REPORT NO. 2011-013
SEPTEMBER 2010

AGENCY FOR WORKFORCE INNOVATION

ONE STOP MANAGEMENT INFORMATION SYSTEM (OSMIS)

Information Technology Operational Audit

For the Period
July 2009 Through April 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DIRECTOR OF AGENCY FOR WORKFORCE INNOVATION

Pursuant to Section 20.50, Florida Statutes, the Agency for Workforce Innovation is created within the Department of Management Services (DMS) and is a separate budget entity, not subject to control, supervision, or direction by DMS in any manner. The Director of the Agency for Workforce Innovation is appointed by the Governor and is the agency head for all purposes. Cynthia Lorenzo served as Director during the audit period.

The audit team leader was Angie Beam, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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

AGENCY FOR WORKFORCE INNOVATION

One Stop Management Information System
(OSMIS)

SUMMARY

The One Stop Management Information System (OSMIS) is operated and maintained by the Office of Information Technology Services within the Agency for Workforce Innovation (Agency). OSMIS is used by the Agency to manage and track grant funding expended through the 24 regional workforce boards providing services around the State.

Our audit focused on evaluating selected information technology (IT) controls applicable to OSMIS for the period July 2009 through April 2010. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2006-086.

The results of our audit are summarized below:

Security Controls

Finding No. 1: Documentation of authorization for some employees' OSMIS access privileges was missing, incomplete, or inaccurate.

Finding No. 2: OSMIS access privileges of one programmer exceeded what was necessary for his job duties. A similar issue regarding access privileges was noted in our report No. 2006-086.

Finding No. 3: The Agency did not have a written procedure for periodic reviews of OSMIS access privileges.

Finding No. 4: Agency management of OSMIS database user accounts needed improvement.

Finding No. 5: The Agency had not designated two OSMIS security officer positions having sensitive IT responsibilities and elevated IT access privileges as positions of special trust and had not performed appropriate background checks and fingerprinting of the two employees. A similar issue regarding positions of special trust was noted in our report No. 2006-086.

Finding No. 6: Certain Agency security controls related to user authentication and application server software maintenance needed improvement.

Finding No. 7: The Agency's OSMIS security plan contained outdated and inaccurate information related to the OSMIS system environment.

Other General Controls

Finding No. 8: The Agency was in the process of developing, but had not yet implemented, written program change control procedures for OSMIS. In addition, as similarly noted in our report No. 2006-086, documentation of key program change controls was lacking for some OSMIS program changes.

Application Controls

Finding No. 9: As similarly noted in our report No. 2006-086, some provisions of OSMIS user documentation were outdated and did not reflect current system functionality.

Additional Matter

Finding No. 10: The Agency had not executed a service-level agreement with the Southwood Shared Resource Center (SSRC).

BACKGROUND

Section 445.004(2), Florida Statutes, designates Workforce Florida, Inc. (WFI), a not-for-profit corporation, as the principal workforce policy organization for the State. WFI contracts with the Agency to provide oversight and policy direction to ensure that the Federal and State grant programs are administered by the Agency in compliance with approved plans. WFI oversees 24 regional workforce boards that implement workforce programs at the local level throughout the State.

Pursuant to Section 445.011(1)(a), Florida Statutes, OSMIS was developed and implemented as the integrated management system to provide one-stop workforce program service delivery. OSMIS is a Web-based application originally composed of three main workforce program modules: Financial Management (FM), Workforce Investment Act, and Wagner-Peyser. As of January 2010, the functionality for the workforce program modules, except for the FM module, had migrated to the Employ Florida Marketplace application, which is Florida's official online portal for job-matching services and other workforce resources. The FM module is used by the Agency and the regional workforce boards for notification of grant award allocations, reporting of cash needs, and reporting of eligible grant expenditures. FM is not scheduled for migration and, according to Agency management, will remain in OSMIS because of the financial resources that would be required to integrate the functionality into the Employ Florida Marketplace application. OSMIS provides a means for the Agency to review and approve cash requests from the regional workforce boards and upload the requests to FLAIR for payment of pass-through funding. Expenditures reported in OSMIS by the regional workforce boards are used in the Agency's Federal grant reporting process.

The security administration function for OSMIS is centrally managed through the Agency headquarters in Tallahassee. OSMIS security officers, including a primary security officer and a backup, are responsible for issuing, monitoring and disabling user accounts based on requests from Agency and regional workforce board staff.

FINDINGS AND RECOMMENDATIONS

Security Controls

Finding No. 1: Documentation of User Access Authorizations

Effective security controls include logical (electronic) access controls that restrict legitimate and appropriate users to the specific IT resources needed and prevent others from accessing the resources. Access controls include, among other things, the use of access authorization forms to document the access privileges that have been authorized by management for system users to be granted.

A security agreement form (authorization form) must be completed and submitted to the Financial Administrator to add, change, or revoke an OSMIS user account. Required information includes user contact information, system access levels, and a security agreement portion which must be read and signed by the user for whom the access is requested, the user's supervisor, and the security officer.

We requested authorization forms for the 50 OSMIS users with active access privileges as of January 11, 2010. For 5 of the 50 users included in our test, authorization forms did not exist upon audit request but Agency management subsequently prepared the forms. Of the 45 authorization forms on file, 5 forms lacked required information. Specifically:

- One form lacked the level of access authorized for the user.
- Two forms lacked the supervisor's signature.
- One form lacked the signatures of both the employee and the supervisor.
- One form lacked both the level of access that was authorized and the supervisor's signature.

Our review of authorization forms for the 50 OSMIS users with active access privileges as of March 8, 2010, disclosed the following:

- Available OSMIS access options were not depicted on 40 of the authorization forms, rendering the forms ineffective in demonstrating the levels of access that had been authorized by management.
- Access levels shown as authorized on the remaining 10 forms did not match the access levels actually granted in OSMIS. However, the access levels granted did not appear excessive for the job duties of OSMIS users listed on the 10 forms.

Without accurate and complete authorization forms to document approved user access privileges, management's ability to monitor the appropriateness of access privileges may be limited.

Recommendation: The Agency should modify its access authorization forms to accurately reflect the available access privileges in OSMIS and ensure that the forms are complete and accurate.

Finding No. 2: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

We examined the access privileges of the 50 active OSMIS users as of March 8, 2010. Our test disclosed that one programmer had complete update access to the application as a user. The access privileges were unnecessary for the performance of the programmer's assigned job responsibilities and increased the risk of unauthorized disclosure, modification, or destruction of OSMIS data. In response to audit inquiry, Agency staff disabled the programmer's application level access privileges. A similar issue regarding access privileges was noted in our report No. 2006-086.

Recommendation: The Agency should limit OSMIS user access privileges to only what is needed for the performance of assigned job duties.

Finding No. 3: Periodic Review of Access

Periodic review of user access privileges helps ensure that user access privileges remain appropriate. Written procedures help provide guidance and direction to employees responsible for performing such reviews by allowing for better communication and consistent application of management-intended controls.

The Agency did not have a written procedure that required OSMIS security officers to perform periodic reviews of access privileges or described management's expectations for how the review was to be performed, including how often the reviews were to be performed and what actions OSMIS security officers should take when discrepancies in access privileges are found. In response to audit inquiry, Agency staff indicated that OSMIS security officers were responsible for ensuring that access to OSMIS was appropriate and that a review of OSMIS user access privileges was performed on February 16, 2010, at the direction of the primary OSMIS security officer. Nevertheless, the lack of a

written procedure for periodic reviews of access privileges increased the risk that reviews would not be conducted in a consistent manner in accordance with management's expectations.

Recommendation: The Agency should develop and implement a written procedure describing management's expectations for periodic reviews of OSMIS access privileges.

Finding No. 4: Database User Account Management

Appropriate controls for management of database user accounts include limiting access to individuals with a valid business purpose; removing, disabling, or otherwise securing unnecessary accounts, including default and guest accounts; and periodically reviewing user accounts for continuing appropriateness.

During our audit of vendor-supplied database user accounts, we noted that the Agency had not changed the default password for one vendor-supplied user account. The database user accounts were used by database administrators to log on to the database to perform database administration functions. In response to audit inquiry, Agency staff changed the default password.

We also noted that there were two active database user accounts that belonged to former database, network, or system administrators who had terminated employment with the Agency. In response to audit inquiry, Agency staff indicated that they had disabled and expired the two corresponding network accounts for the former administrators, effectively restricting database access by anyone outside the network. Nevertheless, an increased risk continued to exist that the accounts could be misused by other authorized network users. The existence of the unneeded database user accounts indicated a need for the Agency to periodically review the appropriateness of the database user accounts.

Recommendation: The Agency should periodically review the appropriateness of active OSMIS database user accounts and disable any unnecessary accounts identified during the review.

Finding No. 5: Positions of Special Trust

Section 110.1127(1), Florida Statutes, provides that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations as a condition of employment and continued employment. The security background investigations are to include, but not be limited to, fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation.

DMS Rule 60DD-2.001(2)(a)75., Florida Administrative Code, defines sensitive locations as physical locations such as a data center, financial institution, network operations center, or any location where critical, confidential, or exempt information resources can be accessed, processed, stored, managed, and maintained. DMS Rule 60DD-2.001(2)(a)80., Florida Administrative Code, defines special trust and position of trust as a position in which an individual can view or alter confidential information or is depended upon for continuity of information resources imperative to the operations of the agency and its mission.

Our audit disclosed that the two OSMIS security officer positions, responsible for establishing and maintaining OSMIS security for Agency staff in Tallahassee and for OSMIS users at the regional workforce boards, had not been designated as positions of special trust. Additionally, background checks (including fingerprinting) had not been performed for the two OSMIS security officers. The sensitive responsibilities and elevated access privileges assigned to OSMIS security officers indicated a need for them to be subject to background checks. Without adequate background checks, including fingerprinting, the risk is increased that a person with an inappropriate background could be assigned OSMIS security officer duties and be provided access to and misuse IT resources. In response to audit inquiry, Agency management arranged for background checks, including fingerprinting, to be performed for the two OSMIS security officers. A similar issue regarding positions of special trust was noted in our report No. 2006-086.

Recommendation: The Agency should continue in its efforts to monitor the job responsibilities and access privileges of its staff to ensure that, where appropriate, positions of special trust are designated and necessary background checks, including fingerprinting, are performed.

Finding No. 6: User Authentication and Application Server Software Maintenance

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Agency security controls related to user authentication and application server software maintenance that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Agency data and IT resources. However, we have notified appropriate Agency management of the specific issues. Without adequate security controls related to user authentication and application server software maintenance, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Agency data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Agency should improve security controls related to user authentication and application server software maintenance to ensure the confidentiality, integrity, and availability of Agency data and IT resources.

Finding No. 7: OSMIS Security Plan

Effective security management includes the development of security plans to provide an overview of the security requirements for a system and a description of the security controls in place or planned for meeting those requirements. Security plans are to be evaluated and adjusted periodically to ensure they are kept up-to-date.

In March 2009, the Agency developed a security plan for OSMIS. The plan outlined various security controls and defined roles and responsibilities. For example, OSMIS security officers were responsible for various user account management functions. In addition, the Information Systems security officer was responsible for various security assessment and planning functions including the system security plan and its updating.

We noted, however, that the plan contained outdated information related to the system environment. Specifications for the platform software and hardware did not reflect the current environment. Additionally, the plan did not accurately reflect the duties performed by the Information Systems security officer. Specifically, the plan stated that the Information Systems security officer would be responsible for ensuring that security controls of the system were monitored on an ongoing basis. The actual duties of the Information Systems security officer were to develop and

periodically evaluate the plan. In the absence of a current and accurate written security plan, the risk is increased that management's IT security objectives will not be effectively communicated or achieved.

Recommendation: The Agency should update its OSMIS security plan to reflect the current system environment and the job duties of the Information Systems security officer.

Other General Controls

Finding No. 8: Program Change Controls

Effective program change controls are intended to ensure that all program changes are properly authorized, tested, and approved for implementation. Although the Agency was in the process of developing written procedures for program changes, the procedures had not yet been implemented as of April 12, 2010. Absent written procedures, there is increased risk that, as indicated by the program change issues described in the following paragraph, appropriate program change controls will not be consistently followed in a manner pursuant to management's expectations.

Our audit disclosed that, of the five program changes made to OSMIS from July 1, 2009, through December 15, 2009, two lacked documentation of program change user acceptance testing and user approval to move program changes into the production environment. Additionally, one of these two program changes lacked program move documentation. Similar issues were disclosed in our report No. 2006-086. Furthermore, Agency staff indicated that changes to the production environment were not logged or reviewed to ensure that unauthorized changes had not been made. Under these conditions, the risk was increased that unauthorized or erroneous programs could be moved into the production environment without timely detection, jeopardizing the ongoing integrity of OSMIS.

Recommendation: To ensure that changes to OSMIS are made in a consistent manner pursuant to management's expectations, the Agency should complete and implement program change procedures that include provisions for authorization of program changes by the system owner, testing and user acceptance of changes, and movement of accepted changes into the production environment by someone independent of the person who developed the changes.

Application Controls

Finding No. 9: OSMIS User Documentation

Adequate system documentation includes user documentation, such as user manuals, that guide employees in the effective and efficient use of a system to timely support business processes. The effectiveness of user documentation can be preserved when the documentation is appropriately updated as system changes are implemented.

Although the Agency had established user documentation to guide the use of OSMIS, our audit disclosed that some provisions of the user documentation were outdated and did not reflect current system functionality. Similar issues regarding user documentation were noted in our report No. 2006-086. Specifically:

- The Regional Financial Management User Manual referenced a Regional Administrator role and the tasks this position performed; however, Agency staff indicated that the Regional Administrator access had never been issued. Additionally, the Manual referenced an error code that had never been activated in OSMIS and an alert that was inactivated in OSMIS on September 9, 2008.

- The Financial Management Administrator User Manual contained references to Florida Accounting Information Resource Subsystem (FLAIR) transactions for general accounting, correcting life-to-date balances, allotments, and disbursement corrections (transactions 10, 11, 20, and 58). These transactions had been inactivated in OSMIS on September 29, 2006. Additionally, this Manual referenced the never-issued Regional Administrator level of access and related tasks discussed in the previous bullet.

The absence of current user documentation may hinder the effective training of new users and the efficient use of the system.

Recommendation: The Agency should update its user documentation to reflect current OSMIS functionality.

Additional Matter

Finding No. 10: Information Technology – Service-Level Agreements

A service-level agreement is a negotiated agreement between two parties where one is the customer and the other is the service provider. Service-level agreements are necessary to define IT services provided by service providers to State agencies and other governmental entities and to ensure that services provided by the service providers support the business objectives of the customer entities. Service-level agreements define the roles and responsibilities of each party, including security management practices, service renewal provisions, and termination requirements. Service-level agreements also set forth the billing methodology and the costs of the services to be paid by the customer entities.

Section 282.203(1)(g), Florida Statutes, provides that each primary data center shall enter into a service-level agreement with each customer entity to provide services as defined and approved by the data center Board of Trustees in compliance with rules of the Agency for Enterprise Information Technology. Section 282.203(1)(g)3., Florida Statutes, states that the failure to execute a service-level agreement within 60 days after service commencement shall, in the case of an existing customer entity, result in a continuation of the terms of the service-level agreement from the prior fiscal year, including any amendments that were formally proposed to the customer entity by the primary data center within the 3 months before service commencement, and a revised cost-of-service estimate. If a new customer entity fails to execute an agreement within 60 days after service commencement, the data center may cease services. Proviso language to Specific Appropriation Item 2206 of Chapter 2010-152, Laws of Florida, provides that by September 1, 2010, the Agency shall execute a service-level agreement, pursuant to Section 282.203(1)(g), Florida Statutes, to specify the services and levels of services it is to receive from the Southwood Shared Resource Center (SSRC).

SSRC houses the two servers on which OSMIS is operated. However, the Agency had not executed a service-level agreement with SSRC for these services and was relying on a prior service-level agreement between the Agency and the Department of Management Services (DMS) to detail the related responsibilities.[1] The absence of a current written service-level agreement with SSRC increases the risk that Agency service requirements, including the security and the availability of the equipment and the data residing therein, will not be sufficiently met.

[1] Effective July 1, 2008, SSRC assumed the responsibility for housing the two OSMIS servers. These services were formerly the responsibility of DMS.

Recommendation: The Agency should establish a written service-level agreement with SSRC that defines the specific requirements related to the housing of the two OSMIS servers.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Agency had taken corrective actions for findings included in our report No. 2006-086.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to OSMIS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine the extent to which the Agency corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2006-086 that were applicable to the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to OSMIS during the period July 2009 through April 2010.

In conducting our audit, we:

- Interviewed Agency personnel.
- Obtained an understanding of OSMIS, including the purpose and goals of the system, and the basic data and business processing flows through the system.
- Obtained an understanding of selected OSMIS application controls, including input, processing, output, and user controls.
- Obtained an understanding of general IT controls related to OSMIS.
- Observed, tested, and evaluated key processes and procedures related to the appropriateness of selected OSMIS application controls, including separation of duties, application edits, and transaction logging within the system.
- Observed, tested, and evaluated key processes and procedures related to the appropriateness of OSMIS user account administration procedures.
- Observed and evaluated key processes and procedures related to the Agency security plan and program, including risk assessments, security policies and procedures, and security awareness training.

- Observed, tested, and evaluated key processes and procedures related to logical access controls over OSMIS IT resources, including adequacy of review and removal of access privileges, adequacy of review of access to OSMIS IT resources, and the adequacy of password controls related to OSMIS.
- Observed, tested, and evaluated key processes and procedures related to the Agency systems modification controls related to OSMIS.
- Determined whether the Agency and SSRC had executed a service-level agreement.

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 IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated September 24, 2010, the Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

Charlie Crist
Governor
Cynthia R. Lorenzo
Director

September 24, 2010

Mr. David W. Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, we have prepared the attached response to the preliminary and tentative findings and recommendations which may be included in your report on the Information Technology Operational Audit of the Agency for Workforce Innovation, One Stop Management Information System (OSMIS), for the period July 2009 through April 2010.

Thank you for providing us the opportunity to respond to your preliminary findings. We hope that this response satisfies your requirements. If you have questions or require additional information, please contact James F. Mathews, Inspector General at (850) 245-7141.

Sincerely,

for Cynthia R. Lorenzo
Director

CRL/js

Enclosure

Agency for Workforce Innovation
The Caldwell Building, Suite 100•107 East Madison Street•Tallahassee, Florida•32399-4120
Telephone (850) 245-7105•Fax (850) 921-3223•TTY/TDD 1-800-955-8771-Voice1-800-955-8770
www.floridajobs.org

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

Florida Agency for Workforce Innovation (AWI)
Response to
Information Technology Operational Audit
One Stop Management Information System
(OSMIS)
September 2010

Finding No. 1: Documentation of User Access Authorizations

Documentation of authorization for some employees' OSMIS access privileges was missing, incomplete, or inaccurate.

Recommendation: The Agency should modify its access authorization forms to accurately reflect the available access privileges in OSMIS and ensure that the forms are complete and accurate.

Agency Response: AWI agrees that the OSMIS access authorization forms should be updated to accurately reflect access privileges granted. To that end, we have revised the access authorization form and have requested updated forms from all Regional Workforce Board users of the system. Updated forms will be distributed to internal AWI users by September 30, 2010, and all forms will be verified as complete and accurate by November 30, 2010.

Finding No. 2: Appropriateness of Access Privileges

OSMIS access privileges of one programmer exceeded what was necessary for his job duties. A similar issue regarding access privileges was noted in our report No. 2006-086.

Recommendation: The Agency should limit OSMIS user access privileges to only what is needed for the performance of assigned job duties.

Agency Response: The individual's access (detected during the audit) was removed on March 30, 2010. A monthly list of access is being provided by Information Technology (IT) Services to the OSMIS security staff for their review, evaluation, and action, if needed.

Finding No. 3: Periodic Review of Access

The Agency did not have a written procedure for periodic reviews of OSMIS access privileges.

Recommendation: The Agency should develop and implement a written procedure describing management's expectations for periodic reviews of OSMIS access privileges.

Agency Response: A procedure is currently being prepared to define expectations for periodic reviews of OSMIS access privileges and will be completed by November 30, 2010.

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

Florida Agency for Workforce Innovation (AWI)
Response to
Information Technology Operational Audit
One Stop Management Information System
(OSMIS)
September 2010

Finding No. 4: Database User Account Management

Agency management of OSMIS database user accounts needed improvement.

Recommendation: The Agency should periodically review the appropriateness of active OSMIS database user accounts and disable any unnecessary accounts identified during the review.

Agency Response: AWI periodically reviews access to its information systems. AWI will include active OSMIS database user accounts with its periodic review and will disable any unnecessary accounts identified during the review. AWI intends to remediate this finding during the next OSMIS access control review scheduled for December 2010.

Finding No. 5: Positions of Special Trust

The Agency had not designated two OSMIS security officer positions having sensitive IT responsibilities and elevated IT access privileges as positions of special trust and had not performed appropriate background checks and fingerprinting of the two employees. A similar issue regarding positions of special trust was noted in our report No. 2006-086.

Recommendation: The Agency should continue in its efforts to monitor the job responsibilities and access privileges of its staff to ensure that, where appropriate, positions of special trust are designated and necessary background checks, including fingerprinting, are performed.

Agency Response: AWI has designated the two OSMIS security officer positions as positions of special trust. The level 2 background screenings have already been run on the personnel in the positions. AWI considers this finding to be resolved.

Finding No. 6: User Authentication and Application Server Software Maintenance

Certain Agency security controls related to user authentication and application server software maintenance needed improvement.

Recommendation: The Agency should improve security controls related to user authentication and application server software maintenance to ensure the confidentiality, integrity, and availability of Agency data and IT resources.

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

Florida Agency for Workforce Innovation (AWI)
Response to
Information Technology Operational Audit
One Stop Management Information System
(OSMIS)
September 2010

Agency Response: AWI is in the process of improving its security controls related to user authentication and application server software maintenance.

Finding No. 7: OSMIS Security Plan

The Agency's OSMIS security plan contained outdated and inaccurate information related to the OSMIS system environment.

Recommendation: The Agency should update its OSMIS security plan to reflect the current system environment and the job duties of Information Systems Security Officer (ISSO).

Agency Response: The OSMIS security plan will be revised to reflect the current system environment by reference to the continually updated *Configuration Management Database, Configuration Item - One Stop Management Information System*. Review and update of the security plan will be complete by November 30, 2010.

Regarding the duties of the ISSO, the intent of the plan was for the ISSO's role to be an oversight/assessment role, functioning to ensure that the security controls of the system (primarily access security) were monitored on an ongoing basis by the OSMIS security officers. Clarification of this expectation will be added to the updated plan.

The procedures addressed in Finding No. 3 will provide for confirmation to the ISSO that security controls of the system are monitored on an ongoing basis.

Finding No. 8: Program Change Controls

The Agency was in the process of developing, but had not yet implemented, written program change control procedures for OSMIS. In addition, as similarly noted in our report No. 2006-086, documentation of key program change controls was lacking for some OSMIS program changes.

Recommendation: To ensure that changes to OSMIS are made in a consistent manner pursuant to management's expectations, the Agency should complete and implement program change procedures that include provisions for authorization of program changes by the system owner, testing and user acceptance of changes, and movement of accepted changes into the production environment by someone independent of the person who developed the changes

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

Florida Agency for Workforce Innovation (AWI)
Response to
Information Technology Operational Audit
One Stop Management Information System
(OSMIS)
September 2010

Recommendation: To ensure that changes to OSMIS are made in a consistent manner pursuant to management's expectations, the Agency should complete and implement program change procedures that include provisions for authorization of program changes by the system owner, testing and user acceptance of changes, and movement of accepted changes into the production environment by someone independent of the person who developed the changes

Agency Response: AWI implemented a new change management software and procedure in September, 2009 as a response to a prior audit. These procedures were documented and formalized for OSMIS on September 10, 2010.

Finding No. 9: OSMIS User Documentation

As similarly noted in our report No. 2006-086, some provisions of OSMIS user documentation were outdated and did not reflect current system functionality.

Recommendation: The Agency should update its user documentation to reflect current OSMIS functionality.

Agency Response: AWI agrees with the finding. The OSMIS user documentation is being updated to reflect current OSMIS functionality. The system is continually being improved, and the user manual must be adjusted accordingly. The updated user documentation will be developed by March 31, 2011.

Finding No. 10: Information Technology – Service-Level Agreements

The Agency had not executed a service-level agreement with the Southwood Shared Resource Center (SSRC).

Recommendation: The Agency should establish a written service-level agreement with Southwood Shared Resource Center that defines the specific requirements related to the housing of the two OSMIS servers.

Agency Response: AWI entered into a Service Level Agreement (SLA) with the SSRC on September 7, 2010.