PERFORMANCE AUDIT

OF

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY

DEPARTMENT OF MANAGEMENT AND BUDGET

March 2002

07-598-01

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.

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

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

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

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).

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

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.

This page left intentionally blank.

March 4, 2002

Mr. Duane Berger, Director
Department of Management and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Berger:

This is our report on the performance audit of Telecommunication Services and Enterprise Security, Department of Management and Budget.

This report contains our executive digest; description of agency; audit objective, scope, and methodology and agency responses; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

The agency preliminary responses were taken from the agency's 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 this audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

TELECOMMUNICATION SERVICES AND ENTERPRISE SECURITY
DEPARTMENT OF MANAGEMENT AND BUDGET

INTRODUCTION

COMMENT, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Telecommunication Services

Telecommunication Services, Department of Management and Budget, is an organizational component of the office of the Chief Information Officer for the State of Michigan. Telecommunication Services was established by Sections 18.1269 and 18.1271 of the *Michigan Compiled Laws* and reprised in Executive Order No. 1995-10 for the purpose of providing telecommunication services to the executive branch agencies.

The mission of Telecommunication Services is to provide telecommunication services efficiently and economically in support of State government objectives. Some of the primary responsibilities of Telecommunication Services include providing State agencies with design, installation, and maintenance of data, voice, video, and radio networks as well as support of agency development and production systems through the enterprise help desk. 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

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, Scope, and Methodology and Agency Responses

Audit Objective

Our audit objective for the performance audit of Telecommunication Services and Enterprise Security, Department of Management and Budget (DMB), was to assess the effectiveness of Telecommunication Services and Enterprise Security in providing a secure environment for the operation of the State's data network.

Audit Scope

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.

Audit Methodology

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. Our audit fieldwork was performed between November 2000 and April 2001. To accomplish our audit objective, our audit methodology included the following phases:

1. Data Gathering Phase

   We collected background information about Telecommunication Services, Enterprise Security, and the State's data network. We identified the data network-related services provided to State agencies and performed an assessment to identify those services that were most critical to the security, integrity, and availability of the network. We obtained an understanding of the internal control* pertaining to the data network.

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

2. Detailed Analysis and Testing Phase

We performed an assessment of internal control pertaining to the security of the State's data network. Specifically:

(a) We examined policies and procedures for the management and security of the data network.

(b) We observed and assessed the security of the network, including physical and logical access controls.

(c) We evaluated the configuration of the firewall and selected services, file servers*, and operating system software.

(d) We assessed the effectiveness of standards and procedures over firewall changes.

(e) We assessed controls over the Domain Name System (DNS).

(f) We evaluated procedures for monitoring the security and performance of the network.

3. Evaluation and Reporting Phase

We evaluated the controls in place over the data network against industry standards for information technology. These standards include Generally Accepted Principles and Practices for Securing Information Technology Systems, published by the National Institute of Standards and Technology (NIST); Telecommunication Security Guidelines, published by NIST; Security Improvement Modules, Security Practices, and Technical Implementations, published by the Carnegie Mellon Software Engineering Institute's CERT Coordination Center; and standards established by the Internet Engineering Task Force (IETF). We reported on the results of the detailed analysis and testing phase.

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.

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

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

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF THE STATE'S DATA NETWORK

COMMENT

Background: The State's data network is used for conducting State business and exchanging information among State agencies, State employees, citizens, and other stakeholders. The data network consists of the Lansing Metropolitan Area Network (LMAN), a wide area network (WAN), and agency local area networks. LMAN and WAN connect approximately 23 Lansing area buildings and 500 locations throughout the State. The network was intended to have secure, controlled connection to the Internet. Telecommunication Services is responsible for securing the perimeter of the network and uses firewall and other technology to provide security. Enterprise Security assists Telecommunication Services in securing the network perimeter by approving firewall changes, monitoring network security, and consulting on network security issues.

A network is a group of connected computers, including the hardware and software used to connect them. Effective controls, such as a security policy, firewalls, and network monitoring, are needed to provide a secure network. The absence of these controls can adversely affect the reliability and security of a network.

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 related to network security policy, vulnerability assessment and penetration testing, and firewall rulebase*. 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,

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

firewall separation of duties, firewall practices and procedures, backup and recovery controls, and contingency planning.

Agency Response: The Department of Management and Budget (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. Telecommunication Services indicated that there has not been, nor is there a serious potential of, a major security breach, compromise, loss of data, or significant downtime of the State's data network. Telecommunication Services believes that this is due to a continuous program of security, architectural, operational, and procedural enhancements.

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. DMB stated that, in the majority of cases, its responses to our findings indicate agreement with the recommendations because the recommendations echo DMB's stated objectives and normal operating processes. DMB also stated that it believes that delivery of successful security and telecommunication services is a dynamic environment in which nothing can be taken for granted, is ever changing, and needs constant refinement. The delivery of services can always be improved and is a principal driver for DMB.

Epilogue: 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 could not ensure that the State's network is adequately protected to minimize both the likelihood and impact of security incidents.

The classification of Findings 1 through 3 as material was based on the mission of Telecommunication Services, which is to provide telecommunication services efficiently and economically in support of State government objectives, and the mission of Enterprise Security, which 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.

FINDING

1. Network Security Policy

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.

The first step in protecting a network is to establish a security policy that addresses each component of computer security. Establishing and implementing a security policy provide a preventative mechanism for protecting important data and processes. A network security policy communicates a coherent security standard to users, management, and technical staff and defines the expectations of proper network use and procedures to prevent and respond to security incidents. It also identifies the threats against which protection is required and defines the required level of protection. DMB Administrative Guide procedure 1410.17 is the State's network security policy.

In accordance with industry accepted standards and guidance provided by recognized security organizations, such as the SANS Institute and the CERT Coordination Center, some items that DMB should expand its security policy to include are: Internet access policy, privacy policy, e-mail policy, web page banner policy, network monitoring policy, and computer technology purchasing guidelines. DMB should update and strengthen the following items of its security policy: firewall policy, intrusion detection policy, and password policy.

Upon expanding and strengthening its network security policy, DMB should explicitly assign the responsibility for enforcement of the policy. DMB should also define procedures to be followed to escalate policy-related conflicts to ensure that security issues are resolved in a timely manner.

Our audit identified several network security weaknesses that were also reported in a security audit conducted in 1996 by Trusted Information Systems (TIS). DMB has taken minimal steps toward resolving the security issues identified by TIS. Establishing a complete network security policy and assigning responsibility for enforcement of this policy would help ensure that the weaknesses identified in this report and in the TIS report are resolved in a timely manner and in accordance with the 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.

FINDING

2. Vulnerability Assessment and Penetration Testing

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.

An independent network vulnerability assessment should be conducted periodically to help network administrators locate vulnerabilities of the network before hackers do. These assessments should be done on a regular basis or when network changes are implemented. Next, penetration testing should be conducted to determine whether the discovered vulnerabilities can be exploited.

Enterprise Security should conduct a risk assessment of its network operations to identify and prioritize their security risks. After this risk assessment is conducted, Telecommunication Services should determine how often and to what extent it needs to conduct vulnerability assessments and penetration tests to provide assurance to customers and business partners that their sensitive information is secure.

All State agencies rely on Telecommunication Services to provide a reliable and secure network on which they conduct their information technology operations. These operations include conducting business through public web sites, intranets, and e-mail. Industry standards suggest that network vulnerability assessments and penetration testing be conducted periodically and prior to implementing new applications to ensure the security of the network.

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.

FINDING

3. Firewall Rulebase

Telecommunication Services had not configured its firewalls to increase the security of the State's data network.

A firewall serves as the primary line of defense against external threats and vulnerabilities to computer systems, networks, and critical information. All traffic to the State's internal network should pass through the firewall, and only authorized traffic should be allowed to pass through. When the State's network is connected to the Internet without adequate firewall security measures in place, the network becomes vulnerable to attacks from external adversaries.

In our audit, we identified several areas in which the State's firewall rules could be strengthened. Subsequent to our bringing this matter to management's attention, Telecommunication Services implemented changes to address several weaknesses in the firewall rules.

This finding was also noted in a security audit conducted in 1996 by TIS, and it was recommended that the number of exceptions through the firewall be reduced.

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 DMZ project for publicly accessible servers has been initiated.

FINDING

4. Operating System Configuration

Telecommunication Services had not fully established controls and documentation for network operating system configuration.

The operating system should be installed with a minimal service configuration to reduce the risk of network intrusion and the exploitation of well-known operating system vulnerabilities. In addition, a well-secured operating system helps provide a stable platform on which to run the firewall and other software.

Our review of the configuration of three systems identified vulnerable operating system configurations and variances in the way administrators configured the operating systems. In addition, Telecommunication Services had not prepared documentation to support and describe how the operating systems have been and should be configured for optimum security.

This weakness was also noted in a security audit conducted in 1996 by TIS, and it was recommended that unnecessary services be removed from the operating system.

RECOMMENDATION

We recommend that Telecommunication Services fully establish controls and documentation for network operating system configuration.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the recommendation and will comply. DMB informed us that documentation of a fully developed control process, including a minimum service configuration checklist, has been initiated and will be completed by March 31, 2002. In addition, DMB informed us that the servers reviewed during the audit have had new network operating system software installed and have been reconfigured.

FINDING

5. Operating System Access

Telecommunication Services had not completely established, documented, and implemented internal policies and procedures for operating system access.

Our review of three systems disclosed:

a. Telecommunication Services did not limit access to sensitive network operating system files. Access to network operating system files should be restricted to network administrators. Limiting access to only network administrators will help ensure the integrity of critical or sensitive operating system files and configuration settings.

b. Password management features had not been implemented. Strong password controls on user and administrative accounts will help prevent unauthorized system access.

RECOMMENDATION

We recommend that Telecommunication Services completely establish, document, and implement internal policies and procedures for operating system access.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the recommendation and will comply. Password control and aging processes are under development and present permissions are being reviewed.

FINDING

6. Demilitarized Zone (DMZ)

Telecommunication Services should continue its efforts in developing and protecting the DMZ.

The DMZ is a network added between the unsecured external network (the Internet) and the State's protected internal network. The DMZ is important in providing an additional layer of protection to the internal network from outside attacks.

Our review of the DMZ disclosed weaknesses over the location of publicly available web servers and firewall protection on the DMZ. During our audit, Telecommunication Services and Enterprise Security were working on a project to expand the DMZ and the security it provides.

RECOMMENDATION

We recommend that Telecommunication Services continue its efforts in developing and protecting the DMZ.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and informed us that it has complied with the recommendation. DMB informed us that a project to enhance the DMZ was underway before the audit. All new public servers are being placed in the DMZ. Since October 2000, DMB has worked with multiple departments to reconfigure, move, or add network connectivity to bring their existing public servers into compliance. This project is intended for completion in early 2002. In addition, in July 2001, Enterprise Security sponsored a standards process request for a new policy for DMZ operations. The standard was presented and adopted at the January 2002 Information Management Policy Advisory Committee (IMPACT) meeting of the State's chief information officers.

FINDING

7. Remote Access

Telecommunication Services should continue its efforts to ensure that State agencies adopt the State's remote access system.

Implementing controls over remote access will help ensure that only authorized users have access to the State's network. DMB Administrative Guide procedure 1410.17 requires that State agencies remove existing network dial-in products after DMB implements a centralized dial-in service. Telecommunication Services implemented SecurID, a centralized dial-in service, in 1997. While some agencies use SecurID, the use of insecure remote access methods continues.

Telecommunication Services and Enterprise Security informed us that they did not have the authority to enforce the remote access policy. They rely on each agency's chief information officer to ensure compliance with the remote access policy. In addition, agencies can purchase and install telecommunications equipment that does not conform to the remote access policy without Telecommunication Services' knowledge.

DMB should better define the roles and responsibilities of Telecommunication Services, Enterprise Security, and agencies to help ensure compliance with the remote access policy.

This weakness was also noted in a security audit conducted in 1996 by TIS, and it was recommended that dial-in connections be eliminated.

RECOMMENDATION

We recommend that Telecommunication Services continue its efforts to ensure that State agencies adopt the State's remote access system.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and informed us that it continues its efforts to identify and secure unauthorized connections to the State's network.

FINDING

8. Network Monitoring

Telecommunication Services and Enterprise Security had not fully established and implemented policies and procedures for network monitoring.

Network monitoring is the process of detecting unauthorized or inappropriate use of a system. Network monitoring is usually accomplished through the use of intrusion detection software and other tools, such as system logs and alarms. Events that can be monitored include signs of network intrusion or misuse, changes to important files on the firewall system, unusual network traffic patterns, and attempts to gain administrative access to the operating system.

Enterprise Security conducted some network and firewall monitoring; however, more regular and timely monitoring may be necessary. Industry standards suggest that an initial risk assessment be completed to identify the threats to the network, establish the types and frequency of monitoring that should occur, and document this in the form of policies and procedures.

RECOMMENDATION

We recommend that Telecommunication Services and Enterprise Security fully establish and implement policies and procedures for network monitoring.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and informed us that it continues to monitor and fine tune the State's network. DMB believes that to "fully" establish and implement in an ever-changing environment is a goal worth striving toward. DMB informed us that it is continuously refining and modifying operating policies and procedures to meet changing technology and security needs. In addition, Enterprise Security sponsored a standards process request for a new policy for intrusion detection and monitoring. Also, DMB informed us that a vendor product for enterprise level "surf control" is currently being evaluated with an expected completion date of spring 2002.

FINDING

9. Domain Name System (DNS)

Telecommunication Services had not fully established and documented policies and procedures for DNS.

DNS is a system that translates a common web site name to its numeric Internet address. The numeric Internet address is the method in which computers communicate. It allows users to connect to servers through easily remembered names rather than the numeric Internet protocol address. Our review of DNS disclosed:

a. Industry best practices for the configuration and security of DNS had not been followed at the time DNS was implemented. However, Telecommunications Services informed us that approximately two years ago it determined that controls over DNS could be improved. During our audit, Telecommunication Services improved controls over DNS by modifying its configuration and security.

b. Telecommunication Services had not established written procedures for managing DNS. DNS procedures should include the roles and responsibilities of staff, standards for configuration of DNS, explanations of how to add or modify DNS records, and criteria for testing records.

RECOMMENDATION

We recommend that Telecommunication Services fully establish and document policies and procedures for DNS.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. Telecommunication Services identified the DNS project in 1999 for budgeting as a fiscal year 2000-01 program. Telecommunication Services began the project in October 2000, and the last agency to be brought into the new environment was completed in September 2001. In addition, Enterprise Security sponsored a standards process request for a new policy for controlling DNS.

FINDING

10. Firewall Testing

Telecommunication Services had not established, documented, and implemented an ongoing process for testing the firewall.

Carnegie Mellon Software Engineering Institute's CERT Coordination Center recommends that firewalls be tested after every configuration change to help ensure that the firewall is secure and that rules operate as expected.

Telecommunication Services contends that complete testing of the firewall is not possible. However, Telecommunication Services should assess its firewall testing software and determine what level of testing can feasibly be conducted to help detect misconfigurations of the firewall.

RECOMMENDATION

We recommend that Telecommunication Services establish, document, and implement an ongoing process for testing the firewall.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. DMB informed us that there is a process in place for testing rule performance after each configuration change. Documentation of this process is under development and will be completed by March 31, 2002.

FINDING

11. Firewall Change Controls

Telecommunication Services had not fully established, documented, and implemented procedures to ensure the integrity and authorization of changes to the firewall rulebase.

Establishing controls over firewall rulebase changes would help ensure that only authorized, tested, and approved changes are implemented. Our review of firewall change controls disclosed:

a. Telecommunication Services did not ensure that only approved rulebase changes were implemented. We reviewed 20 service requests for rulebase

changes and identified 13 that had proper approvals. Telecommunication Services' internal procedures require that requests be approved by Enterprise Security and Telecommunication Services before being implemented. Without proper approvals, firewall rules could be implemented that may compromise the security of the network.

b. Telecommunication Services had not developed written procedures for the firewall rulebase change process. Documented procedures should indicate the process for requesting a rulebase change, persons authorized to request a change, staff authorized to review and approve requests, and staff authorized to implement the change. Procedures help ensure proper management and control over changes to the rulebase.

RECOMMENDATION

We recommend that Telecommunication Services fully establish, document, and implement procedures to ensure the integrity and authorization of changes to the firewall rulebase.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. DMB informed us that it began enforcement of a firewall change process in the first quarter of 2001. Formal procedure documentation is under development and will be completed by March 31, 2002. In addition, in May 2001, Enterprise Security sponsored a standards process request for a new policy for firewall and perimeter access control, which was adopted by the State's chief information officers in October 2001.

FINDING

12. Firewall Separation of Duties

Telecommunication Services did not implement a separation of duties for or compensating controls over firewall administration.

The Telecommunication Services firewall administrator is responsible for implementing firewall rules. However, we identified an instance in which a rule was implemented by the network security administrator. The network security administrator's job responsibilities also include approval of firewall changes and

monitoring of firewall logs. Separating the duties of approving, implementing, and monitoring changes or establishing compensating controls would help reduce the risk of unauthorized firewall changes.

Telecommunication Services informed us that there are limited occasions when the network security administrator must implement or change a firewall rule. To ensure that only proper changes are made to the firewall, Telecommunication Services should separate the duties or implement compensating controls, such as regular review of the log of firewall changes, to help detect unauthorized changes.

RECOMMENDATION

We recommend that Telecommunication Services implement a separation of duties for or compensating controls over firewall administration.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. DMB informed us that it developed a separation of duties matrix in September 2001, which includes provisions for emergency changes to the firewall. Documentation of this process will be completed by March 31, 2002.

FINDING

13. Firewall Practices and Procedures

Telecommunication Services had not developed and documented written firewall administration practices and procedures.

Establishing and documenting firewall administration practices and procedures would help ensure the secure operation and protection of the State's network. Our review disclosed that Telecommunication Services had not:

a. Identified standard rules that should be in every rulebase and guidelines for the order of rules. For example, the firewall lockdown rule is essential for any rulebase. This rule provides access control for the rulebase itself. We noted that the lockdown rule was missing from one rulebase. After we brought this to management's attention, Telecommunication Services immediately added the lockdown rule.

b. Developed procedures for the periodic review of the rulebase. We identified rules that should be removed from the rulebase because the access they allow was no longer needed. We also identified one rule that current firewall administrators could not explain why the rule was authorized. Telecommunication Services should establish and document a process to regularly review and update the rulebases to ensure that all rules are required and adhere to the firewall security policy.

c. Documented its procedures for reviewing firewall logs. Firewall logs can be used to detect possible intruder access attempts, vulnerable services used to access the State's network or the Internet, and access attempts to or through the firewall that violate the firewall security policy. Enterprise Security informed us that it reviewed the firewall logs; however, documented procedures would help ensure that there is clear definition of the monitoring process and the events to be monitored.

Telecommunication Services should document its practices and procedures for firewall administration to help ensure the consistent and proper implementation of firewall rules. Documented procedures would also communicate to staff the extent of their responsibilities.

RECOMMENDATION

We recommend that Telecommunication Services develop and document written firewall administration practices and procedures.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. DMB informed us that Telecommunication Services and Enterprise Security are developing documentation of practices and procedures, which will be completed by March 31, 2002.

FINDING

14. Backup and Recovery Controls

Telecommunication Services had not established complete network backup and recovery controls.

Effective network backup and recovery controls ensure that data and programs can be restored in the event of a disaster.

Telecommunication Services informed us that the network environment is redundant so recovery of files would be possible in the event of a hardware or software failure. However, our review of backup and recovery controls disclosed:

a. Telecommunication Services did not back up all critical servers and services. We noted that Telecommunication Services did not backup the file servers containing the firewalls, performance monitoring software, and domain name servers.

   After we brought this to management's attention, Telecommunication Services began backing up the performance monitoring software and one of the domain name servers.

b. Telecommunication Services did not store current copies of daily backup files off-site. Telecommunication Services stored its daily backup files on-site for up to three months before moving them off-site. In the event of a fire or other disaster, up to three months of data could be lost.

c. Telecommunication Services' off-site storage facility did not meet DMB guidelines. DMB Administrative Guide procedure 1310.02 requires that an off-site file library or vault be utilized that is a minimum of five miles from the main processing site. Telecommunication Services' off-site storage facility was in an adjacent building.

d. Telecommunication Services did not periodically test its backup files to ensure the completeness and integrity of the backup process. Telecommunication Services' backup procedures required monthly testing of backup files.

e. Telecommunication Services did not have complete written backup procedures. Backup procedures should include the roles and responsibilities of staff, backup schedules, and retention and storage requirements.

Data and programs can be lost through human error, equipment malfunction, and natural disaster. Without adequate backup and testing, restoring and recovering

files could be extremely costly and time consuming, if not impossible, and could significantly impair network operations.

RECOMMENDATION

We recommend that Telecommunication Services establish complete network backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and informed us that it has complied with the recommendation. DMB informed us that all servers are backed up and stored in a DMB-approved backup site.

FINDING

15. Contingency Planning

Telecommunication Services had not developed a comprehensive contingency plan.

The process of developing a contingency plan involves identifying critical business functions and the resources that support them, anticipating potential contingencies and disasters, selecting and implementing a contingency planning strategy, and testing and revising the strategy. Contingency planning is important to ensure the State's ability to provide a minimum acceptable level of services in the event of failure of critical information systems and services.

Telecommunication Services provides network and security resources critical to the operation of all State agencies. Telecommunication Services should develop a contingency plan to ensure there are no major disruptions to the State's business operations. We noted:

a. Telecommunication Services had not identified and documented critical systems and services and the resources that support these systems and services. The identification of resources may include human resources, processing capability, automated applications and data, computer-based services, and physical infrastructure. Telecommunication Services provides many Statewide services, such as network security, firewalls, routers, DNS, web services, remote access, and intrusion detection. Telecommunication

Services should identify and prioritize these critical systems and services to determine which are most critical to the operation of the State's network. In the event of a network failure or disaster, this would help ensure that the most important services are restored first.

b. Telecommunication Services had not conducted a risk assessment of the physical security of its computer room. Risk assessments help to identify system and service risks and appropriate measures to be addressed in a contingency plan. Telecommunication Services informed us that it is in the process of moving equipment to the computer room and will conduct a risk assessment afterward. Without periodic, comprehensive risk assessments, security risks may go undetected and uncorrected.

Identifying critical business functions and associated resources and risks will enable Telecommunication Services to take the next steps in selecting, implementing, and testing the contingency strategy. Telecommunication Services informed us that it would begin a disaster recovery evaluation process in April 2001 and develop draft documentation by December 2001.

RECOMMENDATION

We recommend that Telecommunication Services develop a comprehensive contingency plan.

AGENCY PRELIMINARY RESPONSE

DMB agreed with the finding and will comply with the recommendation. Documentation of a comprehensive contingency plan is in process and will be completed by March 31, 2002. In addition, cross-functional and cross-departmental teams have been formed, disaster recovery software has been chosen, and introductory training has been completed. Also, DMB informed us that it has built contingencies into the architecture of State-owned networks so that alternative routing paths can be made operable.

demilitarized zone (DMZ)	A firewall architecture that employs two routers to filter and transfer information between an organization's secure internal network and the Internet.
DMB	Department of Management and Budget.
Domain Name System (DNS)	A database system that translates an Internet protocol address into a domain name.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical for the amount of resources applied or minimizing the amount of resources required to attain a certain level of outputs or outcomes.
file server	A computer that stores files for access by other computers.
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.
internal control	The management control environment, management information system, and control policies and procedures established by management to provide reasonable assurance that goals are met; that resources are used in compliance with laws and regulations; and that valid and reliable performance related information is obtained and reported.
Internet	The worldwide information highway, which is composed of thousands of interconnected computer networks.

intranet	An internal local area network that may not be connected to the Internet but has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so that employees have access to the organization's Web documents.
LMAN	Lansing Metropolitan Area Network.
material condition	A serious 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 opinion of an interested person concerning the effectiveness and efficiency of the program.
mission	The agency's main purpose or the reason that the agency was established.
NIST	National Institute of Standards and Technology.
OAG	Office of the Auditor General.
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.
remote access	Data connections via a modem to a network.
reportable condition	A matter coming to the auditor's attention that, in his/her judgment, should be communicated because it represents either an opportunity for improvement or a significant deficiency in the design or operation of the internal control or in management's ability to operate a program in an effective and efficient manner.

rulebase	An ordered set of rules that define what is allowed and not allowed to access the Internet and intranet. The rulebase describes network communication in terms of the source, destination, and service. It also defines whether the network communication should be accepted or rejected, as well as if it should be logged.
TIS	Trusted Information Systems.
WAN	wide area network.
web-server	A server on the Internet that holds World Wide Web documents and makes them available for viewing by remote browsers.