditing of the firewall rulebase to help reduce the risks to the State's data network.

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