AUDITOR GENERAL

WILLIAM O. MONROE, CPA

SELECTED STATE AGENCIES' PROGRESS IN ASSESSING SYSTEM AND NETWORK VULNERABILITIES

Information Technology Audit

SUMMARY

Pursuant to Florida Law[1], the State Technology Office (STO[2]), in consultation with each agency head, is required to conduct a comprehensive risk analysis to determine the security threats to the data and information technology (IT) resources of each agency. STO information resource policies and standards[3] incorporate guidelines of the National Institute of Standards and Technology (NIST) on risk management for information technology systems. The NIST guidelines[4] provide that security vulnerability testing is an important element of the IT risk assessment process.

Vulnerability scanning is the process of attaining information about the integrity of an organization's networks and associated systems through testing and verification of network-related security controls. These activities result in the identification of vulnerabilities, which are flaws, misconfigurations, or special sets of circumstances in systems and networks that could be exploited in order to bypass the security and misuse data and IT resources.

Our audit of selected State agencies' focused on evaluating the information technology vulnerability detection and remediation methodologies employed at five State agencies; as well as the monitoring and oversight efforts provided by the Department of Management Services (DMS) during the period November 2005 through March 2006. This audit also included assessments of safeguards for the security of modems and wireless access points attached to agency networks at the five selected State agencies. We also examined the adequacy of laws in place to protect the State's networks and IT systems.

The results of our audit disclosed that Florida law needed clarification with respect to responsibilities for IT governance, including, in particular, IT security and risk management. (Finding No. 1) In addition, based on reviewing the policies and procedures at a limited number of agencies, we noted that improvements were needed regarding:

- Agencies' vulnerability testing during interim periods between formal risk assessments. (Finding No. 2)
- Controls to ensure that agency-authorized wireless access points were appropriately secured and in procedures to detect the presence of unauthorized wireless access points. (Finding No. 3)
- Controls to ensure that agency-authorized modems were appropriately secured and in procedures to detect the presence of unauthorized modems. (Finding No. 4)
- Disseminating IT security policies and procedures in a more secure manner. (Finding No. 5)

[1] Section 282.318(2)(a)2., Florida Statutes (2005)

[2] Effective July 1, 2005, the responsibilities of the STO were assimilated by the Department of Management Services.

[3] Chapter 60DD-2.0010(7) Florida Administrative Code

[4] NIST Special Publication 800-30, Section 3.3

Specific details of conditions described in Findings No. 2 through 5 are not disclosed in this report. In addition, the responsible agencies are not named, to avoid the possibility of compromising agency information. However, the appropriate agency personnel have been notified of the deficiencies and have been provided the recommendations included in each of the findings.

DMS, as a part of developing a strategic plan for IT security, should work with the agencies in addressing the issues discussed in this report.

BACKGROUND

As with other large organizations, State agencies rely extensively on information technology (IT) systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, and preventing data tampering, fraud, and inappropriate disclosure of sensitive information. State agencies need suitable IT security programs to protect the confidentiality, integrity, and availability of their information and IT infrastructure.

An important component of a successful IT security program is an effective risk management process that identifies and assesses IT-related risk and takes steps to reduce risk to an acceptable level. Organizations use risk assessment to determine potential threats and associated risks to IT systems and to identify appropriate controls for reducing or eliminating risk.

Florida law[5] provides that the State Technology Office, in consultation with each agency head, shall, among other things, conduct, and periodically update, a comprehensive risk analysis to determine the security threats to the data and IT resources of each agency. The STO promulgated, in the form of administrative rules[6], information resource policies and standards for State agencies. The STO rules[7] provide that State agencies are to maintain information resource security programs that include, in part, an ongoing documented program of risk management, including risk analyses for all critical information resources, and periodic comprehensive risk analyses of all information resources. The STO rules[8] further provide that agency risk analyses are to be performed consistent with guidelines of the National Institute of Standards and Technology (NIST), an arm of the United States Department of Commerce, Technology Administration. Pursuant to the Federal Information Security Management Act (FISMA) of 2002, NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency operations and assets, other than national security systems.

NIST IT risk management guidelines[9] provide that the risk assessment process is usually repeated every three years for Federal systems pursuant to Office of Management and Budget (OMB) requirements, but that risk management should be conducted and integrated into the system development life cycle for IT systems, and that there should be a specific schedule for assessing and mitigating mission risks. The NIST IT risk management guidelines[10] also provide that security vulnerability testing is an important element of the IT risk assessment process. Vulnerabilities are system flaws or weaknesses that could be accidentally triggered or intentionally exploited to cause a security breach. NIST guidelines[11] for network security testing further provide that such testing should be a routine and integral part of the system and network operations and administration.

Security vulnerability tests can be conducted at the host, network, and application level. Testing methods include both manual and automated procedures. Automated tools exist that can be used to scan hosts and networks to identify their components and detect such vulnerabilities as insecure settings and

[5] Section 282.318(2)(a)2, Florida Statutes (2005)
[6] Chapter 60DD-2, Florida Administrative Code
[7] Chapter 60DD-2.001(3)(k), Florida Administrative Code
[8] Chapter 60DD-2.001(8)(d), Florida Administrative Code
[9] NIST Special Publication 800-30, Section 5.1
[10] NIST Special Publication 800-30, Section 3.3
[11] NIST Special Publication 800-42, Section 3.3

configurations, outdated software versions, and inconsistencies with the organization's security policy.

Vulnerability tests, particularly automated methods, provide information about the strengths and weaknesses in IT security as of a point in time. Because organizations frequently update their software and hackers constantly develop new software exploits, the value of a single battery of vulnerability tests in providing assurance about IT security diminishes greatly over time. Therefore, to be most effective, security vulnerability testing should be conducted on a recurring basis.

To promote agency compliance with requirements in Florida law[12] and rule[13] for conducting IT risk analyses, the STO, on February 16, 2005, established task orders with two firms, Dyntek, Inc. (Dyntek), and Integrated Computer Solutions, Inc. (ICS), for providing risk management and assessment activities for State agencies, as described in the NIST guidelines. Between March 22, 2005, and December 2, 2005, thirty-two State entities contracted with Dyntek or ICS for risk assessments of their networks and interconnected systems. These risk assessments were intended to be conducted in a manner consistent with STO rules[14] and NIST guidelines[15], to detect vulnerabilities in systems, to analyze the impact the vulnerabilities could have, and to determine appropriate actions to minimize the risks to those systems. Dyntek and ICS used industry-recognized and NIST-approved automated vulnerability scanning tools to assess the security configurations of agencies' networks and interconnected systems.

Funding for the Dyntek and ICS contracts for the risk assessments came from a variety of sources. Most entities were reimbursed from fiscal year 2004-05 General Revenue and Trust Fund moneys appropriated to the STO and the Department of Law Enforcement and from fiscal year 2005-06 General Revenue and Trust Fund moneys appropriated to DMS. Documentation provided by DMS indicated that the total amount of entity reimbursements for Dyntek and ICS assessments was $1,058,300 and that one additional agency used its own appropriations. Similar funding was not available for fiscal year 2006-07.

Finding No. 1: Responsibility for IT Security and Risk Management

Good business practices for IT security management include positioning the security management at the highest appropriate organizational level, so that the management of security actions is in line with business requirements. In the State of Florida, information technology and the security thereof are essential to the effectiveness of State government as a whole and of individual State agencies. Consequently, strong IT security management, including security planning and risk management, is necessary from an enterprise perspective as well as an agency perspective.

Florida law[16] provides that the STO, in consultation with each agency head, is responsible and accountable for assuring an adequate level of security for all data and IT resources of each agency. As previously discussed, one of the STO's related responsibilities is conducting, and periodically updating, comprehensive IT risk analyses of each agency.

In the fiscal year 2005-06 General Appropriations Act, no appropriations were made for the funding of positions in the STO. Some of the STO's former functions relating to State IT management were assumed by the Department of Management Services, including, in particular, activities relating to State IT security. However, rulemaking authority remained with the STO.

[12] Section 282.318(2)(a)2, Florida Statutes (2005)
[13] Chapter 60DD-2.001(8)(a), Florida Administrative Code
[14] Chapter 60DD-2.001(8)(d), Florida Administrative Code
[15] NIST Special Publication 800-30
[16] Section 282.318(2)(a), Florida Statutes (2005)

Our audit disclosed that, during our audit period, DMS functioned primarily in an advisory and oversight role with respect to agency IT security and risk management. DMS activities included coordinating with Dyntek and ICS for risk assessments to be performed at the agencies, informally monitoring the progress of the risk assessments, and holding monthly meetings with agency information security managers, at which issues that agencies were having in implementing solutions for vulnerabilities were informally discussed. However, agencies provided the day-to-day management of their IT security and it was ultimately their responsibility to remediate identified vulnerabilities.

Agency information security managers are well-positioned to understand, assess, and manage the IT risks inherent to the agency's mission and environment. Yet, because of the interrelationships of State agency business processes, the interconnected nature of State systems and networks, and the potential for Statewide impact of security events, an enterprise view of IT security is also important to promote the adoption of appropriate security practices throughout State government and to seek economical security solutions.

Subsequent findings in this report describe aspects of State agencies' vulnerability testing activities and related security management issues that needed improvement. In response to our audit inquiry, the applicable agencies cited, among other things, a lack of funding, resources, and training as obstacles. Agencies further expressed the need for a central authority to provide resources and technical guidance with respect to security vulnerability testing. Additionally, agencies expressed concerns about being able to retain staff trained to perform these functions due to the pay differential between the public and private sector for this type of work, utilizing their limited staff resources to perform these functions, and their ability to control equipment and security configurations of outsourced staff.

Given the absence of a functioning STO, and the uncertainty of future STO funding, clarification was needed in the provisions of Florida law relating to State IT governance, including, in particular, the placement of responsibility for agency IT security and risk management. Clearly delineated responsibilities within Florida law regarding IT security management at the enterprise level and within individual agencies could help pinpoint accountability for security and facilitate progress in such activities as assessing and mitigating IT security vulnerabilities.

In the implementing provisions for the fiscal year 2006-07 General Appropriations Act[17], the Legislature amended Florida law to provide that DMS, in consultation with each agency head, is responsible for coordinating, assisting, and recommending minimum operating procedures for ensuring an adequate level of security for data and IT resources. The proviso language recognized the need for responsibilities at both the individual agency and enterprise level as discussed above. Each agency was made responsible for, among other things, conducting, and updating every 3 years, a comprehensive risk analysis to determine the security threats to the data and IT resources of the agency.

The implementing provisions for the fiscal year 2006-07 General Appropriations Act[18] also directed DMS to establish an Office of Information Security (OIS) to be headed by a Chief Information Security Officer. The Office was charged with developing, by March 1, 2007, a strategic plan for IT security, developing standards and templates for conducting comprehensive risk analyses and information security audits by State agencies, assisting State agencies in complying with the provisions of the law with regard to security of data and IT resources, establishing minimum standards for the recovery of IT following a disaster, and conducting training for agency information security managers.

[17] Chapter 2006-26, Section 18, Laws of Florida
[18] Chapter 2006-26, Section 18, Laws of Florida

However, the amended requirements of the fiscal year 2006-07 General Appropriations Act[19] will expire on July 1, 2007. Additionally, neither DMS nor OIS were given rulemaking authority with respect to information resource security policies and standards[20] for State agencies.

Recommendation: The Legislature should consider continuing its efforts to clarify in Florida law, for periods subsequent to July 1, 2007, which entity is responsible for ensuring an adequate level of data and IT resource security at State agencies, including, in particular, conducting comprehensive IT risk analyses and maintaining information resource security policies and standards[21].

Finding No. 2: Internal Vulnerability Scans

As previously discussed, the risk assessments performed by Dyntek and ICS at State agencies included procedures for testing networks and systems for vulnerabilities, such as missing security patches, open entry points on systems, and viruses capable of controlling computer systems (such as Trojan horses) However, because of the dynamic nature of IT, it is important to test networks and systems for vulnerabilities not only as a part of a formal risk assessment process, but also as a part of routine system administration. NIST network security testing guidelines recommend that network and vulnerability scanning activities be performed on at least a bimonthly basis for sensitive systems and a semiannual basis for all other systems.

For those agencies within the scope of audit, we examined the extent to which vulnerability testing was being conducted on an interim basis between formal risk assessment activities. Our audit disclosed that:

- Most agencies did not perform interim network and vulnerability scans.
- Some vulnerability scanning tools used did not comprehensively scan all network resources.
- Written policies and procedures for conducting vulnerability testing were often lacking.

Without regular vulnerability scanning of networks and systems, the risk is increased that vulnerabilities within networks and interconnected systems, should they arise, will not be timely detected and corrected, leaving agency data and IT resources exposed to misuse.

Recommendation: The applicable agencies should perform vulnerability scans of their networks and interconnected systems on a basis consistent with NIST[22] recommendations. Detected vulnerabilities should be mitigated in the most efficient and cost effective manner available.

Finding No. 3: Wireless Controls

Wireless networking is quickly becoming a more widely used networking solution. Significant risks to security are presented by wireless networks as most wireless networking equipment is configured insecurely in its default configuration, flaws exist in WEP (Wired Equivalent Privacy) authentication, and the range for many wireless devices can extend beyond intended coverage areas, allowing attackers to gain access to a network without setting foot in the building in which the network is located. Good wireless security controls include provisions to change configurations before implementation to provide stronger security settings than those present in default configurations; use of more advanced authentication, such as Wi-Fi Protected Access 2 (WPA2) with Extensible Authentication Protocol (EAP) on 802.1X authentication servers; and planning to minimize how far wireless signals extend beyond coverage areas.

[19] Chapter 2006-26, Section 18, Laws of Florida

[20] Chapter 60DD-2, Florida Administrative Code

[21] Chapter 60DD-2, Florida Administrative Code

[22] NIST Special Publication 800-42, Section 3

NIST guidelines include recommended procedures for assessing the effectiveness of controls over wireless access points. These include war drives or war walks, which involve patrolling an area with portable computing devices, such as laptops, equipped with wireless access cards, attempting to detect unauthorized wireless access points attached to networks. NIST recommends that this procedure be performed weekly to semiannually, depending on the sensitivity of the systems residing on the network.

Improvements were needed in controls to ensure agency authorized wireless access points were appropriately secured and in agency procedures to detect the presence of unauthorized wireless access points. Our audit disclosed the following:

- ➢ Inadequate controls were used at an agency to secure authorized wireless access points.
- ➢ Most agencies did not perform war drives or war walks to detect unauthorized wireless access points nor had any written procedures to do so.
- ➢ We detected an unauthorized wireless network device on an agency network.
- ➢ Some agencies did not have policies or procedures in place prohibiting unauthorized wireless access points from being attached to their networks.

Without controls to ensure agency authorized wireless access points are appropriately secured and procedures to detect the presence of unauthorized wireless access points, agencies increase the risk of their network security being compromised by an individual with malicious intent or by users installing unauthorized wireless access points.

Recommendation: The applicable agencies should implement appropriate controls to secure authorized wireless access points from attacks that can exploit insecure configurations and weak authentication mechanisms. Agencies should also perform periodic war drives or war walks to detect and remediate unauthorized wireless access points that may be present on their networks allowing attackers to bypass normal network security.

Finding No. 4: Modem Controls

In networks, unauthorized modems are often an overlooked vulnerability. These unauthorized modems provide a means to bypass most or all of the security measures in place on a network. A compromise of security launched via an unauthorized modem could allow an attacker direct and undetected access to a network. NIST guidelines include recommended procedures for assessing the effectiveness of controls over modems. These include war dialing, which entails using a computer to dial large blocks of an organization's phone numbers in search of available modems, to detect unauthorized modems attached to the organization's network. NIST recommends that war dialing be conducted at least annually.

Improvements were needed in controls to ensure agency authorized modems were appropriately secured and in agency procedures that detect the presence of unauthorized modems. Our audit disclosed the following:

- ➢ Most agencies had inadequate controls to secure authorized modems.
- ➢ We detected unauthorized modems at some agencies.
- ➢ Agencies did not perform war dials to detect unauthorized modems.
- ➢ Some agencies did not have policies or procedures in place prohibiting unauthorized modems from being attached to their networks.

Without controls to ensure agency authorized modems are appropriately secured and procedures to detect the presence of unauthorized modems, agencies increase the risk of their network security being compromised by an individual with malicious intent or by users installing unauthorized modems.

Recommendation: The applicable agencies should implement appropriate controls to secure authorized modems from attacks that can exploit insecure configurations and weak authentication mechanisms. Agencies should also perform periodic war dials to detect and remediate unauthorized modems that may be present on their networks allowing attackers to bypass normal network security.

Finding No. 5: Dissemination of Security Policies and Procedures

Florida law[23] provides that internal policies and procedures to assure the security of data and IT resources are confidential and exempt from public disclosure. Our audit disclosed that one agency's practice of disseminating IT security policies and procedures did not adequately safeguard the information from inappropriate disclosure. This increased the risk of unauthorized access to, and misuse of, the agency's data and IT resources.

Recommendation: The agency in question should revise its method of disseminating security policies and procedures to provide increased assurance that sensitive security information is disclosed only to persons with a need to be informed of the requirements.

[23] Section 282.318(2)(a)3., Florida Statutes (2005)

OVERALL CONCLUSION AND RECOMMENDATION

The issues discussed in Findings Nos. 2 through 5 indicate a need for improved and more frequent security vulnerability testing and improvements in certain aspects of IT security. The OIS, when established by DMS, will be well-positioned to promote, facilitate, and assist agency actions to enhance information security, including improvements in security vulnerability testing and the other areas discussed in this report.

We recommend that DMS, in establishing the OIS, continue to facilitate agency IT risk assessment activities. As a part of developing its strategic plan for IT security, DMS should work in consultation with the agencies to establish provisions for improved and more frequent security vulnerability testing consistent with NIST guidelines. Additionally, as a part of the plan, DMS should assist the agencies in addressing the specific security control issues identified in this report in a manner consistent with NIST guidelines and good IT security practices. The DMS strategic planning process should consider the agencies' needs for guidance, training, and assistance in securing resources for these activities.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine what measures had been taken by selected State agencies to assess vulnerabilities in their networks and IT systems, and the effectiveness of procedures followed by selected State agencies to properly manage wireless networks and modems. Audit objectives also included an evaluation of the adequacy of laws, rules, and guidelines in place to protect the State's networks and IT systems.

Our audit scope focused on selected State agencies' IT vulnerability assessment activities and agency safeguards over wireless access points and modems during the period November 2005 through March 2006. We also examined the Department of Management Services' oversight and monitoring of agency vulnerability assessment activities.

In conducting this audit at the selected State agencies, we interviewed appropriate agency personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to vulnerability assessments, wireless controls, and modem controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated July 13, 2006, the Secretary of the Department of Management Services provided a response to our Overall Conclusion and Recommendation. This letter is included at the end of this report as Appendix A.

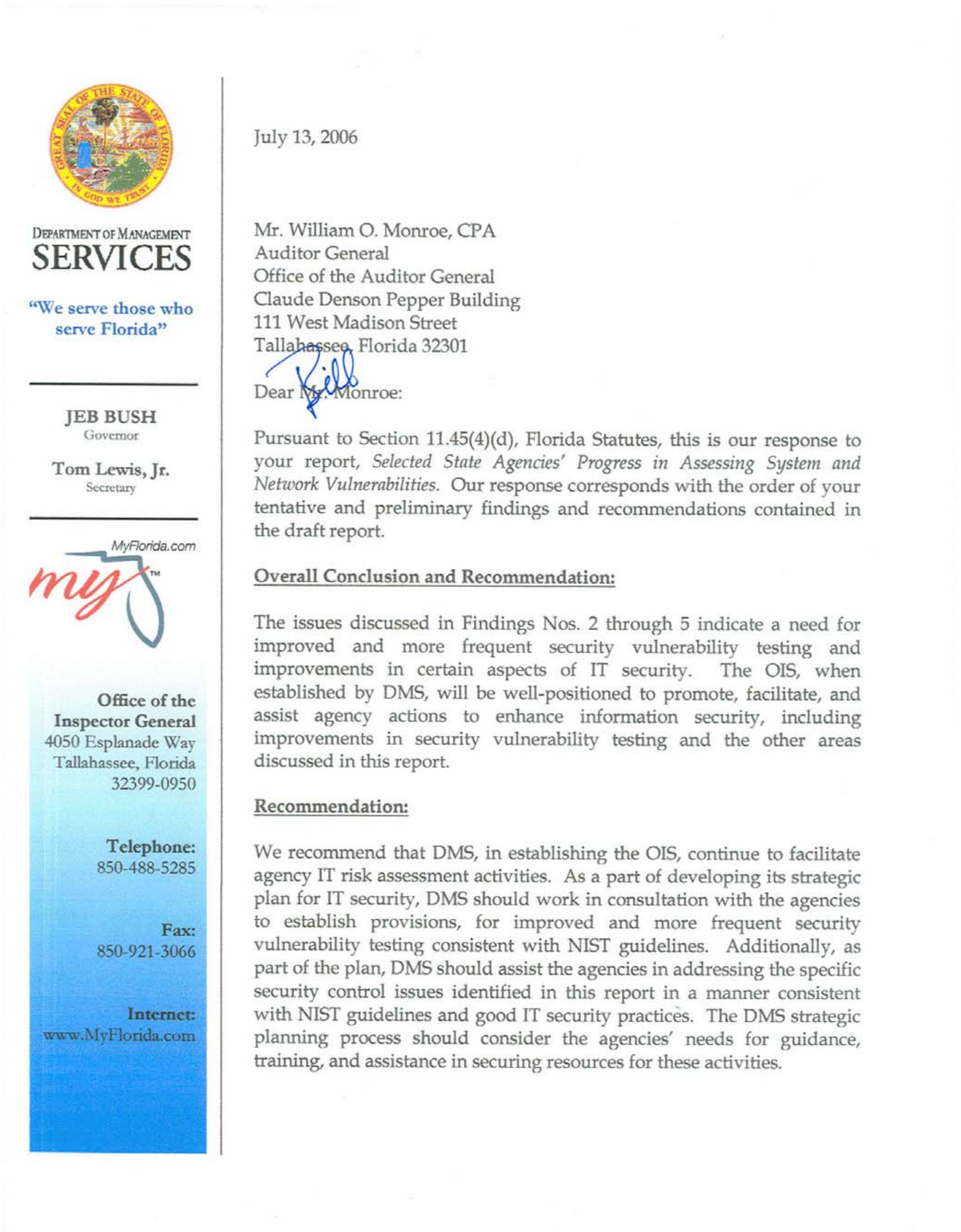
To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Daniel Pearce and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A

MANAGEMENT RESPONSE



DEPARTMENT OF MANAGEMENT
SERVICES

"We serve those who serve Florida"

JEB BUSH
Governor

Tom Lewis, Jr.
Secretary

MyFlorida.com

Office of the Inspector General
4050 Esplanade Way
Tallahassee, Florida
32399-0950

Telephone:
850-488-5285

Fax:
850-921-3066

Internet:
www.MyFlorida.com

July 13, 2006

Mr. William O. Monroe, CPA
Auditor General
Office of the Auditor General
Claude Denson Pepper Building
111 West Madison Street
Tallahassee, Florida 32301

Bill

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report, *Selected State Agencies' Progress in Assessing System and Network Vulnerabilities*. Our response corresponds with the order of your tentative and preliminary findings and recommendations contained in the draft report.

Overall Conclusion and Recommendation:

The issues discussed in Findings Nos. 2 through 5 indicate a need for improved and more frequent security vulnerability testing and improvements in certain aspects of IT security. The OIS, when established by DMS, will be well-positioned to promote, facilitate, and assist agency actions to enhance information security, including improvements in security vulnerability testing and the other areas discussed in this report.

Recommendation:

We recommend that DMS, in establishing the OIS, continue to facilitate agency IT risk assessment activities. As a part of developing its strategic plan for IT security, DMS should work in consultation with the agencies to establish provisions, for improved and more frequent security vulnerability testing consistent with NIST guidelines. Additionally, as part of the plan, DMS should assist the agencies in addressing the specific security control issues identified in this report in a manner consistent with NIST guidelines and good IT security practices. The DMS strategic planning process should consider the agencies' needs for guidance, training, and assistance in securing resources for these activities.

Mr. William O. Monroe
July 13, 2006
Page 2

Response:

DMS concurs with the "Overall Conclusion and Recommendation." DMS will continue to facilitate agencies' IT risk assessment activities as it establishes the Office of Information Security (OIS.)

In developing the strategic plan for information technology security, DMS will coordinate with agencies to address the specific security control issues identified in the audit report. The strategic planning process will consider the agencies' needs for guidance, training, and assistance in securing resources for these issues. As required by Section 282, 318(4), Florida Statutes, the strategic plan will be developed and submitted to the Executive Office of the Governor, President of the Senate, and the Speaker of the House by March 1, 2007.

DMS' continued facilitation of agencies' IT risk assessment activities will be dependent upon adequate and continued funding from the Legislature. (The Legislature has provided funding for only six-months, beginning in January 2007.) Also, to facilitate agencies' IT risk assessment activities, DMS believes that the newly created OIS should be empowered by statute and rule. The OIS will need this authority to enable compliance in this critical mission sensitive area and to ensure that uniform direction is provided to all agencies. We intend to pursue this authority in the 2007 Legislative Session.

If further information is needed concerning any of our responses, please contact Steve Rumph, Inspector General, at 488-5285.

Sincerely,

Tom Lewis, Jr.
Secretary

TL/taw

cc: Ken Granger, Deputy Secretary
Department of Management Services

Mike Russo, Chief Information Officer
Department of Management Services

THIS PAGE INTENTIONALLY LEFT BLANK