Office of Inspector General
Lynne T. Winston, Esq., CIG, Inspector General
2601 Blair Stone Road
Tallahassee, Florida 32399-1018
Phone: 850.414-6700 • Fax: 850.921.2683

Ken Lawson, Secretary

Rick Scott, Governor

MEMORANDUM

TO: Ken Lawson, Secretary

FROM: Lynne T. Winston, Inspector General

DATE: December 21, 2016

SUBJECT: Six-Month Follow-Up Response to Auditor General Report Number 2016-198, *Department of Business and Professional Regulation - Information Technology Operational Audit – Versa: Regulation* (Project Number G-1617BPR-005)

Section 20.055, Florida Statutes, requires that I monitor and report to you on the status of implementation of findings and recommendations made in audits issued by the Auditor General. Accordingly, the attached report is our six-month follow-up response to Auditor General Report Number 2016-198, *Department of Business and Professional Regulation – Information Technology Operation Audit – Versa: Regulation* (published June 21, 2016).

Our review found that management has taken substantive action to address the issues noted in the audit report. We concluded that management has taken sufficient corrective action to three of the five findings and, as described in the attached report, management is actively working to address the remaining issues. We will continue to monitor and report to you on progress in these areas.

We would like to thank the management of the Division of Technology for their assistance.

Please contact me if you have any questions.

LTW:sbh

Attachment

cc: Melinda Miguel, Chief Inspector General
Kathy DuBose, Coordinator, Legislative Auditing Committee
Matilde Miller, Chief of Staff
Joseph Martin, Chief Information Officer

DEPARTMENT OF BUSINESS & PROFESSIONAL REGULATION
Office of Inspector General

Ken Lawson
Secretary

Lynne T. Winston
Inspector General

Six-Month Follow-up Response to *Information Technology Operational Audit: Versa Regulation* Auditor General Report Number 2016-198

OVERVIEW

Section 20.055, Florida Statutes, requires the Inspector General to monitor and report to the Secretary on the status of corrective action taken in response to reports issued by the Auditor General. In June 2016, the Auditor General published Report Number 2016-198, *Information Technology Operational Audit: Versa Regulation*. The audit evaluated selected information technology controls applicable to Versa: Regulation.

The purpose of this report is to inform the Secretary of the status of management's response to the audit findings and recommendations.

STATUS REPORT

Finding 1: Change Management Controls

Change management controls related to Versa: Regulation program changes need improvement to ensure that only authorized, tested, and approved program changes are implemented into the production environment.

Recommendation

We recommend that department management establish controls to ensure that only authorized, tested, and approved program changes related to Versa: Regulation are implemented into the production environment.

Original Agency Response

The department's existing change management policies and procedures are designed to ensure that only authorized, tested, and approved program changes are implemented into the Versa: Regulation production environment. The department agrees, however, that additional monitoring would provide additional assurance. To this end, we will evaluate our existing change management procedures to identify opportunities for improvement. We will also evaluate the feasibility of modifying the application's functionalities in this regard.

Status as of December 2016

The department is still evaluating improvements to meet this recommendation.

OIG Assessment:

OPEN. The department is currently working to establish controls related to Versa: Regulation program changes. The Office of Inspector General will continue to monitor this issue pending adoption and implementation of these controls.

Finding 2: Appropriateness of Access Privileges

The access privileges for some department employees did not promote an appropriate separation of duties and did not restrict users to only those functions appropriate and necessary for their assigned job duties.

Recommendation

We recommend that department management limit user access privileges to Versa: Regulation and the production database to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

Original Agency Response

The department concurs with these recommendations. The department's *Information Systems Security Policy* (DBPR Policy 2.3) requires supervisors to identify least privilege security roles and permissions for each employee granted access to department IT resources, including Versa: Regulation. The policy further requires supervisors to regularly review the access privileges of staff and ensure such access is appropriate for their job duties. During the course of the Auditor General's review, Division of Technology management reviewed the Versa: Regulation permissions of those technology staff identified by the auditors and modified any unnecessary privileges, accordingly. The Division of Technology relies on supervisors in each departmental business unit to identify appropriate access for their employees. To facilitate proper oversight of user privileges, the Division of Technology conducts periodic Versa: Regulation entitlement reviews, at which time supervisors must certify that the employee's access remains appropriate for the responsibilities of the position or notify the division of any required changes.

Status as of December 2016

The Division of Technology conducted an entitlement review for the Modify License Standing Role (LIC_MOD) for the entire department in November 2016. The division intends to perform this review every quarter. Currently, the division is in the process of sending out an annual entitlement review to all business units to verify user access and permissions according to "least privilege."

OIG Assessment:

CLOSED. The Division of Technology has conducted entitlement reviews of Versa: Regulation access privileges. Department staff was also recently required to read and acknowledge the *Information Systems Security Policy*, in which supervisors are to identify and limit access privileges for employees. Based on our discussion with management and review of supporting documentation we concluded that management's actions are sufficient to close this audit finding and recommendation.

Finding 3: Employee Access Deactivation

The department did not timely deactivate the Versa: Regulation accounts for one former and one transferred employee.

Recommendation

We recommend that department management ensure that the Versa: Regulation accounts of former and transferred employees are timely deactivated.

Original Agency Response

The department concurs with this recommendation. The department's existing *Information Systems Security Policy* (DBPR Policy 2.3) requires supervisors to notify the Division of Technology immediately upon a user's separation from or movement within the department. To help ensure adherence to this policy, the Division of Technology will communicate these requirements through periodic email notifications to supervisory staff and in the regularly scheduled meetings of senior and executive staff.

Status as of December 2016

The department's security policy was updated in November 2016 to comply with this recommendation. In addition, PeopleFirst batch jobs used by the Division of Technology have been updated to notify the Chief Information Officer and Infrastructure Chief when employees move from one business unit to another within the department. These notifications are sent daily by email to ensure proper forms are requested so that Versa: Regulation permissions are updated accordingly.

OIG Assessment:

CLOSED. Based on our discussion with management and review of supporting documentation we concluded that management's actions are sufficient to close this audit finding and recommendation.

Finding 4: Retention of Access Control Records

Contrary to the retention requirements set forth in the State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies*, the department did not retain relevant Versa: Regulation access control records related to the deactivation of employee access privileges.

Recommendation

We recommend that department management ensure that relevant Versa: Regulation access control records are retained as required by the General Records Schedule.

Original Agency Response

In accordance with the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies, the department's Division of Technology retains requests to add, modify, or remove user permissions for all business systems, including Versa: Regulation, by use of access request forms and the Remedyforce tracking system. The department acknowledges that access control records are not retained within the Versa: Regulation application itself. The Division of Technology will therefore explore the feasibility of enhancing existing records retention procedures by modifying the Versa: Regulation system to capture permission changes.

Status as of December 2016

Custom modification of the Versa: Regulation functionality to capture permission changes are currently underway.

OIG Assessment:

CLOSED. The Division of Technology retains Versa: Regulation access privileges request forms in compliance with the State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies*. The Division of Technology is also working to capture these permission changes within the Versa: Regulation system itself. Based on our discussion with management and review of supporting documentation we concluded that management's actions are sufficient to close this audit finding and recommendation.

Finding 5: Security Controls – User Authentication, Logging, and Monitoring

Certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources need improvement to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

Recommendation

We recommend that department management improve certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

Original Agency Response

The department has implemented improved security controls in certain areas and is actively working to develop and implement additional improvements to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related information technology resources.

Status as of December 2016

The department is still working to develop improvements according to these recommendations.

OIG Assessment:

OPEN. The department is currently working to establish controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources The Office of Inspector General will continue to monitor this issue pending adoption and implementation of these controls.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this follow-up report was to determine the status of action taken by management of the Division of Technology in response to the findings and recommendations made in Auditor General Report Number 2016-198, *Information Technology Operational Audit: Versa Regulation*. Our review focused on corrective action taken since the report's publication on June 21, 2016.

In December 2016, Division of Technology management provided updated information on the status of its implementing actions. We reviewed the information and supporting documentation and met with division management regarding specific issues the Auditor General did not disclose in the written report.

This work product was prepared pursuant to Section 20.055, Florida Statutes, and in accordance with applicable *Principles and Standards for Offices of Inspector Generals* (as published by the Association of Inspectors General) and *International Standards for the Professional Practice of Internal Auditing* (as published by the Institute of Internal Auditors, Inc.).