MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

WIRELESS LOCAL AREA NETWORK (WLAN) SECURITY

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

August 2012

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

071-0562-12

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

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Wireless Local Area Network (WLAN) Security

Department of Technology, Management, and Budget

Report Number:
071-0562-12

Released:
August 2012

A WLAN is a data network that links various devices within a geographic area through radio communications. The security of a WLAN is dependent upon all of the components of the WLAN, including client devices, access points, and switches. The Telecommunications Division, Department of Technology, Management, and Budget (DTMB), is responsible for the security and management of the State's WLAN. As of April 30, 2012, the Telecommunications Division had installed 942 wireless access points in 139 buildings across 72 Michigan cities to provide wireless network access to State employees and guest access to the Internet.

Audit Objective:
To assess the effectiveness of DTMB's efforts to design and implement a secure WLAN infrastructure.

Audit Conclusion:
DTMB's efforts to design and implement a secure WLAN infrastructure were effective. Our audit report does not include any reportable conditions related to this audit objective.

Noteworthy Accomplishments:
The DTMB Telecommunications Division won the 2009 National Association of State Chief Information Officers (NASCIO) Award for Information Security and Privacy for its implementation of a secure WLAN.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DTMB's efforts to monitor the security of the State's WLAN.

Audit Conclusion:
DTMB's efforts to monitor the security of the State's WLAN were moderately effective. We noted two reportable conditions (Findings 1 and 2).

Reportable Conditions:
DTMB needs to increase its monitoring efforts regarding the investigation of unauthorized wireless access points to determine if the access points are inappropriately connected to the State's network (Finding 1).

DTMB did not perform annual security assessments of the State's WLAN (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective
To assess the effectiveness of DTMB's efforts to implement standards and procedures for the deployment, administration, and monitoring of the State's WLAN.

Audit Conclusion:

DTMB's efforts to implement standards and procedures for the deployment, administration, and monitoring of the State's WLAN were moderately effective. We noted one reportable condition (Finding 3).

Reportable Condition:

DTMB had not fully established and implemented security standards and procedures for the State's WLAN (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 3 findings and 3 corresponding recommendations. DTMB's preliminary response indicated that it agrees with all of the recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

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

August 10, 2012

John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Nixon and Mr. Behen:

This is our report on the performance audit of Wireless Local Area Network (WLAN) Security, Department of Technology, Management, and Budget.

This report contains our report summary; description; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; two exhibits, presented as supplemental information; 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 agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

Sincerely,

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

This Page Left Intentionally Blank

TABLE OF CONTENTS

WIRELESS LOCAL AREA NETWORK (WLAN) SECURITY
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

GLOSSARY

Wireless Local Area Network (WLAN) Security

A WLAN is a data network that links various devices within a limited geographic area, such as an office building, through the use of radio communications. WLANs generally consist of a client device, such as a laptop or a smartphone, that receives wireless access to a network through a wireless access point, which connects the client device to a distribution system, typically a wired network infrastructure. Some WLANs also use wireless switches to act as another barrier between the access points and the wired network.

The security of a WLAN is dependent upon all of the components of the WLAN, including client devices, access points, and switches. Given the interconnected nature of a WLAN to a wired network, the security of a WLAN can have implications for the security of an organization's overall network infrastructure.

Over the past several years, the use of wireless networks has proliferated, becoming an expectation to many professionals. Wireless technology grants the flexibility of maintaining access to information while conducting business throughout an organization. In addition, a wireless network allows for "guest" access to the Internet for use by both customers and vendors. However, the benefits associated with the flexibility of wireless bring the potential for unauthorized access.

The State of Michigan uses wireless networking in all major departments, with guest access available in many State office buildings throughout Michigan (see Exhibits 1 and 2, presented as supplemental information). Given the nature of wireless networks, it is imperative that special precautions are taken to prevent unauthorized access to sensitive or confidential information.

Telecommunications Division

The Telecommunications Division is one of seven divisions within Infrastructure Services, Department of Technology, Management, and Budget (DTMB).

The mission* of the Telecommunications Division is to provide leadership for diligent and cost-effective application of appropriate telecommunications technologies to meet the needs of State government. The Telecommunications Division is responsible for planning, designing, engineering, installing, managing, and supporting the network infrastructure to provide secure connectivity for government operations throughout the State. The network infrastructure consists of the Lansing Metropolitan Area Network (LMAN), the Wide Area Network (WAN), and the Wireless Local Area Network (WLAN) as well as telephone and Internet services. The scope of this audit consisted of the WLAN.

As of April 30, 2012, the Telecommunications Division had installed 942 wireless access points in 139 buildings across 72 Michigan cities to provide wireless network access to State employees and guest access to the Internet.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of Wireless Local Area Network (WLAN) Security, Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to design and implement a secure WLAN infrastructure.

2. To assess the effectiveness of DTMB's efforts to monitor the security of the State's WLAN.

3. To assess the effectiveness of DTMB's efforts to implement standards and procedures for the deployment, administration, and monitoring of the State's WLAN.

Audit Scope

Our audit scope was to examine the information processing and other records related to Wireless Local Area Network security of the State of Michigan. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit procedures, conducted in April and May 2012, generally covered the period October 2011 through May 2012.

Supplemental information was provided by DTMB and is presented in Exhibits 1 and 2. Our audit was not directed toward expressing a conclusion on this information and, accordingly, we express no conclusion on it.

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

Audit Methodology

We conducted a preliminary review of WLAN security to establish our audit objectives. We obtained an understanding of the security of the State's WLAN. We used the results of our preliminary review to determine the extent of our detailed analysis and testing. We used the National Institute of Standards and Technology (NIST) as the criteria for our conclusions on the audit objectives.

To accomplish our first objective, we interviewed DTMB staff and reviewed WLAN infrastructure diagrams to gain an understanding of the design of the State's WLAN. We tested DTMB's process for making changes to the WLAN and performed some limited scanning to verify the existence of authorized access points as well as to document unauthorized access points. We also reviewed the enterprise tools used by DTMB to configure and monitor the WLAN as well as policies and procedures for the administration of the WLAN.

To accomplish our second objective, we interviewed DTMB staff and reviewed policies and procedures to gain an understanding of the nature of the monitoring activities being performed. We also reviewed security assessments that had been performed by DTMB staff regarding the security of the State's WLAN and analyzed reports generated from the enterprise tools used to monitor the WLAN for unauthorized access points.

To accomplish our third objective, we interviewed DTMB staff and reviewed policies and procedures related to the overall administration of the State's WLAN.

We limited our review to the State's WLAN, which includes the configuration, deployment, and monitoring of wireless access points and wireless controllers. Our review did not include components of overall network security used in conjunction with the WLAN, such as firewall* configuration, user authentication*, and intrusion detection system* deployment. We also did not include in our review other wireless technologies used in the State, such as emergency response radio and cellular networks.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by

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

design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis. To the extent practical, we add balance to our audit reports by presenting noteworthy accomplishments for exemplary achievements identified during our audits.

Agency Responses

Our audit report contains 3 findings and 3 corresponding recommendations. DTMB's preliminary response indicated that it agrees with all of the recommendations.

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 the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO DESIGN AND IMPLEMENT A SECURE WIRELESS LOCAL AREA NETWORK (WLAN) INFRASTRUCTURE

COMMENT

Audit Objective: To assess the effectiveness of the Department of Technology, Management, and Budget's (DTMB's) efforts to design and implement a secure WLAN infrastructure.

Audit Conclusion: DTMB's efforts to design and implement a secure WLAN infrastructure were effective. Our audit report does not include any reportable conditions* related to this audit objective.

Noteworthy Accomplishments: The DTMB Telecommunications Division won the 2009 National Association of State Chief Information Officers (NASCIO) Award for Information Security and Privacy for its implementation of a secure WLAN.

EFFECTIVENESS OF EFFORTS TO MONITOR THE SECURITY OF THE STATE'S WLAN

COMMENT

Audit Objective: To assess the effectiveness of DTMB's efforts to monitor the security of the State's WLAN.

Audit Conclusion: DTMB's efforts to monitor the security of the State's WLAN were moderately effective. Our assessment disclosed two reportable conditions related to WLAN monitoring and security assessments (Findings 1 and 2).

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

FINDING

1. WLAN Monitoring

DTMB needs to increase its monitoring efforts regarding the investigation of unauthorized wireless access points to determine if the access points are inappropriately connected to the State's network. Without sufficient monitoring, DTMB cannot provide reasonable assurance that the State's network is secured from unauthorized wireless access points.

Any wireless access point that creates a wireless network within the range of the State's WLAN is considered to be an unauthorized wireless access point. These wireless networks can originate from other branches of State government, private businesses, individuals in the general area of a State building, or even an individual's cellular phone. However, unauthorized access points can also be connected directly to the State's network, creating a security vulnerability.

National Institute of Standards and Technology (NIST) *Guidelines for Securing Wireless Local Area Networks* recommends that organizations monitor for unauthorized wireless access points. Monitoring is important for all networks, but it is even more important for WLANs because unauthorized wireless access points can easily be installed at any time and may allow unauthorized users access to the network. Monitoring should include both the detection and investigation of unauthorized access points.

DTMB uses enterprise software to detect unauthorized wireless access points. We noted that, over a four-day period during the first week of May 2012, the enterprise software detected an average of 1,281 unauthorized wireless access points per day. DTMB informed us that it stopped investigating unauthorized wireless access points detected by the software in December 2011 because of limited resources and the significant amount of time and manpower required to investigate whether identified unauthorized wireless access points are connected to the State's network.

DTMB could improve the effectiveness of its monitoring efforts related to the investigation of unauthorized wireless access points by using a risk-based approach to help ensure that the scope and frequency of monitoring is appropriate for the threats facing the State's network. For example, DTMB could prioritize its

monitoring efforts by identifying high risk areas to investigate, such as unauthorized access points with weak encryption, to ensure that they are not connected to the State's network.

RECOMMENDATION

We recommend that DTMB increase its monitoring efforts regarding the investigation of unauthorized wireless access points to determine if the access points are inappropriately connected to the State's network.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with this finding and recommendation. DTMB informed us that it will increase its monitoring efforts regarding the investigation of unauthorized wireless access points and will develop and implement a risk-based approach to help ensure that the frequency of monitoring is improved.

FINDING

2. Security Assessments

DTMB did not perform annual security assessments of the State's WLAN. As a result, DTMB cannot ensure that the State's WLAN is protected from new vulnerabilities.

NIST *Guidelines for Securing Wireless Local Area Networks* recommends that periodic security assessments be conducted, at a minimum, on an annual basis. Periodic security assessments provide a valuable way to evaluate the overall security of the WLAN, assess new and emerging threats, and determine the effectiveness of security controls.

Our review disclosed that DTMB had not performed a wireless security assessment of the State's WLAN since May 2008.

RECOMMENDATION

We recommend that DTMB perform annual security assessments of the State's WLAN.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with this finding and recommendation. DTMB informed us that it will initiate a process and assign responsibility to perform a periodic security assessment of the State's WLAN on at least an annual basis.

EFFECTIVENESS OF EFFORTS TO IMPLEMENT WLAN STANDARDS AND PROCEDURES

COMMENT

Audit Objective: To assess the effectiveness of DTMB's efforts to implement standards and procedures for the deployment, administration, and monitoring of the State's WLAN.

Audit Conclusion: DTMB's efforts to implement standards and procedures for the deployment, administration, and monitoring of the State's WLAN were moderately effective. Our assessment disclosed one reportable condition related to WLAN standards and procedures (Finding 3).

FINDING

3. WLAN Standards and Procedures

DTMB had not fully established and implemented security standards and procedures for the State's WLAN. As a result, DTMB cannot ensure that it has communicated the requirements to maintain a secure WLAN to those who use and administer the network.

Establishing and implementing wireless security standards and procedures would help identify the required security practices to manage the risks related to WLANs. In addition, wireless security standards and procedures should dictate the acceptable use and enforcement of wireless technologies to users, management, and technical staff. Our review disclosed:

a. DTMB had not developed procedures for monitoring the security of the State's WLAN. As a result, DTMB had not assigned or communicated the roles, responsibilities, and expectations for monitoring the WLAN.

b. DTMB had not formally implemented standards identifying how WLAN technologies are to be used, deployed, administered, monitored, and supported. DTMB informed us that it has drafted a standard to address the requirements of the WLAN. The standard is in the process of being approved by the DTMB Cross Functional Review Team*. Without published standards, DTMB cannot ensure that users and technical staff are aware of the expectations for the use, management, and security of the wireless network.

RECOMMENDATION

We recommend that DTMB fully establish and implement security standards and procedures for the State's WLAN.

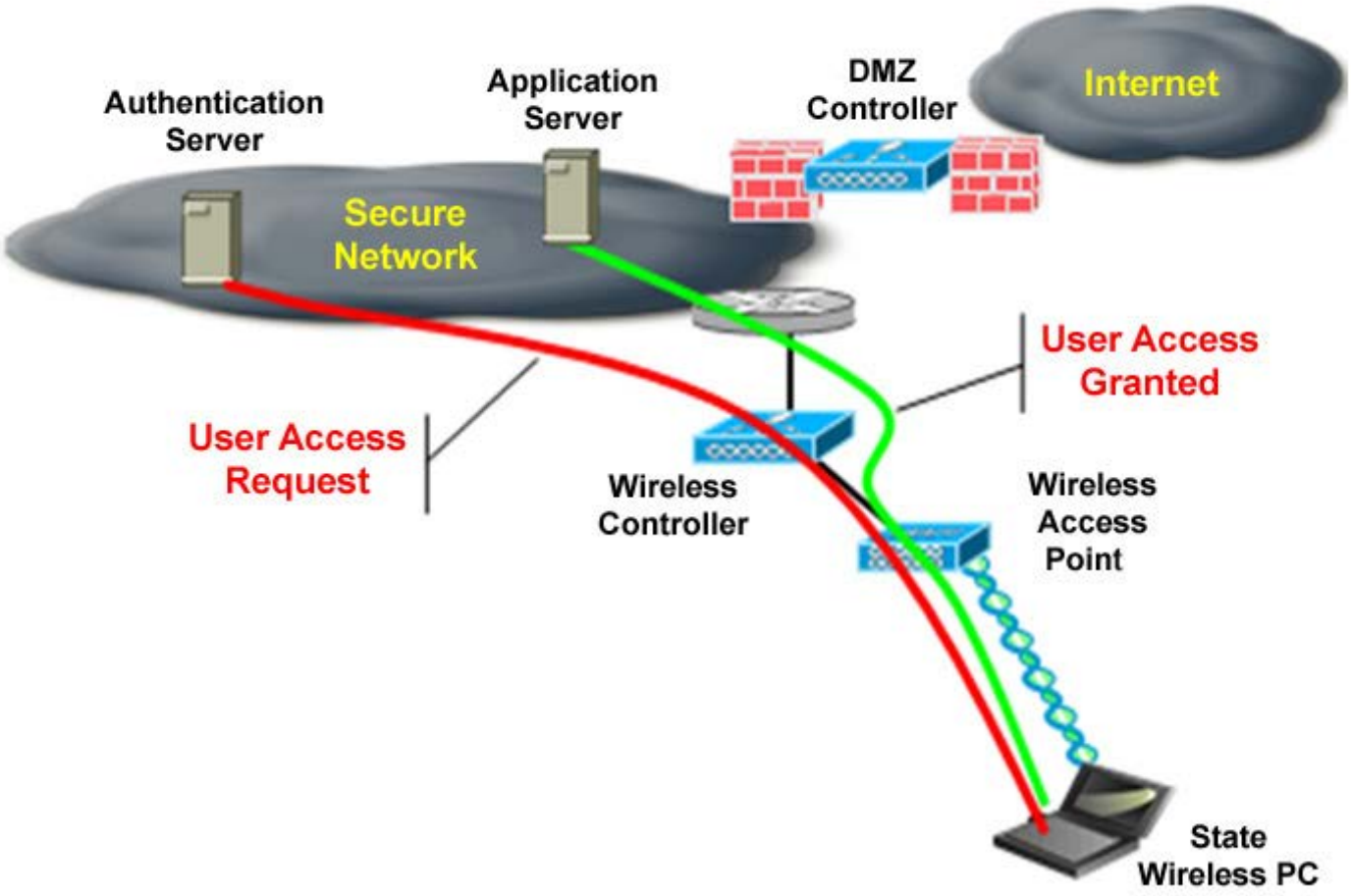
AGENCY PRELIMINARY RESPONSE

DTMB agrees with this finding and recommendation. DTMB has drafted standards and procedures to address the security requirements for the State's WLAN. The WLAN standards, which are currently under review for approval by DTMB's Cross Functional Review Team, will be fully implemented by October 31, 2012.

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

SUPPLEMENTAL INFORMATION

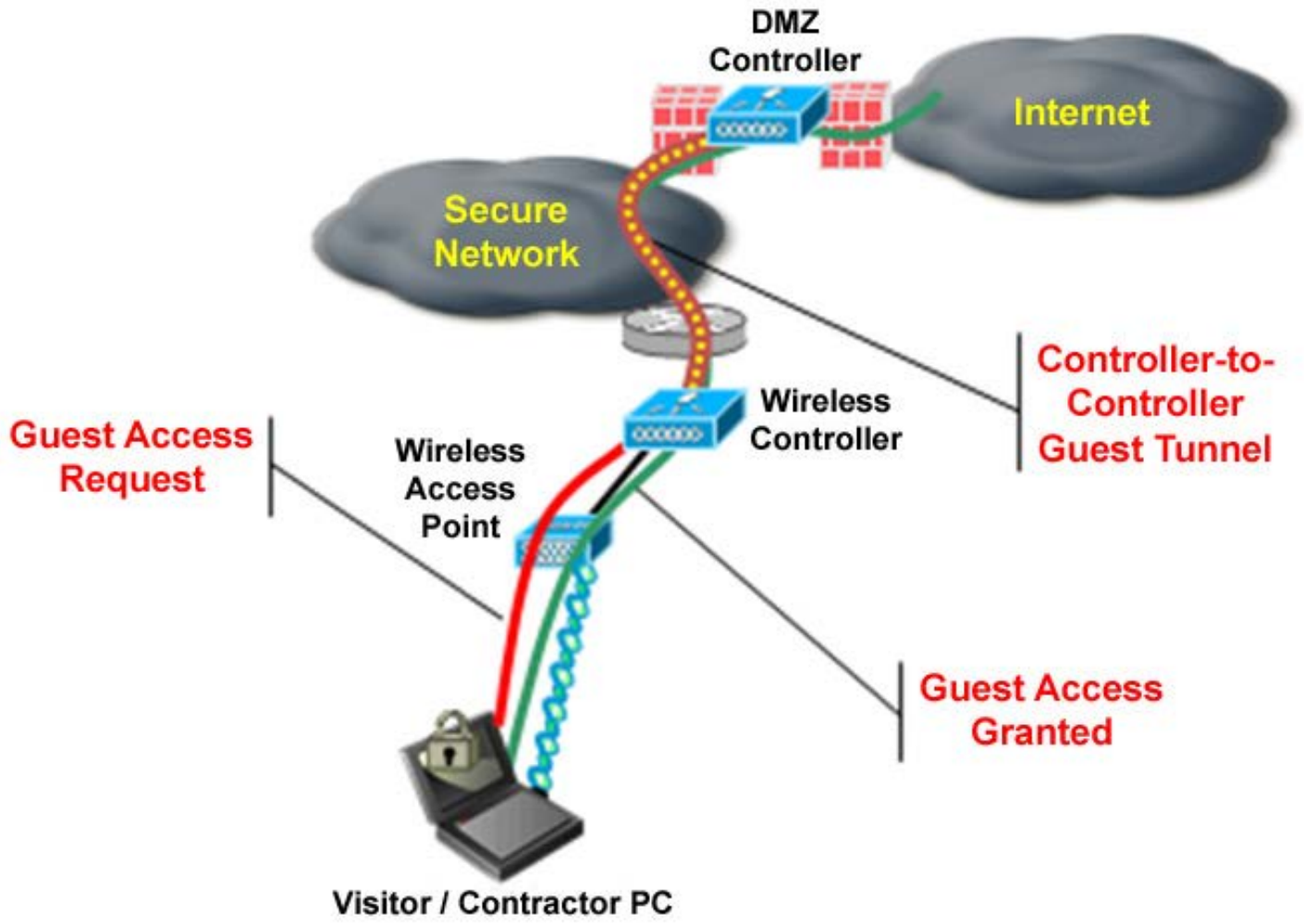
WIRELESS LOCAL AREA NETWORK (WLAN) SECURITY
Department of Technology, Management, and Budget (DTMB)
State of Michigan Wireless Network Access



A State of Michigan employee can obtain wireless access to the State's network using a wireless access point that connects to an authentication server which verifies that the device is a State-issued laptop and that the userID and password entered by the State employee are authorized to connect to the network (red line on the exhibit). Once authenticated, the State employee is granted access to the State's secure wired network (green line on the exhibit).

Source: DTMB's WLAN Service Power Point Demonstration.

WIRELESS LOCAL AREA NETWORK (WLAN) SECURITY
Department of Technology, Management, and Budget (DTMB)
State of Michigan Guest Wireless Network Access



A visitor or a contractor can obtain wireless access to the Internet using the State's wireless "guest" access. A guest userID and password can be obtained by calling a telephone number posted on information cards located in State buildings that allow wireless access. Upon inputting a guest userID and password (red line on the exhibit), the individual is granted access (green line on the exhibit) to the Internet via a secure encrypted tunnel (dotted yellow line on the exhibit).

Source: DTMB's WLAN Service Power Point Demonstration.

GLOSSARY

authentication	To positively verify the identity of a user, a device, or another entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Cross Functional Review Team	The team that reviews and approves DTMB policies, standards, and procedures.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
firewall	Hardware and software components that protect one set of system resources (e.g., computers or networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.
intrusion detection system	Software installed on a system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise the system.
mission	The main purpose of a program or an entity or the reason that the program or the entity was established.
NIST	National Institute of Standards and Technology.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and

	oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely or have occurred.
WLAN	Wireless Local Area Network.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL