AUDITOR GENERAL

WILLIAM O. MONROE, CPA

SELECTED STATE AGENCIES' PUBLIC WEB SITES

Information Technology Audit

July 2004 Through June 2005

With Selected Actions Taken Through October 2005

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this information technology (IT) audit were to evaluate the effectiveness of selected IT controls applicable to State agency Web sites. Our scope focused on the Web sites, selected on-line applications, and supporting networks at the following State agencies: Department of Agriculture and Consumer Services (DACS); Department of Financial Services (DFS); Fish and Wildlife Conservation Commission (FWC); Department of Health (DOH); Department of Highway Safety and Motor Vehicles (DHSMV); State Technology Office (STO)[1]; and Department of Transportation (DOT). We also reviewed the agencies' progress in making their e-Gov services accessible to people with disabilities. This portion of our audit was extended to include the MyFloridaMarketPlace and People First applications of DMS. Our audit was for the period July 2004 through June 2005, with selected agency actions taken through October 2005.

In conducting the audit, we interviewed appropriate agency personnel, reviewed agency policies and procedures and other applicable documentation, and performed various other audit procedures to test selected controls.

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 Brian Rue, CPA*, CISA, and supervised by Nancy Reeder, CPA*, 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.

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

SELECTED STATE AGENCIES'

PUBLIC WEB SITES

TABLE OF CONTENTS

SUMMARY OF FINDINGS

State of Florida agencies increasingly rely on electronic government (e-Gov) services for the delivery of government services to citizens; dissemination of information; enhanced interaction with vendors conducting business with the State; and more efficient government management. E-Gov utilizes information technology (IT), including the Internet and internal State networks (Intranets), to interact with citizens, State employees, and those conducting business with the State.

Our audit focused on evaluating certain general IT controls applicable to selected public Web sites, on-line applications, and supporting networks during the period July 2004 through June 2005, with selected actions taken through October 2005, at the following State agencies: Department of Agriculture and Consumer Services (DACS); Department of Financial Services (DFS); Fish and Wildlife Conservation Commission (FWC); Department of Health (DOH); Department of Highway Safety and Motor Vehicles (DHSMV); State Technology Office (STO)[2]; and Department of Transportation (DOT). Our audit also included an evaluation of the agencies' progress in making their e-Gov services accessible to people with disabilities. This portion of our audit was extended to include the MyFloridaMarketPlace and People First applications of the Department of Management Services (DMS). Appendix A lists the Internet addresses of the agency Web sites and on-line applications included within the scope of our audit.

Certain deficiencies were noted relating to various agencies' Web sites, on-line applications, and supporting networks. Specifically, we noted that:

Finding No. 1: Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.

Finding No. 2: Certain STO enterprise standards for coding and design of Web sites were not consistently followed.

Finding No. 3: Agencies lacked written Web content management strategies for ensuring the integrity of Web site content.

Finding No. 4: The six agencies within the scope of audit that had e-Gov applications either had not established written procedures, or had incomplete procedures, for response strategies to be followed if personal identification information was compromised in a security breach.

Finding No. 5: We noted deficiencies in hyperlinks within the agencies' Web sites.

Finding No. 6: Current written procedures for managing Web domain names were not maintained by all agencies.

Finding No. 7: Written procedures had not been fully developed by several agencies for maintaining Web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.

Finding No. 8: Certain deficiencies were noted in security-related controls at DHSMV.

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

BACKGROUND

A Web site is a collection of Web pages accessible over the World Wide Web (Internet) or Intranets. Each agency Web site included in our audit tests contained a home page representing an entry point to on-line information and services available to users. The agencies tested presented their e-Gov services through Web sites that varied in layout, navigation, style, and function.

All seven agencies deployed technologies to protect the confidentiality of user information during transactions processed over the Internet. Each e-Gov service in our audit tests utilized the e-commerce standard, Secure Sockets Layer (SSL), a commonly-used telecommunications protocol to protect the confidentiality and integrity of transactions between the user and the network providing the e-Gov service. The SSL procedure enables the encryption of data, such as logon passwords and credit card numbers, to prevent unauthorized individuals from intercepting users' information for malicious intent. The process incorporated the use of digital certificates maintained by the agencies to validate the identity of the agencies' servers to the users' Web browsers during SSL connections. This decreases the chance that communication links from the users' computers to the agencies' servers could be intercepted and rerouted to unauthorized servers. All agencies within the scope of this audit maintained unexpired certificates issued by a Certificate Authority Service.

Risk assessments of all seven agencies' applications were performed by the agencies or third parties to reduce the chance of programming errors creating vulnerabilities that could be exploited to violate the confidentiality of the data stored by the agency. Also, when a certain dollar value of transactions was met, those agencies accepting Visa and Master Card were required to periodically obtain vulnerability assessments by outside vendors.

The IT equipment supporting e-Gov services was comprised of unique technology infrastructures. These included Web, application, and database servers; agency or vendor networks; the State's network; and the Internet. Florida law[3] contained provisions designating the STO as responsible for collaborating with agencies to implement safeguards to reduce, eliminate, or recover from identified risks to their data and IT resources. Those agencies supplementing their internal technologies by purchasing hosting services from outside vendors relied on those vendors for certain privacy and security provisions over State data.

[3] Section 282.318, Florida Statutes

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Accessibility of e-Gov Services

Accessibility of e-Gov services refers to the ability of physically disabled users to engage an assistive technology to enjoy the same e-Gov services available to the general population. Assistive technologies include software-based screen readers used by visually disabled users to navigate an e-Gov service. These programs translate the code used to construct the Web page to provide audio prompts such as reading the text of a headline on a page. However, the Web page has to be coded properly for these technologies to function. A nonconforming (noncompliant) page would produce unintelligible sounds rendering the e-Gov service unusable for the visually disabled user.

Title II of the Americans with Disabilities Act (ADA) of 1990 and its implementing regulations require states to provide qualified individuals with disabilities equal access to their programs, services, or activities, unless doing so would fundamentally alter the nature of their programs, services, or activities or would impose an undue burden[4]. The ADA also requires that states ensure that their communications with individuals with disabilities are as effective as communications with others[5]. The ADA is flexible on the methods to accomplish this access; however, one way to satisfy these requirements would be to ensure that government Web sites have accessible features.

Section 508 of the Rehabilitation Act of 1973, as amended[6] (Section 508), effective June 21, 2001, requires Federal departments and agencies that develop, procure, maintain, or use electronic and information technology to assure that these technologies provide access to information and data for people with disabilities. Section 508 also requires the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards for Federal agencies setting forth a definition of electronic and information technology and the technical and functional performance criteria necessary for accessibility for such technology[7].

The STO Enterprise Standard, Portal Coding and Design[8], effective January 21, 2004, provides that all executive branch Florida government Web sites must comply with Section 508 to ensure the widest possible audience easy access to government information. This Enterprise Standard was not issued as a rule, and the authority of the STO to impose this requirement is unclear.

On June 24, 2005, the Executive Office of the Governor issued Executive Order Number 05-133. The Executive Order created the Governor's Accessible Electronic and Information Technology Task Force (Task Force) to provide guidance in improving the accessibility of the state's electronic and information technology to persons with disabilities. The Order further specified the Task Force shall adopt Section 508 standards when reviewing and assessing state electronic information technology systems. Additionally, all agencies under the authority of the Governor were directed and all other agencies were requested to use reasonable efforts to comply with Section 508 standards when purchasing and implementing electronic and information technology. The Task Force is charged with submitting a report, including recommendations to the Governor, on January 31, 2006.

[4] 42 U.S.C. § 12132, 28 CFR 35.149-35.150
[5] 28 CFR 35.160-35.164
[6] 29 U.S.C. 794d
[7] These standards are located in 36 CFR Part 1194.
[8] STO-2-72-006, Enterprise Standard, Portal Coding and Design

Creating accessible e-Gov services requires that Web programmers and Web page designers be knowledgeable on the techniques required to create, test, and maintain content that is accessible to the visually disabled user. Also, appropriate contract provisions help ensure that purchased e-Gov services are accessible. In Florida, the Americans with Disabilities Act Working Group (ADAWG) has been established[9], in part, to assist agencies in assuring that their communications with individuals with disabilities are as effective as communications with others.

We requested each agency within the scope of this audit to provide information and documentation regarding their determinations of whether their Web sites and e-Gov applications met the Section 508 accessibility standards, which were incorporated in the STO Enterprise Standard, Portal Coding and Design. The validity of the agencies' determinations of Section 508 compliance was beyond the scope of this audit.

The STO provided the results of a scan that analyzed the coding used by the MyFlorida.com Web site to conform with Section 508 compliance. Additionally, DOT provided a copy of a scan completed by an application used to verify Section 508 standards compliance. Its scan indicated that the SunPass e-Gov application was in compliance with those standards. None of the other agencies within the scope of this audit were able to provide documentation of their Web site or e-Gov application being fully Section 508 compliant. Specifically, we noted:

- **DACS – Web Site** – DACS maintained Web standards requiring Section 508 compliance of its Web Site and was in the process of implementing a redesign of its Web site to ensure that all content meets Section 508 standards.
- **DACS – e-Gov Service Center** – DACS provided scans from a computer application designed to examine compliance with Section 508 of the e-Gov Service Center application. The scans indicated compliance with Section 508 standards for the components of the application maintained by DACS. However, DACS was still negotiating with the credit card vendor to bring the Web pages maintained by the vendor and used to enter credit card payments within the e-Gov Service Center application into compliance with Section 508 standards.
- **DFS – Web Site** –Although DFS did not provide documentation of being fully compliant with Section 508, it maintained an IT Section 508 compliance policy to promote conformity with Section 508 requirements. Also, as of June 10, 2005, DFS was in the process of deploying a content management system, which it indicated would automate the task of enforcing compliance with Section 508 standards by providing compliant Web page templates for all staff to use.
- **DFS – Filing Assembly Submission System** – DFS indicated that it had requested the vendor supporting the e-Gov application to initiate a Section 508 compliance scan.
- **FWC – Web Site** – FWC posted accessibility guidelines for application developers to follow for new development and planned to engage a vendor to make Web site changes for full compliance.
- **FWC – Total Licensing System** – There were no contract provisions requiring FWC's vendor to deliver the Total Licensing System in a format compliant with Section 508. In response to our audit inquiries, FWC staff indicated that alternate methods existed for the sale of licenses by agents, such as those in retail stores, and by telephone.
- **DOH – Web Site** – Although DOH did not provide documentation of being fully compliant with Section 508, it maintained an IT Section 508 compliance policy as a method to promote conformity with Section 508 requirements and planned to deploy a content management system.
- **DOH – Medical Quality Assurance (MQA)** – DOH acknowledged that MQA was not fully Section 508 compliant. DOH had established a goal of meeting Section 508 accessibility standards during MQA's development and was continuing its efforts to make the application compliant.

[9] Executive Order Number 01-161

- **DHSMV – Web Site** – DHSMV had begun the process of using tools to scan its Web site to determine which Web pages were not in compliance.
- **DHSMV – Express Lane** – While DHSMV indicated that it offered alternate methods to transact business, such as by telephone, those methods do not comply with the requirements of the STO Enterprise Standard, Portal Coding and Design.
- **DMS – MyFloridaMarketPlace (MFMP)** – DMS determined that selected components of MFMP did not meet Section 508 accessibility requirements. During our audit period, the responsibility for remediation costs had not been determined since DMS's contract with the vendor supplying the components did not contain specific language requiring delivery in a compliant format.
- **DMS – People First** – To be Section 508 compliant, the State employment application process available at the People First Web site required additional coding that would allow assistive technologies to decipher text on the Web site and convert the text to verbal instructions for the visually-impaired user. Although alternate methods existed for visually-impaired users, such as filling out and submitting paper applications for employment or utilizing telephone support, these methods do not comply with the requirements of the STO Enterprise Standard, Portal Coding and Design. Additionally, DMS had not determined who was responsible for the remediation costs since its contract for the e-Gov application did not contain specific language requiring Section 508 compliance.
- **DOT – Web Site** – DOT had integrated software to scan its Web site to assist in remediation of non-compliant Web pages. However, the Web site was not fully compliant with Section 508 standards.

Recommendation: The aforementioned agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, as appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.

Finding No. 2: Coding and Design Standards

During our audit period, the STO Enterprise Standard, Portal Coding and Design[10], governed specific coding and design functions for executive branch agency Web sites. For example, the standard specified that the MyFlorida logo (hyperlinked to the MyFlorida home page) would appear in the upper left-hand corner of every Web page. The inclusion of the hyperlink was to provide users with a consistent method to access the State portal from any agency Web site. Additionally, the MyFlorida.com logo was to present users with a visual cue that the Web site they were visiting was a State agency Web site. The standard also required the placement of an agency privacy statement hyperlinked on all pages within a Web site.

We compared the coding and design of agency Web sites to selected components of the enterprise standard. Our comparison disclosed the following instances where the standard was not followed:

- DACS placed the MyFlorida.com hyperlink on the bottom left of the Department's home page. DACS considered itself exempt from the requirements of the enterprise standard because it was headed by a Cabinet Officer.
- DFS did not display the MyFlorida.com hyperlink on all pages within its Web site.
- Although FWC had placed the MyFlorida.com logo on the footer of all Web pages, it was in the process of redesigning its Web site and stated that it would reposition the MyFlorida.com hyperlink during the redesign.

[10] STO-2-72-006, Enterprise Standard, Portal Coding and Design

- DOT did not provide a link to its privacy statement on each page of its Web site.

Recommendation: The above-listed agencies should comply with the provisions of the State Enterprise Standard in the areas described above.

Finding No. 3: Web Site Content Management Strategy

A content management strategy generally utilizes a central management authority, such as an enterprise Webmaster or Web team, and may include a content management system, to help ensure that policies and procedures for Web development are consistently followed throughout a Web site. The content management strategy may include provisions to ensure that all Web pages meet the agency Web design standards and provide for a standard look of the Web pages whereby certain components such as menus and information hyperlinks carry the same design style throughout the Web site. An enterprise Webmaster or Web team usually establishes the overall Web site design, manages Web development, and remains current on Web site compliance issues, while additional staff is responsible for constructing and maintaining specific Web pages. A content management system is an automated control method used to manage Web site content through the adoption of Web page templates that allow a central management of content.

All agencies included in our audit tests maintained diverse management techniques to control the creation, modification, and deployment of Web pages presented on the Internet. Each agency maintained a principal Webmaster responsible for coordinating the home page and core aspects of the agency Web site structure. Each agency also employed multiple individuals with the capability to create and manage selected agency Web pages, relying on high-level Web design standards and procedures to direct the activities of those individuals. Certain agencies utilized additional control procedures, which included the use of public information officers to review new Web pages prior to deployment. Additionally, DHSMV maintained a policy whereby an agencywide Web team was established to supervise all Web activities. Nonetheless, other than DHSMV, no agencies tested had a management-approved written Web site content management strategy including the designation of a central management authority, such as an enterprise Webmaster, or empowered a Web team to actively manage all agency Web development. Two agencies, however, as previously mentioned in Finding No. 1, were either planning or in the process of deploying a content management system.

The absence of a Web site content management strategy, including a central management authority at each agency with knowledge of Web site compliance issues, may have contributed to our two previously-mentioned findings. For example, as discussed in Finding No. 1, certain Web sites and e-Gov services needed enhancement to be accessible by people with disabilities. However, the decentralized management structure utilizing multiple individuals creating and updating Web page content without a compensating control, such as a content management system, may have contributed to certain Web pages within agencies' Web sites not meeting accessibility standards. The decentralized management structure may also have contributed to the coding and design standards not being consistently followed, as described in Finding No. 2.

Recommendation: All agencies should develop a content management strategy to provide increased assurance of maintaining Web site content that is consistent with management's intent.

Finding No. 4: Data Privacy Response Procedures

Maintaining e-Gov applications involves a risk that stored personal identification information could be obtained and ultimately used in an identity theft crime. News media reports involving data security breaches illustrate

conditions that could result in an agency's loss of control over confidential user information, including an incident in Florida where a former Convergys[11] employee obtained confidential information from the State's People First application and perpetrated identity theft.

Excluding the STO, which only maintained the MyFlorida.com Web site, the six agencies providing e-Gov applications included in our audit tests kept written security policies and procedures, privacy policies, active monitoring, electronic counter-measures, and Computer Incident Response Teams to limit the risk of personal identification information theft. However, written procedures were not completely developed for a response strategy to be followed if personal identification information was compromised in a security breach. We noted the following:

- DFS, DHSMV, and DOT had not established complete written procedures for a response strategy.
- Although an inventory of personal identification information captured in its e-Gov application was maintained by DACS, with data privacy activities being coordinated by the DACS Information Security Officer and other staff members, written procedures for a response strategy had not been developed.
- Contract provisions specifying that a response strategy be followed by the vendor, if security breaches involving personal identification information occur, were not included in the FWC's contract for its Total Licensing System e-Gov application.
- Although DOH's General Counsel had been involved in developing a response strategy for DOH and data privacy activities were being coordinated by DOH's privacy officer, written procedures for a response strategy had not been developed.

A new Florida law[12], effective July 1, 2005, addresses security breaches of confidential personal information in third-party possession. The law requires persons conducting business in Florida and maintaining computerized data in a system that includes personal information to provide notice of any breach of the system's security to any Florida resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law further requires that, in part, notification be made without unreasonable delay and no later than 45 days following the determination of the breach unless specific exclusions apply. Although this law became effective subsequent to our review of the agencies' response strategies, it is incumbent upon all agencies to maintain written procedures to ensure a proper response to any data security breaches of confidential data maintained in support of e-Gov services.

Recommendation: All agencies should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida law, to be followed if the security over confidential personal identification information is breached.

Finding No. 5: Hyperlink Deficiencies

Web hyperlinks transport users from highlighted text or images on a Web page to either another place on the same Web page or to an entirely different Web page.

We noted that all seven agency Web sites tested contained Web pages with broken hyperlinks that took users either to error pages when the hyperlinked page no longer existed or to redirect pages that transported the user to another Web page to view the link content. Also, selected hyperlinks directed users to Web pages that no longer contained material matching the hyperlink description.

[11] Convergys is the contractor to whom the State's human resources functions (People First) were outsourced.
[12] Section 817.5681(1)(a), Florida Statutes (2005)

Agencies utilized various automated applications to search their Web sites for broken hyperlinks; however, there were limitations to this approach. These applications could only reliably detect bad hyperlinks if a Web page did not exist. The applications did not consistently warn the Webmaster when a Web site did not allow link checking applications to run against it, when redirect pages were used, or when Web page content no longer matched the hyperlink description on the agency Web page.

Additionally, we noted that all agencies utilized hyperlinks within their Web sites transporting users to Web pages or content that was not maintained, contracted, or controlled by the agencies or other State entities. Examples included hyperlinks within the DFS Web site to Weather.com and the United States Small Business Administration. However, not all agencies maintained adequate disclaimer statements to caution users that certain hyperlinks could route the users to third-party Web sites, the content of which would be beyond the control of the agency or other State entities.

Specifically, our audit tests disclosed the following:

- Disclaimer statements had not been developed by DFS for its Web site or by the STO for the MyFlorida.com Web site.
- Although DOT maintained a disclaimer statement on its Web site, the statement did not explicitly address the use of links to Web content outside of DOT's control.

While maintaining hyperlinks to outside sites can complement agency Web content, the hyperlinks can also result in users accessing content that may be inappropriate to the agency or infer agency approval of advertisements presented on the hyperlinked page. Also, the lack of controls to limit broken and incorrect hyperlinks could reduce the usability of the Web sites.

Recommendation: Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

Finding No. 6: Web Domain Management

When typed into a browser, a Web domain name is an alphanumeric representation of a numeric Internet Protocol (IP) address used by the Internet to direct a user to a Web site. Domain names represent valuable assets to owners who establish an association to an organization, product, or service. For example, the State has incorporated *MyFlorida.com* into Florida license plates to associate the domain name as the link to the State's official information portal. The agencies in our audit utilized a mix of *.com* and *.state.fl.us* suffixes as their top-level domain names.

All agencies maintained inventories of domain names used for different e-Gov services or held for future Web projects. Domain names were purchased from registrars who sell and administer specific top-level domains. Maintaining ownership of domain names requires active administration of the accounts set up by the agencies with their selected registrar, including maintaining current contact information. The use of written procedures helps to control this process. Failure to properly administer domain name accounts could result in loss of ownership of a domain name, through non-renewal of the domain name, resulting in possible economic loss or damage of image should a new owner use the domain name to publish objectionable content.

We noted the following deficiencies regarding Web domain management:

- Written procedures to manage the acquisition, monitoring, and renewal of Web domain inventory were not maintained by DFS, STO, and DOT.
- A person no longer associated with the STO was listed as the technical contact name for the MyFlorida.com registration during our audit period.

Recommendation: Agencies should maintain current, written procedures for the acquisition, monitoring, and renewal of their domain names, including, at a minimum, procedures to ensure the automatic renewal of domain names and to maintain current contact information.

Finding No. 7: Emergency Event and Continuity Procedures for e-Gov Services

The delivery of information and services through State e-Gov services represents a relatively new technology that has grown in importance. Agency Web sites have become key communication portals to disseminate information during emergency events, such as hurricanes. E-Gov applications also represent an alternate method for users to transact business should the buildings supporting government services in certain geographic areas of the State become unusable due to natural disasters or terrorist activities. Therefore, it is important for agencies to retain written procedures to manage the availability of agency Web sites and e-Gov applications. Requirements for maintaining Web site availability during emergency events includes, for example, the need for network engineers to monitor and obtain additional communications capacity for increased traffic on the Web site; server support staff to build additional Web servers to accommodate the increased traffic; procedures for personnel responsible for supplying information to update the pages; review and approval of content changes; and ensuring that equipment is deployed in a secure manner. Additionally, agencies should consider continuity procedures for e-Gov equipment and network communications to ensure availability should conditions warrant moving operations to a backup site. Accordingly, the evaluation of the importance of e-Gov services is critical in each agency's identification of essential functions used to develop its IT disaster recovery plan. Further, testing and validating components of the plan determines the completeness of the plan and the organization's ability to recover and dispense e-Gov services.

Specific issues concerning the continuity of operations and IT disaster recovery planning were covered in our audit report No. 2006-038, dated October 2005. The following conditions regard emergency event and continuity procedures of selected e-Gov services that supplement the information contained in that report:

- DACS had not considered its Web site or e-Gov application as mission critical applications as of the date of the most recent testing of its IT disaster recovery plan. Therefore, neither service had been tested to verify the ability to operate the e-Gov services at its alternate site.
- DOT maintained procedures to react to emergency events, requiring the use of its Web site to disseminate information. However, it did not maintain a consolidated set of written procedures to guide this process. Additionally, DOT had contracted for disaster recovery services requiring the achievement of an IT conversion process prior to its ability to test central office functions, including e-Gov services. While DOT maintained a written plan for the recovery of e-Gov services, the testing of the plan had been suspended until the completion of this conversion process.
- DHSMV had received funding for the 2005-06 fiscal year to expand its disaster recovery operations and DHSMV had made it a priority to negotiate a contract through the STO for an alternate site to host the business recovery of its Web infrastructure. However, DHSMV had not considered its Web site or e-Gov application as mission critical applications as of the date of the most recent testing of its IT disaster recovery plan.
- FWC did not maintain complete written procedures documenting steps needed to maintain the availability of its Web site during emergency events. Further, FWC purchased Web hosting services from

the STO's Technology Resource Center, making DMS responsible for the availability of network and server equipment used to host its Web site. However, as of October 4, 2005, FWC was still negotiating with DMS regarding disaster recovery services.

- The STO maintained a contract for an outside vendor to provide recovery services for the equipment hosting its MyFlorida.com Web site. However, as of July 22, 2005, there were no written procedures for the recovery of the Web site, nor had the e-Gov services been tested at an alternate site.
- DOH had classified the Medical Quality Assurance application as a priority 3, mission essential application. This application had not had not been tested to verify the ability to recover this service at the alternate site during the most recent testing of the IT disaster recovery plan. However, DOH had scheduled the application for testing at the alternate site in 2006. DOH indicated that critical components of the DOH Web site had been tested in 2004 at an alternate site to verify the viability of their plan.
- DFS maintained generic procedures for its e-Gov applications in its IT Disaster Recovery Plan. The Filing Assembly Submission System was ranked as a medium priority item for recovery and therefore was not fully tested to validate recovery procedures at the contracted recovery site.

The absence of complete written procedures to ensure the availability and continuity of e-Gov services increases the risk that the agency may not timely or effectively disseminate critical information or services during an emergency event or recover from a disruption and resume e-Gov services deemed critical.

Recommendation: Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

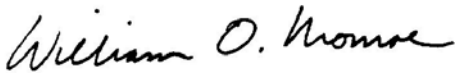
Finding No. 8: Security-Related Controls

The utilization of adequate security-related controls helps to ensure access to IT resources is properly restricted. We noted two instances where DHSMV's utilization of certain security-related controls need improvement. Specific details are not disclosed in this report to avoid the possibility of compromising agency information. However, appropriate agency personnel have been notified.

Recommendation: DHSMV should strengthen controls to provide increased assurance of the security and availability of its information resources.

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, CPA
Auditor General

MANAGEMENT RESPONSES

In letters dated December 21, 2005, through January 19, 2006, the heads of the applicable agencies provided responses to our preliminary and tentative findings. These letters are included at the end of this report as Appendix B.

APPENDIX LIST

APPENDIX A
WEB SITE HOME PAGE AND E-GOV APPLICATION URLS[13]
FOR AGENCIES INCLUDED IN OUR AUDIT

Web Site Home Page

Agency	URL
DACS	www.doacs.state.fl.us
DFS	www.fldfs.com
FWC	MyFWC.com
DOH	www.doh.state.fl.us
DHSMV	www.hsmv.state.fl.us
STO	MyFlorida.com
DOT	www.dot.state.fl.us

e-Gov Application

Agency	Application	Description	URL
DACS	e-Gov Center	On-line services, such as purchasing a subscription and license renewals for businesses	www.fl-ag-online.com
DFS	Filing Assembly Submission System	Portal for the electronic submission of documents by the insurance industry	iportal.fldfs.com/ifile/
FWC	Total Licensing System	On-line purchase and renewal of hunting and fishing licenses and permits	www1.wildlifelicense.com/fl/
DOH	Medical Quality Assurance	On-line services for medical licensees, health care businesses, and others	ww2.doh.state.fl.us/mqaservices
DHSMV	Express Lane	On-line renewal and address changes for drivers licenses, ID cards, and mobile home, vessel, and vehicle registrations	express.hsmv.state.fl.us
DMS	MyFloridaMarketPlace	On-line State procurement system	dms.myflorida.com/dms/purchasing/myfloridamarketplace
DMS	People First	On-line personnel system for State employees, managers, and job seekers	peoplefirst.myflorida.com
DOT	SunPass	On-line services for prepaid toll program	www.sunpass.com

[13] Uniform Resource Locator (URL): The global address of the Web site or e-Gov application on the Internet.

APPENDIX B

MANAGEMENT RESPONSES

Jeb Bush
Governor

M. Rony François, M.D., M.S.P.H., Ph.D.
Secretary

December 21, 2005

Mr. William O. Monroe, C.P.A.
Auditor General
Room G74, Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

This letter is in response to your December 8 correspondence regarding the preliminary and tentative findings of your report entitled, *Information Technology Audit of Selected State Agencies' Public Web Sites.* The agency's response and corrective action plans to your findings and recommendations may be found in the enclosed document.

We appreciate the work of your staff and will diligently pursue appropriate resolution to the findings.

If I may be of further assistance, please let me know.

Sincerely,

M. Rony François, M.D., M.S.P.H., Ph.D.
Secretary, Department of Health

MRF/kir
Enclosure

4052 Bald Cypress Way • Tallahassee, FL 32399

	Finding	*Recommendation*	*Management's Response*	*Corrective Action Plan*
1	Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.	DOH should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, DOH should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. DOH should consult, as appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.	The Florida Department of Health concurs with the finding and is committed to providing accessible web sites and E-gov services to the citizens of the State of Florida and all our online visitors. In January of 2004, Dr. Agwunobi signed the IT Section 508 compliance policy into effect to ensure all elements and entities of the agency provide accessible information and services via the Internet. At the time of the audit the FDOH web site was 86 percent accessible to individuals who use assistive technology and a report produced with HiSoft ACC Monitor & Verify accessibility software was provided to the auditor. The Florida Department of Health was an active participant in the MyFlorida Portal Knowledge Domain group which produced the current State Technology Office Portal Coding and Design standards document (STO-2-72-006), and maintains an active voice and level of participation in enterprise wide meetings such as the ADAWG and the Governor's Accessible Electronic and Information Task Force. The Florida Department of Health continues to make every effort to ensure full web and application accessibility with a planned implementation of a content management system and modifications for accessibility to existing applications. All future contracts and service level agreements will include specified accessibility requirements.	The Florida Department of Health will remain fully committed to improving existing services and providing accessible information to our online visitors. FDOH will continue to participate and benefit from our association with ADAWG and the Governor's Accessible Electronic and Information Task Force in order to achieve full accessibility.

	Finding	*Recommendation*	*Management's Response*	*Corrective Action Plan*
3	Agencies lacked written Web content management strategies for ensuring the integrity of Web site content.	DOH should develop a content management strategy to provide increased assurance of maintaining Web site content that is consistent with management's intent.	The Florida Department of Health concurs with the finding and recognizes the need for content management strategy.	The Florida Department of Health is currently in the process of implementing a content management system which will provide increased levels of operational continuity, ensure levels of accessibility, and provide a strategic approach to web content management with significant improvements to existing documented processes and procedures. This imminent implementation of a content management system will ensure agency leadership that all web content is consistent with the intent and mission of the agency.
4	The six agencies within the scope of the audit that had e-Gov applications either had not established written procedures, or had incomplete procedures, for response strategies to be followed if personal identification information was compromised in a security breach.	DOH should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida law, to be followed if the security over confidential personal identification information is breached.	As stated in the Preliminary and Tentative Audit Finding the law for the above requirement became effective subsequent to the review of our agency. Based on the new requirement of the law, we agree that our current polices do not completely meet these requirement at the present time.	The agency policy that governs the reporting of security breach of personal identification information is under review and will be revised to incorporate the requirement stated in chapter 817.5681 Florida Statues.

	Finding	*Recommendation*	*Management's Response*	*Corrective Action Plan*
5	We noted deficiencies in hyperlinks within the agencies' Web sites.	DOH should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also, disclaimer statements should be maintained on the Web site to alert users that certain hyperlinks to outside sources represent content not controlled by the agency and do not necessarily reflect the agency's views.	The Florida Department of Health concurs with the finding and recognizes the challenge of external hyperlinks and currently maintains a legal disclaimer.	The Florida Department of Health is currently in the process of implementing a content management system which will provide increased levels of operational continuity, ensure levels of accessibility, and provide a strategic approach to web content management with significant improvements to existing documented processes and procedures. A content management system will provide the capability to ensure the viability and functionality of all internal hyperlinks. Hyperlinks to external sources which appear in agency web content are provided to our online visitors with an existing disclaimer located at -- http://www.doh.state.fl.us/rw_navigation/disclaimer.htm

	Finding	*Recommendation*	*Management's Response*	*Corrective Action Plan*
7	Written procedures had not been fully developed by several agencies for maintaining Web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.	DOH should establish written procedures to ensure the ability to respond effectively to emergency events via their Web site. Further, if DOH is not maintaining written e-Gov recovery procedures, the agency should reevaluate these services for possible inclusion in their IT disaster recovery plan to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.	DOH concurs with the finding listed: Current state of DOH bandwidth and infrastructure as of December 2005: DOH has upgraded its connection to the State backbone in order to improve our accessibility during periods of high demand. Additionally, DMS has upgraded and continues to upgrade the State internet. This increased capacity should ensure that ALL state agencies have sufficient bandwidth to sustain high demand situations created by emergency events. In addition, DOH has expressed to DMS a desire to add a second interface for redundancy of infrastructure. DMS has agreed to work with DOH to develop a cost model for providing the additional interface. The current state of DOH infrastructure demonstrates an actively improving structure continually changing to meet demand. Procedure in the case of emergency events demanding increased service: In a DOH emergency, the Division of Information Technology would submit the online request according to the State process, call DMS, and participate in a conference call meeting. In a State-declared emergency, Information Technology will also notify ESF2. Strategic planning for selected critical applications: Selected systems classified as critical to government operations are duplicated in the DOH disaster recovery environment. Once a system is duplicated, DOH can apply load balancing techniques to divide service between the two environments during periods of high demand. For each system that qualifies for the duplication and load balancing service, DOH management must make a decision based on criticality and cost. An example of a DOH system which demands duplication and load balancing is the Merlin Communicable Disease Surveillance System.	Written procedures to manage the availability of agency Web sites and e-Gov applications during periods of high demand created by emergency events will be added to the Agency's disaster recovery documents. Written procedures for classifying, monitoring, and taking load balancing action for selected systems will be added to the Agency's disaster recovery documents.

Finding	*Recommendation*	*Management's Response*	*Corrective Action Plan*
		DOH is actively addressing the recovery of e-Gov services in their IT disaster recovery plans as follows: DOH agency management has classified all applications, inclusive of e-Gov services, by criticality and the corresponding recovery time frame appropriate to the classification. Recovery category levels 1, 2, and 3, the most crucial categories for availability and need, have recurring testing schedules. Schedule of testing for Recovery Categories 1, 2, and 3: --Categories 1 and 2 have completed initial recovery tests. --Categories 1 and 2 are scheduled for re-test in January and February of 2006. --Categories 1, 2, and 3 are scheduled for re-test and initial test in May of 2006.	

Florida Department of Transportation

JEB BUSH
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

DENVER J. STUTLER, JR.
SECRETARY

January 5, 2006

William O. Monroe, CPA
Auditor General
Office of the Auditor General
Room G74, Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning the audit of:

Selected State Agencies' Public Web Sites
July 2004 through June 2005

As required by Section 11.45(4)(d), Florida Statutes, our response to the findings is enclosed.

We appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact Cecil Bragg, our Inspector General, at 410-5800.

Sincerely,

Denver Stutler, Jr., P.E.
Secretary

DS:hmt

Enclosure

cc: Cecil Bragg, Inspector General

Finding No. 1: Accessibility of e-Gov Services

Finding: DOT had integrated software to scan its Web site to assist in remediation of non-compliant Web pages. However, the Web site was not fully compliant with Section 508 standards.

Recommendation: The agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, as appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.

Department Response: The department has implemented processes to initiate scanning of department web sites to ensure section 508 compliance. Scans are run monthly and the FDOT Webmaster works directly with web authors and owners to coordinate the correction of any compliance issues. As of the December 2005 run, our scans showed that 86% of FDOT Internet web sites met compliance standards, up 16% from the June scan. The Webmaster team will continue to work with web owners and authors to improve this percentage. Also, early in 2006 we will begin providing Section 508 reviews for the department's intranet sites in addition to the Internet sites.

Finding No. 2: Coding and Design Standards

Finding: DOT did not provide a link to its privacy statement on each page of its Web site.

Recommendation: The agencies should comply with the provisions of the State Enterprise Standard in the areas described above.

Department Response: The department developed a revised privacy statement based on feedback from the AG's office and included the link on the department's Internet home page. The Webmaster team will work with the department's web authors and owners to have the link posted on all Internet web site pages.

Finding No. 3: Web Site Content Management Strategy

Finding: Agencies lacked written Web content management strategies for ensuring the integrity of Web site content.

Recommendation: All agencies should develop a content management strategy to provide increased assurance of maintaining Web site content that is consistent with management's intent.

Department Response: The department has incorporated Web Standards into its department procedures for Information Technology Resource Standards and has created a web standards workgroup to facilitate the creation and maintenance of documented web standards within the department. Intranet static web design standards were the first area addressed as a department standard. Content management will be addressed through this process.

Finding No. 4: Data Privacy Response Procedures

Finding: DFS, DHSMV, and DOT had not established complete written procedures for a response strategy.

Recommendation: All agencies should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida law, to be followed if the security over confidential personal identification information is breached.

Department Response: The department does not have an extensive portfolio of e-government applications where this particular finding is focused. However, we do agree that written procedures should be in place to address a response to security breaches of confidential personal information. The department will develop and adopt procedures addressing this area pursuant to Chapter 817, Florida Statutes.

Finding No. 5: Hyperlink Deficiencies

Finding: Although DOT maintained a disclaimer statement on its Web site, the statement did not explicitly address the use of links to Web content outside of DOT's control.

Recommendation: Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

Department Response: The department's disclaimer statement has been revised and posted on our Internet web site.

Finding No. 6: Web Domain Management

Finding: Written procedures to manage the acquisition, monitoring, and renewal of Web domain inventory were not maintained by DFS, STO, and DOT.

Recommendation: Agencies should maintain current, written procedures for the acquisition, monitoring, and renewal of their domain names, including, at a minimum, procedures to ensure the automatic renewal of domain names and to maintain current contact information.

Department Response: Based on recommendations by the AG, the department has obtained a written procedure from the Department of Highway Safety and Motor Vehicles. Work is underway to modify and adopt it as a department procedure for web domain management.

Finding No. 7: Emergency Event and Continuity Procedures for e-Gov Services

Finding: DOT maintained procedures to react to emergency events, requiring the use of its Web site to disseminate information. However, it did not maintain a consolidated set of written procedures to guide this process. Additionally, DOT had contracted for disaster recovery services requiring the achievement of an IT conversion process prior to its ability to test central office functions, including e-Gov services. While DOT maintained a written plan for the recovery of e-Gov services, the testing of the plan had been suspended until the completion of this conversion process.

Recommendation: Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

Department Response: The department does not have an extensive portfolio of e-government applications and the department's IT disaster recovery plan includes recovery components for our web infrastructure. The conversion of the plan to Sungard's format has been completed and the department is now reviewing and updating the plan in the new format. Testing is being scheduled at Sungard's facilities each year based on an allocation of time through the Sungard contract in conjunction with establishing priorities for testing various components of our applications and infrastructure.

CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

TOM GALLAGHER

January 6, 2006

Mr. William O. Monroe
Auditor General
State of Florida
Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings and recommendations which may be included in a report to be prepared on the Auditor General's Information Technology Audit of Selected State Agencies' Public Web Sites.

If you have any questions or would like to discuss the matter further, please contact David Harlan, Inspector General at (850) 413-4960.

Sincerely,

Tom Gallagher

TG:Hc

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 • TELECOPIER (850) 413-2950

Florida Department of Financial Services
Audit Response
Selected State Agencies'
Public Web Sites
Information Technology Audit
Preliminary and Tentative Audit Findings

Finding No. 1: Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.

Recommendation: The aforementioned agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.

Response: As the Auditor General's findings reflected in their Information Technology Audit for the period from July 2004 through July 2005, Section 508 of the Rehabilitation Act of 1973 applies only to Federal departments and agencies. In that audit report, it was further cited that the STO Enterprise Standard for Portal Coding and Design was not issued as a rule, and the authority of the STO to impose this requirement is unclear.

Executive Order Number 05-133 issued by the Executive Office of the Governor created the Governor's Accessible Electronic and Information Technology Task Force (Task Force) to provide guidance in improving the accessibility of the state's electronic and information technology to persons with disabilities. The order directed all agencies under the authority of the Governor and requested all other agencies to use reasonable efforts to comply with Section 508 standards when purchasing and implementing electronic and information technology.

The Department of Financial Services (DFS) has voluntarily created official Department guidelines based on the MyFlorida web design standards which reference Section 508 accessibility requirements. In addition, DFS has developed a draft policy for web design standards to promote Section 508 accessibility enterprise-wide; the anticipated timeframe for approval of this policy is during the second quarter of CY 2006. DFS also currently provides compliant web page design templates and is continuing its deployment of a content management solution.

Recognizing the importance of statewide ADA compliance, DFS is an active participant in the efforts of the Task Force and is coordinating efforts with both the Task Force members and the Americans with Disabilities Act Working Group (ADAWG) staff. ADAWG has assisted with analysis and feedback of Project Aspire for ADA compliance review and DFS' current web

content and applications for further recommendations. DFS' participation in the Task Force is significant in that the Aspire Project has been recognized as one of four major Web-based applications under review for ADA compliance. DFS has assisted the Task Force by providing multiple presentations regarding the Aspire project status and DFS' approach to ADA compliance. In addition DFS has provided professional industry presentations and input from Oracle/PeopleSoft experts regarding the implementation of ADA compliance in conjunction with applications development. DFS has also contributed language for Task Force recommendations to the Governor for potential model legislation to be considered in 2006. Upon implementation of such legislation, DFS would be positioned to become a statewide leader in meeting Section 508 compliance.

Finding No. 2: Certain STO enterprise standards for coding and design of Web sites were not consistently followed.

Recommendation: The above-listed agencies should comply with the provisions of the State Enterprise Standard in the areas described above.

Response: DFS has placed the MyFlorida logo and hyperlink on the www.fldfs.com home page. During the fourth quarter of CY 2005, DFS converted 90% of its original web pages to newly designed templates which automated the process of placing the privacy statement hyperlink on every page by default. The estimated completion for converting the remaining 10% of DFS' web pages is first quarter of CY 2006.

Finding No. 3: Agencies lacked written Web content management strategies for ensuring the integrity of Web site content.

Recommendation: All agencies should develop a content management strategy to provide increased assurance of maintaining Web site content that is consistent with management's intent.

Response: The Department is currently developing its written content management strategy which includes a Web Committee that has been established to serve as the Department's central management authority. The Committee will enforce DFS' content management and web standards via approval and implementation of its policy (which is currently in draft status). The Department's strategy also includes an automated content management solution to enforce compliance through Web page templates.

Finding No. 4: The six agencies within the scope of audit that had e-Gov applications either had not established written procedures, or had incomplete procedures, for response strategies to be followed in personal identification information was compromised in a security breach.

Recommendation: All agencies should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida law, to be followed if the security over confidential personal identification information is breached.

Response: By the end of the first quarter of CY 2006, DFS will establish a management-approved written response strategy that will be followed if the security over confidential personal identification information is breached.

Finding No. 5: We noted deficiencies in hyperlinks within the agencies' Web sites.

Recommendation: Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

Response: DFS periodically performs review and analysis of hyperlinks and forwards all findings to agency Web content managers for correction. DFS is in the process of developing a disclaimer statement to be placed on the www.fldfs.com website during the first quarter of CY 2006.

Finding No. 6: Current written procedures for managing Web domain names were not maintained by all agencies.

Recommendation: Agencies should maintain current, written procedures for the acquisition, monitoring, and renewal of their domain names, including, at a minimum, procedures to ensure the automatic renewal of domain names and to maintain current contact information.

Response: The Department has an electronic diary system in place which provides advance and real-time notification of expirations and automated renewals. In addition, DFS performs quarterly reviews of all departmental domain name registrations. By the end of second quarter of CY 2006, DFS will develop written procedures to document its processes for the acquisition, monitoring, and renewal of domain names.

Finding No. 7: Written procedures had not been fully developed by several agencies for maintaining Web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.

Recommendation: Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

Response: Recently, DFS has successfully tested and recovered several of its major e-Gov services and recognizes the importance of their availability and recoverability. Because DFS understands the critical need for complete recovery of these types of services a consultant was

hired to perform a professional risk analysis for the Department's most critical applications. The risk analysis was completed in December 2005. By the end of the second quarter of CY 2006, the Department will conclude its review of the risk analysis. This review will enable the Department to determine an approach which will include development of written procedures to be added to DFS' Disaster Recovery Plan to ensure the availability and effective recovery of these services in an emergency.

State of Florida
DEPARTMENT OF
HIGHWAY SAFETY AND MOTOR VEHICLES

FRED O. DICKINSON
Executive Director

JEB BUSH
Governor

CHARLIE CRIST
Attorney General

TOM GALLAGHER
Chief Financial Officer

CHARLES H. BRONSON
Commissioner of Agriculture

January 6, 2006

Mr. William O. Monroe, CPA
Auditor General
State of Florida
111 West Madison Street
Tallahassee, Florida 32302-1735

Dear Mr. Monroe:

Enclosed is a copy of this agency's response to the preliminary and tentative audit findings regarding your information technology audit of Selected State Agencies' Public Web Sites, for the period July 2004 through June 2005 and selected actions through October 2005.

If you should need additional information, please contact Mr. Laurence W. Noda, Inspector General, at 488-1407.

Sincerely,

Fred O. Dickinson
Executive Director

FOD/gc
Enclosure

■ FLORIDA HIGHWAY PATROL ■ DRIVER LICENSES ■ MOTOR VEHICLES ■ ADMINISTRATIVE SERVICES ■
Neil Kirkman Building, Tallahassee, Florida 32399-0500
http://www.hsmv.state.fl.us/

Department of Highway Safety & Motor Vehicles
Response to Auditor General's Preliminary and Tentative
Audit Findings for Selected State Agencies' Public Web Sites

Finding No. 1:
Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.

Recommendation:
The aforementioned agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, as appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.

Department Response:
DHSMV has used an automated tool to confirm ADA compliance for the main entry pages on the Department's web site, including the main pages for the Driver License, Motor Vehicles, and FHP portions of the web site. The Department has recently obtained and installed the ADA compliance toolsets utilized by the Governor's Working Group on the ADA - Real Choice Partnership Project (HiSoftware's ACCVerify and ACCRepair). DHSMV staff is currently using this tool with the Department's public facing web site and web-enabled applications with the goal of full ADA compliance for these sites during the 1st quarter of CY2006. Additionally, the vendor (HP) for the GoRenew web application has likewise obtained this tool, and the ADA enhancements for GoRenew are scheduled to be installed with the software enhancement release currently planned for March 2006.

Finding No. 4:
The six agencies within the scope of audit that had e-Gov applications either had not established written procedures, or had incomplete procedures, for response strategies to be followed if personal identification information was compromised in a security breach.

Recommendation:
All agencies should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida law, to be followed if the security over confidential personal identification information is breached.

Department Response:
DHSMV is formalizing its strategy by drafting a "Breach of Confidential Personal Data Response Procedure", with the goal of completion during the 1st quarter of CY2006.

Finding No. 5:
We noted deficiencies in hyperlinks within the agencies' Web sites.

Recommendation:
Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

Department of Highway Safety & Motor Vehicles
Response to Auditor General's Preliminary and Tentative
Audit Findings for Selected State Agencies' Public Web Sites

Department Response:
DHSMV fixes broken hyperlinks as they are detected; however, the audit identified the need to address a broader range of hyperlink issues. A DHSMV web team is developing a plan to strengthen its web site management processes. The target period for plan completion is the 1st quarter CY2006. Additionally, DHSMV has placed an appropriate Disclaimer page on its web site to alert and warn users regarding links to external entities.

Finding No. 7:
Written procedures had not been fully developed by several agencies for maintaining Web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.

Recommendation:
Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

Department Response:
DHSMV has developed Emergency Event Web Procedures and will continue to expand these procedures as need and functionality dictate and permit. The Department has ranked the priority of the GoRenew e-Gov function as being low in a disaster scenario (i.e., low is defined as not needed within 30 days) based on current driver licensing workflow. However, the DHSMV is actively in the process of purchasing and installing the infrastructure necessary to support its public facing web site and internally-developed web applications at the DMS Shared Resource Center, with anticipated completion in the 2nd quarter CY2006.

Finding No. 8:
In two instances improvements are needed in security-related controls at DHSMV.

Recommendation:
DHSMV should strengthen controls to provide increased assurance of the security and availability of its information resources.

Department Response:
DHSMV is appropriately addressing the confidential recommendations.

FLORIDA FISH AND WILDLIFE CONSERVATION COMMISSION

January 6, 2006

Mr. William O. Monroe
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

RE: Preliminary and Tentative Audit Findings for the Information Technology Audit of Selected State Agencies' Public Web Sites

Dear Mr. Monroe:

We have reviewed the preliminary and tentative audit findings and recommendations included with your letter dated December 8, 2005. Please find enclosed our responses to the six audit findings related to our agency.

We appreciate the constructive comments and technical assistance provided by your staff. If further information is required, please contact our Director of Auditing, Trevor Phillips, at 488-6068.

Sincerely,

for Kenneth D. Haddad
Executive Director

kh/tp

Enclosures

INFORMATION TECHNOLOGY AUDIT
SELECTED STATE AGENCIES' PUBLIC WEB SITES
FLORIDA FISH & WILDLIFE CONSERVATION COMMISSION (FWC) RESPONSE

Finding No. 1: Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.

- FWC – Web Site – FWC posted accessibility guidelines for application developers to follow for new development and planned to engage a vendor to make Web site changes for full compliance.
- FWC – Total Licensing System – There were no contract provisions requiring FWC's vendor to deliver the Total Licensing System in a format compliant with Section 508. In response to our audit inquiries, FWC staff indicated that alternate methods existed for the sale of licenses by agents, such as those in retail stores, and by telephone.

Recommendation: The aforementioned agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, as appropriate, with the ADAWG and the Governor's Accessible Electronic and Information Technology Task Force to achieve these objectives.

FWC Response: We concur. FWC recognizes the need to provide accessibility to our web sites for people with disabilities and is fully committed to complying with the Governor's Executive Order Number 05-133. We have implemented/will implement the AG's recommendations by taking the following steps:

- Incorporating compliance verification reports into normal site maintenance activities. FWC utilizes ACCVerify in-house and ACCMonitor through the DMS MyFlorida Portal Team. Each of these software tools provides reports on MyFWC.com, and related Commission Web sites for ADA compliance. The Commission's Web Services Section will run these reports monthly, and make appropriate code changes for the compliance.
- Ensuring future FWC e-Gov service contracts require the service to meet Section 508 accessibility requirements.
- Consulting with the ADAWG and the Governor's AEITTF, as appropriate.
- Ensuring that FWC's RFP for a new Web Content Management System states that the selected CMS system must facilitate ADA compliance with Section 508.
- Adding an item to the Total License System's vendor's 2006 Work Plan to make the Internet portion of the system compliant with Section 508 and Executive Order 05-133.

620 South Meridian Street • Tallahassee • FL • 32399-1600
Visit MyFWC.com

Finding No. 2: Certain STO enterprise standards for coding and design of Web sites were not consistently followed.

- Although FWC had placed the MyFlorida.com logo on the footer of all Web pages, it was in the process of redesigning its Web site and stated that it would reposition the MyFlorida.com hyperlink during the redesign.

Recommendation: The above-listed agencies should comply with the provisions of the State Enterprise Standard in the areas described above.

FWC Response: We concur and recognize the importance of state-wide web standards. We have implemented/will implement the AG's recommendations by taking the following steps:

- The Commission banner was revised to add the MyFlorida logo into the banner with the hyperlink clicking to the MyFlorida.com.
- In future designs FWC will have the MyFlorida logo prominently placed on each page of the website.

Finding No. 3: Agencies lacked written Web content management strategies for ensuring the integrity of Web site content.

Recommendation: All agencies should develop a content management strategy to provide increased assurance of maintaining Web site content that is consistent with management's intent.

FWC Response: We concur and will implement the AG recommendation by issuing a Request for Proposals for a Web Content Management System. Implementation is planned for fiscal year 06-07.

Finding No. 4: The six agencies within the scope of audit that had e-Gov applications either had not established written procedures, or had incomplete procedures, for response strategies to be followed if personal identification information was compromised in a security breach.

- Contract provisions specifying that a response strategy be followed by the vendor, if security breaches involving personal identification information occur, were not included in FWC's contract for its Total Licensing System e-Gov application.

Recommendation: All agencies should establish and maintain a management-approved written response strategy, consistent with the requirements of Florida

620 South Meridian Street • Tallahassee • FL • 32399-1600
Visit MyFWC.com

law, to be followed if the security of confidential personal identification information is breached.

FWC Response: We concur. We have implemented/will implement the AG's recommendations by taking the following steps:

- Working with the contractor responsible for FWC's e-Gov application - Total Licensing System (TLS) - to set up formal procedures for notifying both the individuals affected, and the FWC, of any security breach involving the personal identification information collected by the TLS. This procedure will include:
  - Notifying Central Bank of Missouri that they will be subject to this Florida law as our contractor. Their compliance with the law after a personal information security breach would entail disclosing to FWC that a security breach involving personal information in TLS has occurred in accordance with section 817.5681(2)(a), Florida Statutes, and their notice to the individuals affected in accordance with section (6).
  - Asking them to formally acknowledge and agree to comply with the law
  - Asking them for details on how they intend to comply
  - Providing FWC with the template they will use to notify individuals of a breach, as well as providing their alternate support methods (web site, toll-free #). Reporting back to FWC after that notice had been successfully accomplished.
- Developing a general, agency-wide data privacy response procedure that will comply with section 817.5681(2)(a), Florida Statutes.

Finding No. 5: We noted deficiencies in hyperlinks within the agencies' Web sites.

Recommendation: Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

FWC Response: We concur. We have implemented/will implement the AG's recommendations by taking the following steps:

- FWC procedure is to run Hyperlink checks using HiSoftware Link Validation Utility and make corrections on a routine basis.
- The FWC Webmaster provides training for distributed Web Authors and has enlisted them to assist to periodically check every broken hyperlink within the agency's Website.
- Redirects were checked with Microsoft FrontPage and corrected as needed.

620 South Meridian Street • Tallahassee • FL • 32399-1600
Visit MyFWC.com

- Procedures include informing users that they are being redirected to another site either on MyFWC.com or to an external site.
- The Commission has posted an updated disclaimer regarding hyperlinks.
- Hyperlink issues will also be addressed as part of our new content management system.

Finding No. 6: Not Applicable to FWC

Finding No. 7: Written procedures had not been fully developed by several agencies for maintaining web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.

- FWC did not maintain complete written procedures documenting steps needed to maintain the availability of its Web site during emergency events. Further, FWC purchased Web hosting services from the STO's Technology Resource Center, making DMS responsible for the availability of network and server equipment used to host its Web site. However, as of October 4, 2005, FWC was still negotiating with DMS regarding disaster recovery services.

Recommendation: Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

FWC Response: We concur. We have implemented/will implement the AG's recommendations by taking the following steps:

- The Commission depends on DMS for its web site hosting services, including network connections and servers. FWC has asked DMS for an updated Service Level Agreement to include e-Gov recovery procedures. The Service Level Agreement with DMS should include disaster recovery services, since the Commission does not have on-site direct access to the hardware or backups for the website.
- Disaster recovery services will be included in future Service Level Agreements with DMS or other contracted hosted services.

Finding No. 8: Not Applicable to FWC

620 South Meridian Street • Tallahassee • FL • 32399-1600
Visit MyFWC.com

Florida Department of Agriculture and Consumer Services
CHARLES H. BRONSON, Commissioner
The Capitol • Tallahassee, FL 32399-0800

Please Respond to:
Office of Inspector General
Terry L. Rhodes Bldg, Ste., E
2005 Apalachee Parkway
Tallahassee, FL 32399-6500

January 6, 2006

William O. Monroe, CPA
Auditor General
111 West Madison Street
Claude Pepper Building, G-74D
Tallahassee, Florida 32399

Dear Mr. Monroe:

The following comments are provided in response to the preliminary and tentative findings and recommendations in your audit of "Public Web Sites" which included the Department of Agriculture and Consumer Services.

While the Department is included in several findings, none of the specific issues relative to us are considered to be major deficiencies. It is our belief that the Department's e-Gov services are generally being managed in an effective manner. Controls and security measures have been and will continue to be implemented where appropriate to provide reasonable assurance that our information is accessible and safeguarded.

Finding 1: Accessibility of e-Gov Services
Thanks for acknowledging the Department's efforts to have our Web Sites and e-Gov Service Center accessible to people with disabilities as required by Section 508. The adoption of standards, redesign of web sites, and compliance monitoring have contributed to a compliancy rate of 91% as of January 4, 2006. Efforts to improve and maintain accessibility to Department e-Gov services will be continued.

Finding 2: Coding and Design Standards
We have no further comments regarding the location of the MyFlorida.com hyperlink.

Finding 3: Web Site Content Management Strategy
The Department established a distributed (not decentralized) Web site management structure with standards set at the enterprise level and implementation responsibilities placed in the divisions. Web site content management is a daunting task assigned to our limited human resources. Efforts to identify and acquire a workable content management system have been unsuccessful to date but automation tools will continue to be evaluated to help compensate for the lack of sufficient human resources.

Finding 4: Data Privacy Response Procedures
While detailed procedures are not established for each type of potential security incident, the Department's Computer Security Incident Response Team would be quite capable of responding to a security breach to confidential information and meeting the notification requirements of Section 817.5681(1)(a), Florida Statutes. However given the recent focus on breaches to confidential personal identification information, the Department's response strategy will be reevaluated.

Finding 5: Hyperlink Deficiencies
Hyperlinks by their nature are problematic to control or monitor and automated tools have limited capabilities as noted. The Department will continue to review Web sites for broken or incorrect hyperlinks to the extent possible. Disclaimer statements are maintained on Department Web sites to alert users of issues regarding hyperlinks to outside sources.

Finding 6: Web Domain Management
No issues were identified for the Department of Agriculture and Consumer Services.

Finding 7: Emergency Event and Continuity Procedures for e-Gov Services
The Department is very proud of its disaster recovery planning and testing which is risk based and focused on mission critical applications. In fact, your recent audit of selected agencies Continuity of Operations and Information Technology Disaster Recovery Planning in October 2005 presented no adverse findings or issues of concern for this Department. The Department has recently elevated certain e-Gov services to mission critical status. Those applications will be subject to disaster recovery testing in 2006.

Finding 8: Security-Related Controls
No issues were identified for the Department of Agriculture and Consumer Services.

I appreciate the interest and efforts of your staff and the professionalism they exhibited in helping to improve operations of state government.

Sincerely,

CHARLES H. BRONSON
COMMISSIONER OF AGRICULTURE

CHB/gb

DEPARTMENT OF MANAGEMENT
SERVICES

"We serve those who serve Florida"

JEB BUSH
Governor

Tom Lewis, Jr.
Secretary

MyFlorida.com

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

Telephone:
850-488-2786

Fax:
850-922-6149

Internet:
www.MyFlorida.com

January 19, 2006

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

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our written response to your preliminary and tentative audit report, titled *Selected State Agencies' Public Web Sites Information Technology Audit.* The response corresponds with the order of your findings and recommendations in the preliminary audit report.

Finding No. 1: Accessibility of e-Gov Services

Agencies could not demonstrate that certain Web sites and e-Gov services were accessible to people with disabilities.

Recommendation:

The aforementioned agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508 accessibility requirements, as required by the STO Enterprise Standard and Executive Order 05-133. Further, agencies should, in future contracts for e-Gov services, include provisions for the delivered services to meet Section 508 accessibility requirements. The agencies should consult, as appropriate, with the ADAWG and the Governor' s Accessible Electronic and Information Technology Task Force to achieve these objectives.

Response:

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d, as amended) only applies to Federal agencies when they develop, procure, maintain, or use electronic and information technology. We do not believe there is any legal requirement for Florida to comply

with Section 508. Therefore, MyFloridaMarketPlace (MFMP) and People First are not required to be Section 508 compliant. However, the Department agrees wholeheartedly that compliance with Section 508 is appropriate and we concur with the Auditor General's recommendation that "agencies should make appropriate enhancements to their Web sites and applications to comply with Section 508." DMS is currently working to ensure that its Web sites and applications comply with Section 508. We have worked closely with and supported the work of the Governor's Accessible Electronic and Information Technology Task Force, as it addresses this important topic.

Executive Order 05-133 established the Governor's Accessible Electronic and Information Technology Task Force (Task Force) to provide guidance in improving the accessibility of the State's electronic and information technology to persons with disabilities. The Task Force will deliver a report and legislative recommendations to the Governor by January 31, 2006. The Task Force is composed of a broad spectrum of advocates, experts, and government officials in order to ensure representation from all facets. The Task Force has met six (6) times, including its last meeting in Tallahassee January 10, 2006, and has worked very hard to encourage and receive various views regarding this important issue to a measurable percentage of Floridians.

The Executive Order required the Task Force to adopt Section 508 standards for state electronic information technology, including recognized exemptions and exceptions, when reviewing and assessing state Web-based systems. Section 1.E. of Executive Order 05-133 says, *" All agencies under the authority of the Governor are directed, and all other agencies are requested, to use reasonable efforts to comply with Section 508 standards when purchasing, deploying or implementing electronic and information technology."* Task Force Recommendation Number 1 states, *" Consistent with the Governor's directive set forth in the Executive Order, Section E, each agency should document and report by March 15, 2006 on the 'reasonable efforts' taken to comply with Section 508 standards when purchasing, deploying or implementing electronic and information technology. DMS shall provide state agencies reporting guidelines by February 15, 2006."*

Even though MFMP and People First were implemented prior to the establishment of the STO Enterprise Standard and the publication of Executive Order 05-133, the Department has, and is currently in the process of, taking actions towards seeing that both systems become Section 508 compliant. These efforts were discussed with the auditors during the course of their review.

Steps taken by the Department to ensure that both People First and MFMP move towards becoming Section 508 compliant include:

- Requesting $333,000 for the Fiscal Year 2006-07 to be used for the purpose of taking initial steps towards having People First become Section 508 compliant. The People First project office is currently in the process of contracting for a review to determine those areas which are non-compliant and to recommend corrections to the non-compliant areas.

- Using Business Requirements documents to require enhancements and new developments to the People First system be Section 508 compliant. The Business Requirements document contains details of how software enhancements or new features should operate.

- Requiring the People First vendor to upgrade the SAP platform by the completion of calendar year 2006. The upgrade will make it easier to develop Section 508 compliant features for People First.

- Requiring the MFMP vendor to make changes to all system components that are not part of the core Ariba commercial-off-the-shelf program to ensure Section 508 compliance.

- Implementing upgrades to both the Ariba Buyer Application and Ariba Sourcing Application that should allow these applications to become Section 508 compliant. The MFMP project team is projecting that the Ariba Sourcing Application upgrade should be completed by the end of the fiscal year. The Ariba Buyer Application upgrade will be completed when Aspire goes live.

Finding No. 5: Hyperlink Deficiencies

We noted deficiencies in hyperlinks within the agencies' Web sites.

Recommendation:

Each agency should periodically review its strategy to manage the risk of broken and incorrect hyperlinks within its Web site and deploy resources accordingly. Also disclaimer statements should be maintained on Web sites to alert users that certain hyperlinks to outside sources represent content not controlled by the agencies and do not necessarily reflect the agencies' views.

Response:

Concur: The Department will review our strategy to manage the risk of broken and incorrect hyperlinks within our Web sites. As part of that strategy, the Department will periodically take action to check all hyperlinks and correct them as necessary.

The MyFlorida.com Portal Team will review the various approaches used for hyperlink disclaimers. The team will also ask the Portal Advisory Group (PAG) to review and make recommendations on the hyperlink disclaimer issue. The PAG was established in July and has representatives from multiple agencies that are providing direction and recommendations for development of the Portal. Based on the recommendations of the PAG, the Portal Team will then develop an approach for this issue no later than June 1, 2006.

Finding No. 6: Web Domain Management

Current written procedures for managing Web domain names were not maintained by all agencies.

Recommendation:

Agencies should maintain current, written procedures for the acquisition, monitoring, and renewal of their domain names, including, at a minimum procedures to ensure the automatic renewal of domain names and to maintain current contact information.

Response:

Concur: The Division of Enterprise Information Technology Services (previously STO) has established draft internal policies on its domain acquisition, monitoring, renewal, technical responsibility, and automatic renewal of domain names. These draft policies are in review and should become policy within 90 days.

Finding No. 7: Emergency Event and Continuity Procedures for e-Gov Services

Written procedures had not been fully developed by several agencies for maintaining Web site availability during periods of high demand created by emergency events, such as hurricanes. Additionally, not all agencies addressed the recovery of e-Gov services in their IT disaster recovery plans.

Mr. William O. Monroe, CPA
Auditor General
Page 5

Recommendation:

Agencies should establish written procedures to ensure the ability to respond effectively to emergency events via their Web sites. Further, all agencies not maintaining written e-Gov recovery procedures should reevaluate these services for possible inclusion in their IT disaster recovery plans to provide increased assurance of the continuity of essential agency e-Gov functions. E-Gov services selected for recovery should be periodically tested to substantiate the viability of the planned procedures.

Response:

Concur: The Enterprise Information Technology Services Recovery Plan, created and established in conjunction with our vendor SunGard, was finalized and approved October 15, 2005. The Recovery Plan includes the MyFlorida.com Portal and establishes the same fail-over capabilities that are in place today.

Initial testing of the Recovery Plan was to occur in the last quarter of 2005. Due to State emergency situations brought about by the 2005 hurricane season, initial testing has been rescheduled to occur in the second quarter of 2006. This testing will include the recovery of the MyFlorida.com Portal.

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

Sincerely,

Tom Lewis, Jr.
Secretary

cc: John Holley, Chief of Staff
Department of Management Services

Cindi Marsiglio, Deputy Secretary
Department of Management Services

Mr. William O. Monroe, CPA
Auditor General
Page 6

Lee Ann Korst, Deputy Secretary
Department of Management Services

John Ford, Interim Deputy Secretary
Department of Management Services

Ken Granger, Chief Information Officer
Department of Management Services

Lisa Truckenbrod, Director Human Relations Management
Department of Management Services

Fred Springer, Director State Purchasing
Department of Management Services

Steve Godwin, Deputy General Counsel
Department of Management Services

Joe Wright, Chief of Application and Platform Services
Department of Management Services

Steve Rumph, Inspector General
Department of Management Services