JANUARY 2006 REPORT NO. 2006-086

AUDITOR GENERAL

WILLIAM O. MONROE, CPA

AGENCY FOR WORKFORCE INNOVATION

ONE STOP MANAGEMENT INFORMATION SYSTEM

Information Technology Audit

SUMMARY

The Agency for Workforce Innovation (Agency) is the designated administrative agency for receipt of Federal workforce development grants and other Federal funds. The Agency is responsible for providing program and fiscal instructions to regional workforce boards pursuant to plans and policies of Workforce Florida, Inc. (WFI). WFI, a not-for-profit corporation, is the principal workforce policy organization for the State. WFI serves as the State's Workforce Investment Board. Pursuant to Florida law[1], WFI provides oversight and policy direction to ensure that the workforce development programs are administered by the Agency in compliance with approved plans and under contract with WFI. To more efficiently administer the workforce development programs, the Agency contracted with Gulf Computers, Inc, which was subsequently purchased by HCL Technologies (Mass), Inc. (HCL), to design and build an automated information system for the operation and management of the workforce development programs.

The One Stop Management Information System (OSMIS) is designed to maximize public access to data, focus on self-service, provide a "single point of entry", and replace Tallahassee-based legacy systems and all existing standalone regional workforce boards systems. The system provides functions for employment service providers, customers, program and agency management, and the Legislature in support of the workforce development program vision. OSMIS supports various Federal programs, including, but not limited to, Workforce Investment Act (WIA) – Youth, WIA – Adult, WIA – Dislocated Worker, Wagner-Peyser, Veterans (VETS), Welfare to Work, and Food Stamp Employment Training.

Our audit focused on evaluating selected general and application information technology (IT) controls related to OSMIS, and selected user controls during the period July 1, 2004, through June 30, 2005, with selected actions taken through December 16, 2005. Our audit was limited to the controls at the Agency and did not extend to WFI or the regional workforce boards.

The results of our audit are summarized as follows:

<u>Finding No. 1:</u> Access capabilities to the various modules within OSMIS had been granted to users who did not need the access for their job function.

<u>Finding No. 2:</u> The Maintain User screen for security administration for the Financial Management module of OSMIS granted all access rights upon user set-up unless rights were specifically denied when the user account was established.

<u>Finding No. 3:</u> There was a lack of coordination between the Agency and the regional workforce boards for security administration.

<u>Finding No. 4:</u> Access capabilities to the OSMIS application had not been timely deleted for users who had terminated employment and no longer needed access.

<u>Finding No. 5:</u> There was not a policy at the Agency to identify positions of special trust and there were no procedures for reviewing the work of employees who occupy critical or sensitive positions.

[1] Section 445.004(5)(b), Florida Statutes

Finding No. 6: Improvements were needed in certain security controls protecting OSMIS.

Finding No. 7: Cash disbursement functionality within the Financial Management module of OSMIS included transactions not needed for cash disbursement processing.

Finding No. 8: Written procedures for the reconciliation of OSMIS data to FLAIR had not been developed.

Finding No. 9: There were inadequate controls over certain aspects of the change management process.

Finding No. 10: OSMIS user documentation did not always accurately reflect system functionality.

Finding No. 11: The Agency had not developed policies and procedures for exception reporting and error handling for OSMIS interface transactions.

BACKGROUND

The Workforce Investment Act of 1998[2] was implemented to consolidate, coordinate, and improve employment, training, literacy, and vocational rehabilitation programs in the United States. This Act provided for workforce investment activities, through statewide and local workforce investment systems, to increase the employment, retention, and earnings of participants, and increase occupational skill attainment by participants, and, as a result, improve the quality of the workforce, reduce welfare dependency, and enhance productivity and competitiveness.

As the State's Workforce Investment Board, WFI has been granted the powers and authority to carry out the Workforce Investment Act of 1998. WFI's purpose is to design and implement strategies that help Floridians enter, remain in, and advance in the workplace, in order to benefit these individuals, businesses, and the entire State.

The Agency is the designated administrative agency for the receipt of Federal workforce development grants and other Federal funds pursuant to the Workforce Investment Act of 1998. The Agency provides direction to regional workforce boards regarding the following programs, in part, pursuant to the direction of and under contract with WFI:

- Certain programs authorized under Title I of the Workforce Investment Act of 1998;
- Programs authorized under the Wagner-Peyser Act of 1933, as amended[3];
- Welfare transition services funded by the Temporary Assistance for Needy Families Program; and
- The Food Stamp Employment and Training Program.

One regional workforce board has been appointed in each of the 24 designated delivery areas and serves as the local workforce investment board. Each regional workforce board has the responsibility of overseeing the one-stop delivery system in its local area. The one-stop delivery system is the State's primary customer-service strategy for offering every Floridian access, through service sites or telephone or computer networks, to the following services, in part:

- Job search, referral, and placement assistance.
- Career counseling and educational planning.
- Recruitment and eligibility determination.
- Employability skills training.
- Adult education and basic writing skills training.
- Other appropriate and available workforce development services.

Regional workforce boards are responsible for designating one-stop delivery system operators.

Florida law[4] instructed WFI to implement automated information systems that are necessary for the efficient and effective operation and management of the workforce development system. The law provides that these information systems include an integrated management system for the one-stop service delivery system, including, at a minimum, common registration and intake, screening for needs and benefits, case planning and tracking, training benefits management, service and training provider management,

[2] Public Law 105-220 105th Congress

[3] Title 29, Section 49 et seq, United States Code

[4] Section 445.011(1)(a), Florida Statutes

performance reporting, executive information and reporting, and customer satisfaction tracking and reporting.

The automated information system under development for the operation and management of the workforce development programs was OSMIS. As of the completion of our field work, additional modules were still under development by HCL, with a targeted completion in February 2007. The Agency Project Management Office was managing this project.

Finding No. 1: System Access Capabilities

Effective security controls provide that access to and use of IT resources be generally restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules that provide access security control based on the individual's demonstrated need to view, add, change, or delete data.

We noted the following instances of excessive or inappropriate access privileges within OSMIS:

- One employee with programming responsibilities within the Agency's OSMIS Project Management Office had been granted update access as a Financial Administrator user type within the Financial Management module of OSMIS. This user could, therefore, not only make programming changes to the application, but with the Financial Administrator access, could update Grant Awards, update Notices of Funds Available to the regions, approve regions' Cash Requests, and override cash requests in excess of the established Maximum Amount Drawable. The level of access granted exceeded the level requested and approved according to the Security Agreement Form and created a potentially insufficient segregation of duties. This level of access was not required by the job function and, in response to our inquiries, the security administrator subsequently removed the Financial Administrator user type from this employee.
- Three employees within WFI and one employee within the Agency had been granted update access as the AWI user type within the Financial Management module of OSMIS. The AWI user type, as with the Financial Administrator user type, allowed update of Grant Awards, Notices of Funds Available to the regions, approval for regions' Cash Requests, and override capabilities for cash requests in excess of the established Maximum Amount Drawable. The level of access granted exceeded the level requested and approved according to the Security Agreement Form. This level of access was not required by the job function and, in response to our inquiries, was subsequently removed by the security administrator.
- Three contracted monitoring staff, four Agency users, and one WFI user, had been granted access as an AWI user type within the Financial Management module with greater than read only capability to one to two functions. This level of access granted exceeded the level requested and approved according to the Security Agreement Form, was not necessary for the performance of their job functions, and had been granted inadvertently due to the security administration configuration within the Financial Management module of OSMIS as described further in Finding No. 2. In response to our inquiries, the security administrator modified the access level to read only.
- Certain members of the Project Management Office had excessive access capabilities in OSMIS. Specific details of the access capabilities in question are not disclosed in this report to avoid the possibility of compromising Agency information, but have been provided to the appropriate Agency staff.

Excessive access capabilities increase the risk that inappropriate transactions could be initiated within the application.

The Agency should periodically review the appropriateness of all OSMIS users' access capabilities and, where appropriate, make modifications to restrict access consistent with the users' functional responsibilities.

Finding No. 2:
Security Administration Software Configuration

Effective security controls provide for access capabilities to be based upon an individual's demonstrated need to view, add, change, or delete data. In particular, good security management practices provide for logical access to be granted based upon the principle of least privilege, or need-to-know.

During our audit, we noted that the security administration function for the Financial Management module involved assigning function level access based on the user's need to read, update, or delete specific activity. However, the mechanism for establishing initial access defaulted to full access (denoted by checkmarks within the access screens) for each of the functions. This required the security administrator to manually remove the unneeded access by "clicking" on the checkmark to remove it.

As demonstrated by the inappropriate access capabilities noted in Finding No. 1, third bullet, the configuration of the security administration features in the Financial Management module creates a significant risk that security administrators will overlook the default unrestricted access initially generated by the system and fail to reduce the access to a level appropriate for the user's job requirements.

Recommendation: The Agency should seek software configuration modifications that would eliminate granting full access by default and provide a mechanism for granting only the specific access capabilities that are required to perform the job function assigned. Until the software can be appropriately re-configured, the Agency should, for the Financial Management module, provide for an independent review of access privileges immediately after they have been set up for the users.

Finding No. 3:
State/Region Security Coordination

Effective security controls include procedures to ensure timely action relating to requesting, issuing, suspending, and closing user accounts. This also includes ensuring that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a coordinated manner to obtain consistency and efficiency of access control.

During our audit, we noted that the Agency had various security policies that addressed many areas of the data security environment. It also had both an AWI Information Security Manual and a Regional Security Officer User Manual. However, the coordination of security administration between the Agency security group and the regional security officers was not addressed in any of these documents. Application security management is distributed among the Customer Support Center in Tallahassee and the regional security officers within the twenty-four regions. The Customer Support Center is responsible for establishing and maintaining security for Agency staff in Tallahassee and for the security officers located in the regions. The regional security officers are responsible for establishing and maintaining security for their respective regions. Additionally, the Agency does not have authority over the regional workforce boards. As such, the Agency and the regions did not coordinate security administration. For example, the regions did not provide documentation of user terminations so that the Agency could monitor the promptness of the removal of user access.

Inadequate coordination between the Agency and the security officers for security administration increases the risk of unauthorized disclosure, modification, or loss of data and IT resources. The lack of coordination between the Agency and the regional security officers may have been a contributing factor to access capabilities not being timely deleted for users who had terminated employment, as noted in Finding No. 4.

Recommendation: The Agency should implement formal written policies and procedures that address the security administration coordination between the Agency and the regional security officers. If necessary to promote coordination, the Agency should request WFI to implement security administration policies for the regions regarding access control over OSMIS.

Finding No. 4: Terminated Employee Access

Effective security controls include procedures to ensure that access is granted only to personnel authorized by management. When an authorized user terminates employment, their access should be revoked immediately to ensure that privileges are not exploited by the terminated user or others.

Upon our audit request, the Agency provided us a list of terminated Agency employees for the period July 1, 2004, through June 30, 2005. Our review disclosed that, of 314 employees who had terminated employment, 8 continued to have OSMIS application user log-in IDs as of June 30, 2005, even though they had been terminated for periods ranging from 6 to 179 days. Of these 8 application user log-in IDs, 1 appeared to have been used after the date of termination.

In response to our inquiries, the Agency noted that the system provides for an automatic inactivation of the user log-in ID after a pre-defined period of time. We determined that, pursuant to the OSMIS Application System User Guide, automatic inactivation is set to occur after 60 days of continuous nonuse. However, access privileges need immediate removal to sufficiently reduce the risk of misuse.

Lack of coordination for security administration between the regions and the Agency may have contributed to the inconsistency in the removal of access capabilities for terminated employees. Without timely deletion of access of employees who terminate employment with the Agency, the risk is increased that a terminated employee's access privileges could be used to view or modify data.

Recommendation: The Agency should implement stronger controls over the termination of access privileges in order to minimize the risk of compromising the Agency's data and information.

Finding No. 5: Positions of Special Trust

Florida law[5] provides that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive locations of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. During our audit, we noted that there was not a policy at the Agency to identify positions of special trust and there were no procedures for reviewing the work of employees who occupy critical or sensitive positions. The Agency had not designated key IT employees, such as, but not limited to, security administrators, systems programmers, and database administrators, as occupying positions of special trust, or implemented adequate monitoring and review procedures over the actions of the individuals in those positions.

According to the Agency, the UNIX administrator and the database administrator, in addition to their customary duties, were responsible for moving OSMIS programs into the production environment. Additionally, according to the Agency, HCL staff had the access capabilities, per contract, to move OSMIS programs into the production environment. The Agency stated that, under contract, HCL was entirely responsible for the OSMIS application, including production, and that there were HCL staff that had this level of access, but that they were only permitted (by contract) to use it in emergency situations. These high-level access capabilities create an increased risk of unauthorized or erroneous program changes. Furthermore, there was no indication in the contract with HCL that contracted staff would be subject to background checks and fingerprinting.

[5] Section 110.1127, Florida Statutes

By not designating individuals with high access levels as positions of special trust, performing adequate background checks, including fingerprinting, and documenting detailed monitoring procedures for employees or contractors in those positions, the risk is increased that data or information will be inappropriately modified or destroyed and such actions not be detected in a timely manner.

Recommendation: The Agency should implement an appropriate policy to designate positions that, due to their special responsibility or sensitive location, require background checks and fingerprinting. The Agency should also document detailed monitoring and review procedures over the actions of the individuals in those positions. Furthermore, the Agency should, as soon as practicable, require background checks for contractors who are given high access levels and perform critical or sensitive duties.

Finding No. 6:
Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data resources. During our audit, we identified the following deficiencies in certain security control features implemented by the Agency:

- Improvements were needed in controls protecting the confidentiality of OSMIS user passwords.
- The AWI Financial Administrator User Manual did not accurately describe password change requirements.

Specific details of the security control deficiencies are not disclosed in this report to avoid the possibility of compromising Agency information. However, the appropriate Agency management staff have been notified of the deficiencies.

Recommendation: The Agency should take the appropriate actions to correct the control deficiencies stated above.

Finding No. 7:
Excessive System Functionality

Effective controls include limiting system functionality to prevent access to transactions that are not used for the business process that the system supports.

During our audit, we noted that weekly cash disbursements were processed utilizing a Cash Approval transaction within OSMIS (transaction 51) that is generated and transferred to FLAIR for processing. In addition to transaction 51 functionality within the Financial Management module of OSMIS, we noted that additional transaction options were available. These included General Accounting, Correcting Life to Date Expenditures, Allocation, and Cash Adjustments transactions (transactions 10, 11, 20, and 58). These additional transaction options were not currently used in the Financial Management module cash disbursement process.

While there is a manual review of the vouchers that occurs before processing, the availability of functionality for transactions that should not be used in the disbursement process increases the risk that additional transactions may be unintentionally processed.

Recommendation: The Agency should remove the access capability to the unnecessary transactions from the users' security profiles.

Finding No. 8:
Reconciliation Procedures

Effective user controls include procedures to assure that output is routinely balanced to relevant control totals, procedures to facilitate tracing of transaction processing, and reconciliation procedures. During our audit, we noted that while reconciliations between OSMIS and the Florida Accounting Information Resource Subsystem (FLAIR) were performed on a monthly basis for all active grants, written procedures to govern the reconciliation process had not been developed.

Without written reconciliation procedures, the risk is increased that the reconciliation process may not be accurately or consistently performed, and that inaccurate, inconsistent, or incomplete OSMIS and FLAIR data, should it exist, will not be timely detected. Subsequent to our field work, the Agency indicated that it had developed written procedures for the monthly reconciliation between OSMIS and FLAIR.

Recommendation: In the future, the Agency should ensure that key processes, such as reconciliations, have adequate written procedures to ensure the accuracy, consistency, agreement, and completeness of the OSMIS and other information systems' data.

Finding No. 9: Change Management Process

Establishing controls over the modification of application software helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Additionally, a proper segregation of duties includes providing a separation between who performs program changes, user acceptance testing, and the movement of programs into the production environment.

During our audit, we requested evidence of controls in place during the various stages of the change management process. We noted the following deficiencies:

- ➢ We selected 20 modifications from the release notes (documentation of changes applied in the release) produced by HCL and tested for user request/initiation, development of specifications, testing prior to movement into the production environment, independent monitoring of program moves, proper segregation of duties, and user acceptance testing by reviewing information contained in the Track-It system. We noted the following:
  - Six of the 20 items tested were made prior to the implementation of the Track-It system, and there was no other documentation that provided specific identification of the individuals involved in each step of the change control process. Therefore, it was not possible to identify who performed the individual steps within the change control process and, as a result, we were unable to determine, for these 6 items, whether an appropriate segregation of duties existed between the modification of programs, the testing of program changes, and the movement of programs into the production environment.
  - There was no documentation of user acceptance testing for 14 of the 17 items that required user acceptance testing.
- ➢ We tested the change management controls for the procedure that generates the Workforce Investment Act Standardized Record Data (WIASRD) file that is used to produce the WIA Annual Report and the WIA Quarterly Report that are submitted to the U.S. Department of Labor (USDOL). The procedure was rewritten in order for the generated WIASRD file to be in the correct format that is required by the Mathematica software, WIA Data Validation Application, which is the USDOL-approved software that creates the WIA Annual Report and the WIA Quarterly Report. Although there was documentation to evidence programmer testing and acceptance of the change, quality control testing and acceptance of the change, and user testing of the change, there was no documentation to evidence WFI or Agency user acceptance of the program change.

The aforementioned deficiencies in the change control process increased the risk that unauthorized or erroneous programs could be moved into the production environment without timely detection, which could jeopardize the ability of the Agency to meet its objectives.

Recommendation: The Agency should take the necessary steps to ensure that all change control process procedures are being followed for OSMIS.

Finding No. 10: OSMIS User Documentation

An effective information system development methodology provides, among other things, that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation, or modification project. State Technology Office (STO) rules[6] provide, in part, that a user manual be prepared which contains all essential information for the user to make full use of the information system.

During our audit, we noted several instances where the OSMIS One Stop Staff User Manual did not accurately reflect functionality within OSMIS as follows:

- The user manual stated that the "salary" field was mandatory, when, in fact, this field was only mandatory when the basis of payment field had been entered.
- The user manual stated that the "preferred referral method" field was optional, when, in fact, this field was a drop down menu with two choices and was mandatory.
- The user manual stated that the "comment" field was optional, when, in fact, this field was mandatory when the "result" field stated "placed."
- The user manual stated that the "number of job openings for this job order" field was a mandatory field with a numeric field of three characters maximum, when, in fact, this field could have a maximum of four characters.
- The user manual stated that the "number of hours per week" field was mandatory with a numeric field of three characters maximum, when, in fact, this field was restricted to no more than 154 hours.
- The user manual stated that the "reason for leaving" field was mandatory if the job seeker selected a valid end date other than "present." However, the system did not have this field denoted with an asterisk indicating a mandatory field, when, in fact, it was mandatory.

Inaccurate user documentation increases the risk that users may not efficiently and effectively enter information into OSMIS.

Recommendation: The Agency should make the necessary corrections to the user documentation to accurately reflect OSMIS functionality and to promote user efficiency.

Finding No. 11: Exception Reporting and Error Handling

Effective input controls over data transfer include data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruptions of the processing of other valid transactions. Effective error handling procedures include a review of exception reports and correction of all errors.

During our audit, we noted that the Agency had not developed written policies or procedures for exception reporting and error handling for OSMIS interface transactions. We identified six Wagner-Peyser inbound interfaces, of which five produced an interface import log file of transactions accepted and rejected. All interface logs were reviewed by technical staff to ensure that the data was loaded. However, business staff, who own the OSMIS data, reviewed only the Priority Re-employment Program (PREP) interface log. The remaining four logs were not reviewed by the business staff. Since no review was required of the business staff, the exceptions and errors were not followed-up on.

By not providing appropriate policies and procedures for exception reporting, the risk is increased that rejected, excluded, or inaccurate data may not be identified and resolved in a timely manner.

[6] 60DD-7.008, Florida Administrative Code

Recommendation: The Agency should implement formal policies and procedures for exception reporting and error handling for OSMIS interfaces to ensure the accuracy and completeness of OSMIS data.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to OSMIS, and selected user controls. Our audit scope focused on evaluating selected IT and user controls applicable to OSMIS during the period July 1, 2004, through June 30, 2005, with selected actions taken through December 16, 2005. Our audit was limited to the controls at the Agency and did not extend to WFI or the regional workforce boards.

In conducting the audit, we interviewed appropriate Agency personnel, reviewed policies and procedures and other applicable documentation, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to OSMIS.

AUTHORITY

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

William O. Monroe

William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

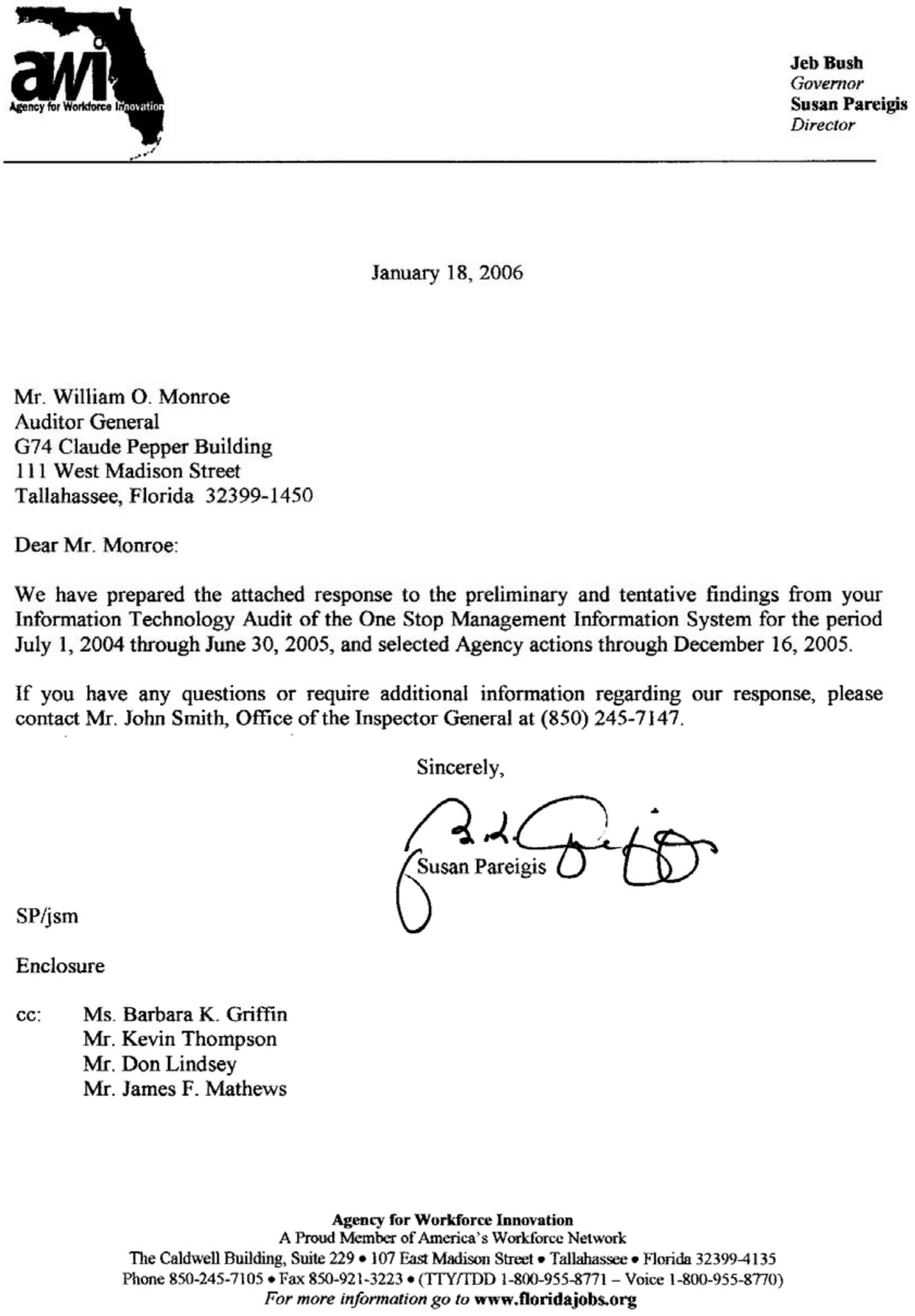
In a letter dated January 18, 2006, the Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

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

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

*Regulated by State of Florida.

APPENDIX A
MANAGEMENT RESPONSE



awi
Agency for Workforce Innovation

Jeb Bush
Governor
Susan Pareigis
Director

January 18, 2006

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

Dear Mr. Monroe:

We have prepared the attached response to the preliminary and tentative findings from your Information Technology Audit of the One Stop Management Information System for the period July 1, 2004 through June 30, 2005, and selected Agency actions through December 16, 2005.

If you have any questions or require additional information regarding our response, please contact Mr. John Smith, Office of the Inspector General at (850) 245-7147.

Sincerely,

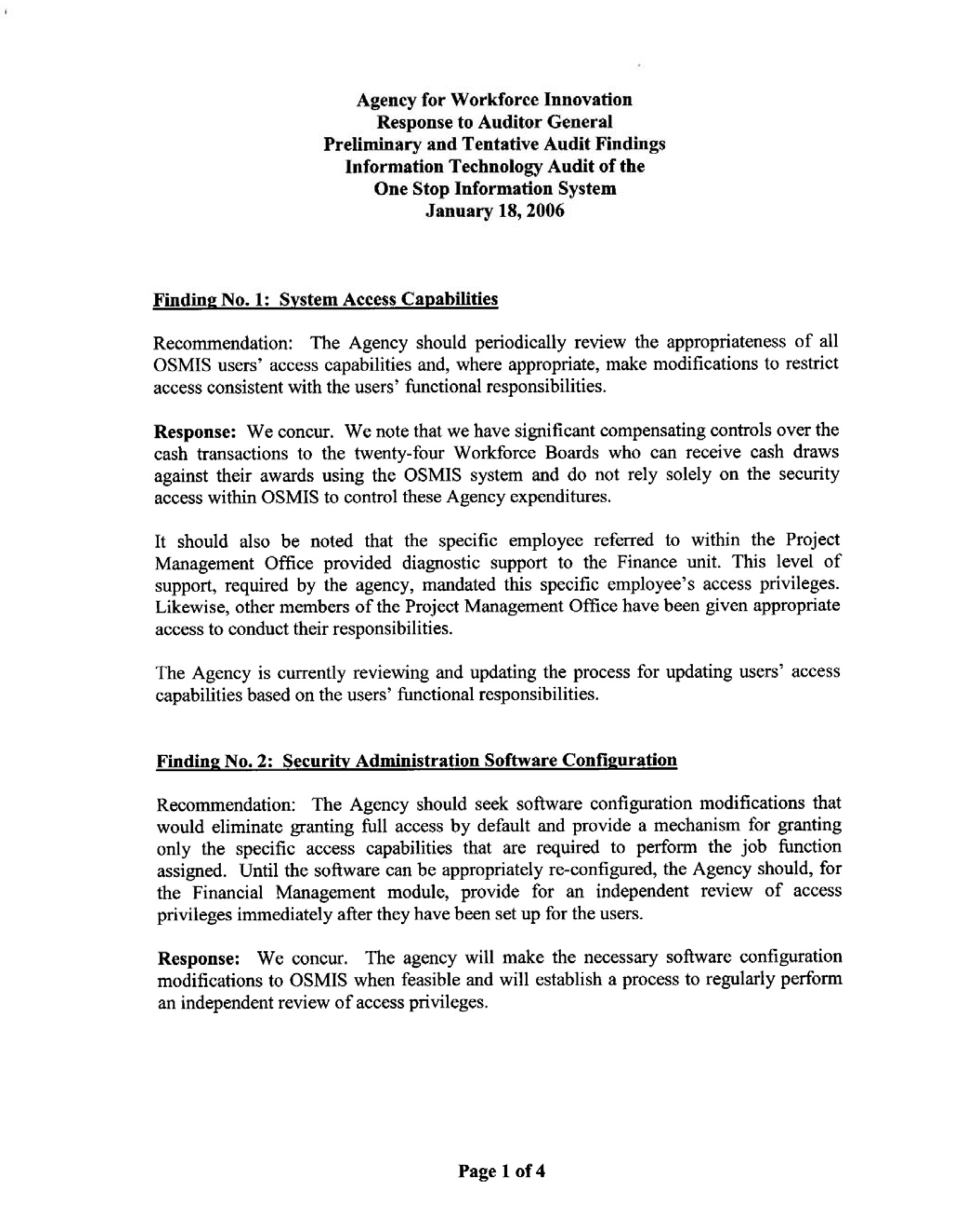
Susan Pareigis

SP/jsm

Enclosure

cc: Ms. Barbara K. Griffin
Mr. Kevin Thompson
Mr. Don Lindsey
Mr. James F. Mathews

Agency for Workforce Innovation
A Proud Member of America's Workforce Network
The Caldwell Building, Suite 229 • 107 East Madison Street • Tallahassee • Florida 32399-4135
Phone 850-245-7105 • Fax 850-921-3223 • (TTY/TDD 1-800-955-8771 – Voice 1-800-955-8770)
For more information go to **www.floridajobs.org**



Agency for Workforce Innovation
Response to Auditor General
Preliminary and Tentative Audit Findings
Information Technology Audit of the
One Stop Information System
January 18, 2006

Finding No. 1: System Access Capabilities

Recommendation: The Agency should periodically review the appropriateness of all OSMIS users' access capabilities and, where appropriate, make modifications to restrict access consistent with the users' functional responsibilities.

Response: We concur. We note that we have significant compensating controls over the cash transactions to the twenty-four Workforce Boards who can receive cash draws against their awards using the OSMIS system and do not rely solely on the security access within OSMIS to control these Agency expenditures.

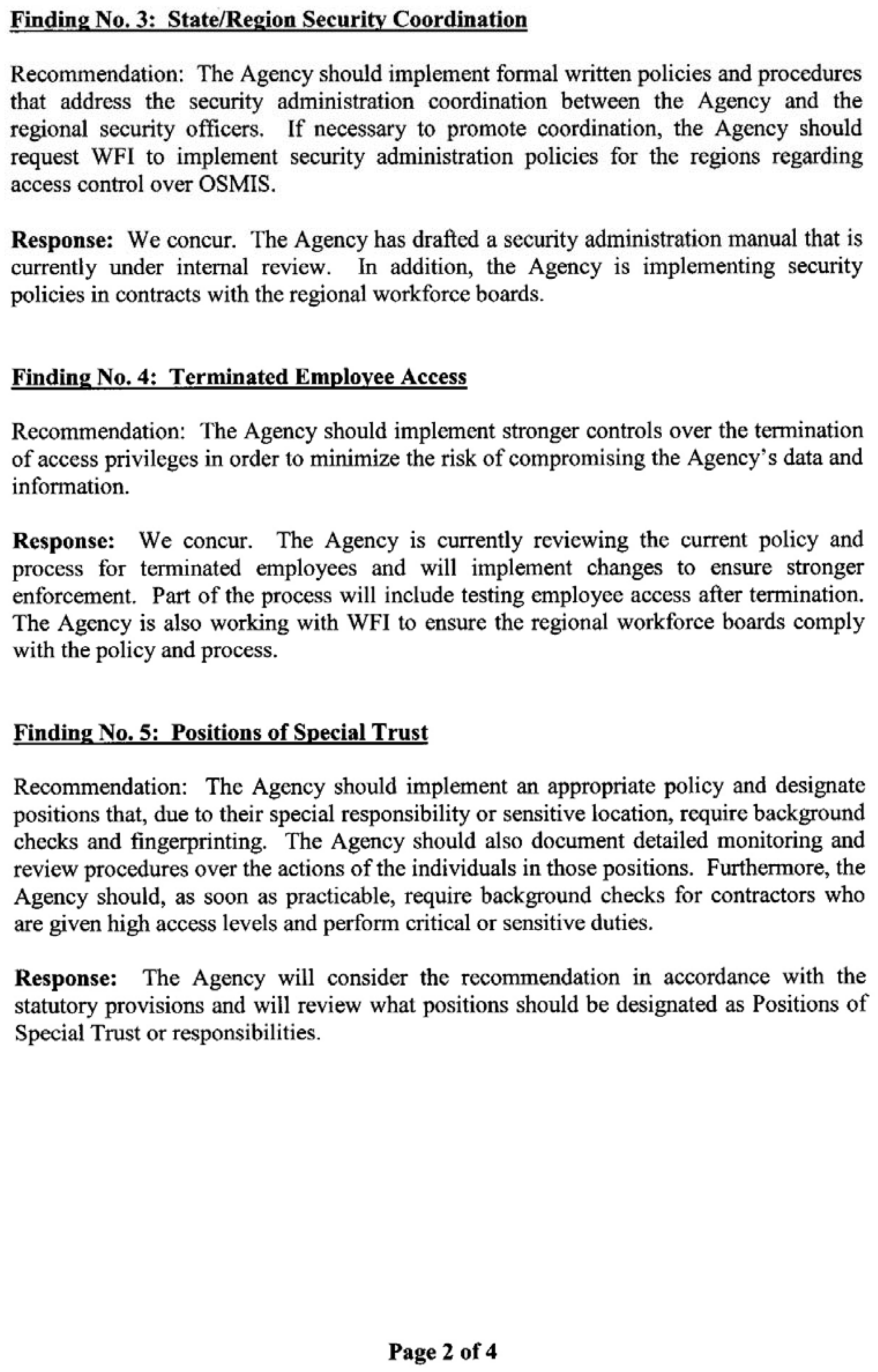
It should also be noted that the specific employee referred to within the Project Management Office provided diagnostic support to the Finance unit. This level of support, required by the agency, mandated this specific employee's access privileges. Likewise, other members of the Project Management Office have been given appropriate access to conduct their responsibilities.

The Agency is currently reviewing and updating the process for updating users' access capabilities based on the users' functional responsibilities.

Finding No. 2: Security Administration Software Configuration

Recommendation: The Agency should seek software configuration modifications that would eliminate granting full access by default and provide a mechanism for granting only the specific access capabilities that are required to perform the job function assigned. Until the software can be appropriately re-configured, the Agency should, for the Financial Management module, provide for an independent review of access privileges immediately after they have been set up for the users.

Response: We concur. The agency will make the necessary software configuration modifications to OSMIS when feasible and will establish a process to regularly perform an independent review of access privileges.



Finding No. 3: State/Region Security Coordination

Recommendation: The Agency should implement formal written policies and procedures that address the security administration coordination between the Agency and the regional security officers. If necessary to promote coordination, the Agency should request WFI to implement security administration policies for the regions regarding access control over OSMIS.

Response: We concur. The Agency has drafted a security administration manual that is currently under internal review. In addition, the Agency is implementing security policies in contracts with the regional workforce boards.

Finding No. 4: Terminated Employee Access

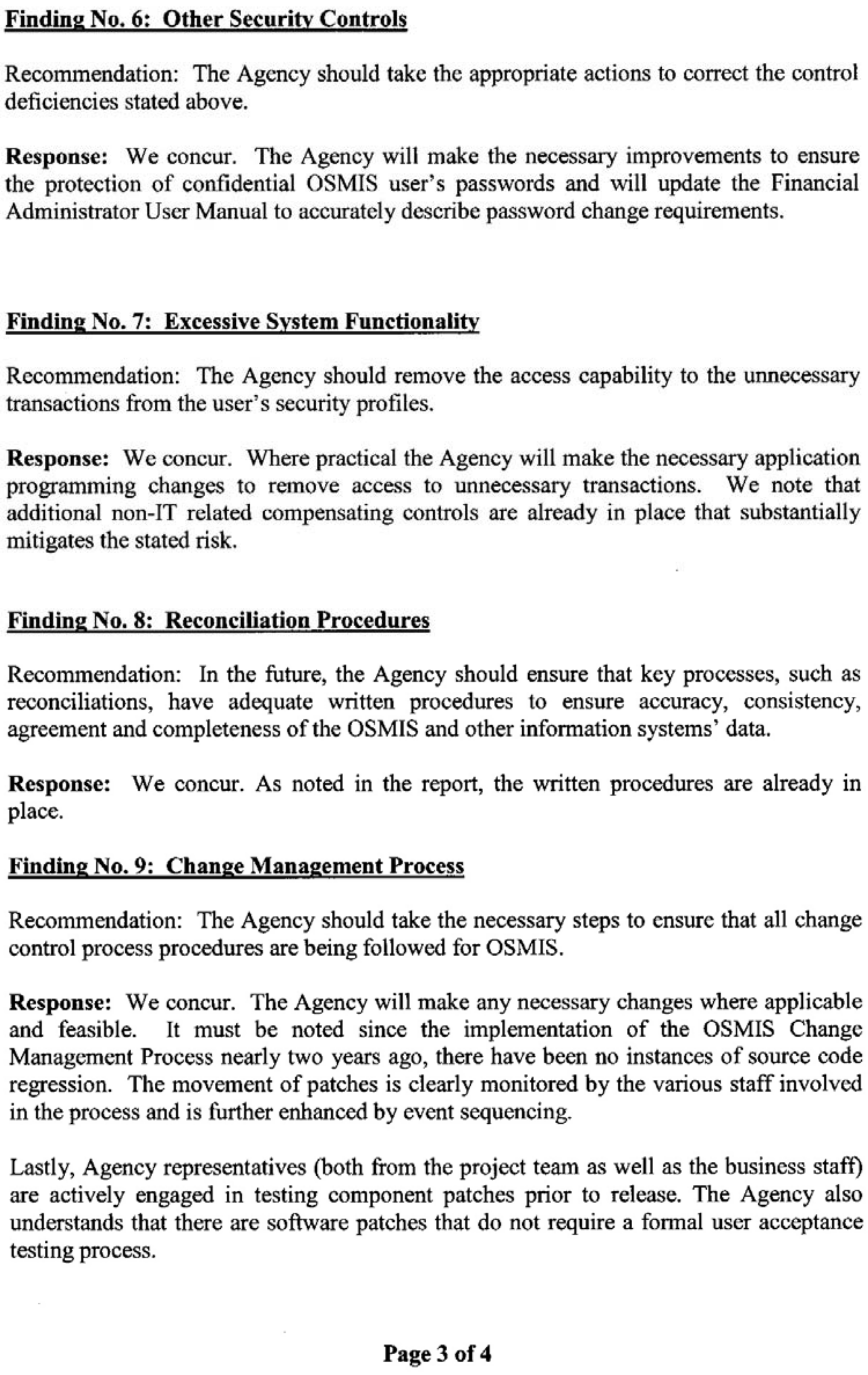
Recommendation: The Agency should implement stronger controls over the termination of access privileges in order to minimize the risk of compromising the Agency's data and information.

Response: We concur. The Agency is currently reviewing the current policy and process for terminated employees and will implement changes to ensure stronger enforcement. Part of the process will include testing employee access after termination. The Agency is also working with WFI to ensure the regional workforce boards comply with the policy and process.

Finding No. 5: Positions of Special Trust

Recommendation: The Agency should implement an appropriate policy and designate positions that, due to their special responsibility or sensitive location, require background checks and fingerprinting. The Agency should also document detailed monitoring and review procedures over the actions of the individuals in those positions. Furthermore, the Agency should, as soon as practicable, require background checks for contractors who are given high access levels and perform critical or sensitive duties.

Response: The Agency will consider the recommendation in accordance with the statutory provisions and will review what positions should be designated as Positions of Special Trust or responsibilities.



Finding No. 6: Other Security Controls

Recommendation: The Agency should take the appropriate actions to correct the control deficiencies stated above.

Response: We concur. The Agency will make the necessary improvements to ensure the protection of confidential OSMIS user's passwords and will update the Financial Administrator User Manual to accurately describe password change requirements.

Finding No. 7: Excessive System Functionality

Recommendation: The Agency should remove the access capability to the unnecessary transactions from the user's security profiles.

Response: We concur. Where practical the Agency will make the necessary application programming changes to remove access to unnecessary transactions. We note that additional non-IT related compensating controls are already in place that substantially mitigates the stated risk.

Finding No. 8: Reconciliation Procedures

Recommendation: In the future, the Agency should ensure that key processes, such as reconciliations, have adequate written procedures to ensure accuracy, consistency, agreement and completeness of the OSMIS and other information systems' data.

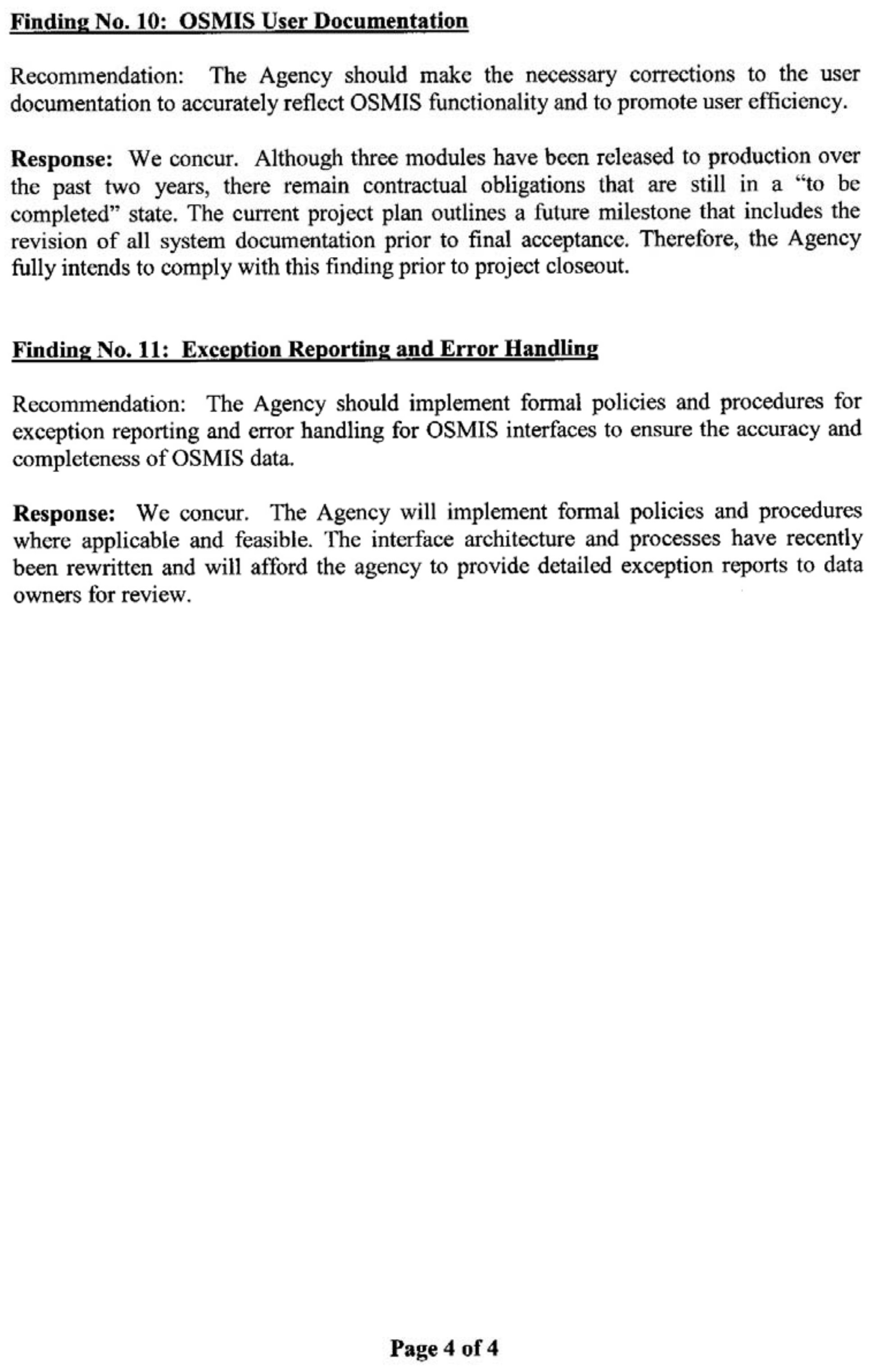
Response: We concur. As noted in the report, the written procedures are already in place.

Finding No. 9: Change Management Process

Recommendation: The Agency should take the necessary steps to ensure that all change control process procedures are being followed for OSMIS.

Response: We concur. The Agency will make any necessary changes where applicable and feasible. It must be noted since the implementation of the OSMIS Change Management Process nearly two years ago, there have been no instances of source code regression. The movement of patches is clearly monitored by the various staff involved in the process and is further enhanced by event sequencing.

Lastly, Agency representatives (both from the project team as well as the business staff) are actively engaged in testing component patches prior to release. The Agency also understands that there are software patches that do not require a formal user acceptance testing process.



Finding No. 10: OSMIS User Documentation

Recommendation: The Agency should make the necessary corrections to the user documentation to accurately reflect OSMIS functionality and to promote user efficiency.

Response: We concur. Although three modules have been released to production over the past two years, there remain contractual obligations that are still in a "to be completed" state. The current project plan outlines a future milestone that includes the revision of all system documentation prior to final acceptance. Therefore, the Agency fully intends to comply with this finding prior to project closeout.

Finding No. 11: Exception Reporting and Error Handling

Recommendation: The Agency should implement formal policies and procedures for exception reporting and error handling for OSMIS interfaces to ensure the accuracy and completeness of OSMIS data.

Response: We concur. The Agency will implement formal policies and procedures where applicable and feasible. The interface architecture and processes have recently been rewritten and will afford the agency to provide detailed exception reports to data owners for review.

THIS PAGE LEFT BLANK INTENTIONALLY