

EXECUTIVE DIGEST

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY

INTRODUCTION

This report, issued in March 2002, contains the results of our performance audit* of Telecommunication Services and Enterprise Security, Department of Management and Budget (DMB).

AUDIT PURPOSE

This performance audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*.

BACKGROUND

Telecommunication Services is an organizational component of the office of the Chief Information Officer for the State of Michigan. The mission* of Telecommunication Services is to provide telecommunication services efficiently and economically in support of State government objectives. Telecommunication Services provides State agencies with data, voice, video, and radio networks. The scope of this audit consisted of the data network services provided by Telecommunication Services. Data network services include the Lansing Metropolitan Area Network (LMAN), a wide area network (WAN), Internet*, intranet*, firewall* and network security, network monitoring, and e-mail.

Telecommunication Services receives revenue from customer billings for services provided. For fiscal year 1999-2000, Telecommunication Services had revenue of approximately \$22.7 million and 41.5 full-time equated positions for data network services.

Enterprise Security is an organizational component of Computing Services, under the office of the Chief Information Officer for the State of Michigan. Enterprise Security works with Telecommunication Services to help ensure the security of the data network. The mission of Enterprise Security is to provide the highest level of security possible to protect the integrity of State computing resources and instill and maintain the confidence and trust of all customers of these services.

**AUDIT OBJECTIVE
AND CONCLUSION**

Audit Objective: To assess the effectiveness of Telecommunication Services and Enterprise Security in providing a secure environment for the operation of the State's data network.

Conclusion: Telecommunication Services and Enterprise Security were not effective in providing a secure environment for the operation of the State's data network. Our assessment disclosed three material conditions*:

- DMB did not ensure that the State's network security policy completely addressed important security issues. In addition, DMB did not clearly define and assign responsibility for enforcement of the network security policy. (Finding 1)

DMB agreed with the corresponding 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.

- Enterprise Security had not conducted a risk assessment to determine the extent of and frequency for performing vulnerability assessments and penetration testing of the network perimeter (Finding 2).

DMB agreed with the corresponding recommendation and informed us that it routinely conducts vulnerability scans as part of the change management control process. DMB believes that its vulnerability scans have been effective in reducing its overall level of risk.

- Telecommunication Services had not configured its firewalls to increase the security of the State's data network (Finding 3).

DMB agreed with the corresponding recommendation and informed us that it continues to configure its firewalls to increase the security of the State's data network.

In addition, we identified reportable conditions* related to operating system configuration, operating system access, the demilitarized zone* (DMZ), remote access*, network monitoring, the Domain Name System* (DNS), firewall testing, firewall change controls, firewall separation of duties, firewall practices and procedures, backup and recovery controls, and contingency planning (Findings 4 through 15).

Agency Response: DMB did not believe that sufficient data was presented to support claims that the State's data network is ineffective and at risk of being compromised. DMB did not agree with the classification of Findings 1 through 3 as material conditions. It believes that the findings did not show a pattern of undue exposure, did not constitute a serious risk to the integrity of the State's data, and, therefore, did not warrant classification as material conditions.

Epilogue: The classification of Findings 1 through 3 as material was based on the missions of Telecommunication Services and Enterprise Security, which are to provide secure telecommunication services. Because Telecommunication Services and Enterprise Security had not developed a complete network security policy (Finding 1), had not identified and tested vulnerabilities of the network (Finding 2), and had not securely configured the firewall (Finding 3), it is our opinion that they cannot ensure that the State's network is adequately protected to minimize both the likelihood and impact of security incidents.

**AUDIT SCOPE AND
METHODOLOGY**

Our audit scope was to examine the information technology and other records of Telecommunication Services and Enterprise Security, Department of Management and Budget. 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.

Our methodology included examination of Telecommunication Services' and Enterprise Security's information technology and other records, generally, for

the State's data network for the period November 2000 through April 2001.

AGENCY RESPONSES

Our audit report contains 15 findings and 16 corresponding recommendations. The agency preliminary response indicated that DMB has complied or will comply with all of the recommendations.