CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

Report IA 21-502

Office of Inspector General

Audit of the Department of Financial Services' Division of Agent And Agency Services, Bureau Of Licensing Confidential Data Access

Informational technology operational audit performed by the Office of Inspector General to evaluate whether internal controls of the Department of Financial Services' Division of Agent and Agency Services, Bureau of Licensing over confidential data are adequate and operating effectively

David T. Harper, Inspector General
Office of Inspector General
Department of Financial Services

May 3, 2021

CONTENTS

EXECUTIVE SUMMARY

The Department of Financial Services (DFS), Office of Inspector General (OIG) conducted an information technology operational audit of the DFS Division of Agent & Agency Services (AAS), Bureau of Licensing (BOL). The overall objective of this audit was to provide leadership with an independent assessment relating to the effectiveness of general information technology (IT) controls to secure confidential data for BOL applications. The audit focused on select general IT controls for two BOL applications, Automated Licensing Information System (ALIS) and Department of Insurance Continuing Education (DICE), that are used to administer insurance agents' licensing and education requirements. Specifically, the audit focused on access controls and segregation of duties.

Effective IT general controls are required to maintain data confidentiality, integrity and availability. The audit disclosed that there are opportunities for BOL and the Office of Information Technology (OIT) to strengthen access and segregation of duties controls. During the audit, BOL took some corrective action to address issues identified.

INTRODUCTION, BACKGROUND, AUDIT OBJECTIVE AND SCOPE

Introduction

The Office of Inspector General (OIG), Internal Audit Section, conducted an audit of Agency and Agency Services (AAS) Bureau of Licensing (BOL) confidential data access controls. This audit was based on our Fiscal Year 2020-2021 Annual Audit Work Plan and conducted in conformance with professional standards.

Background

Florida Statutes, Section 626.112 states that no person may be, act as, or advertise or hold himself or herself out to be an insurance agent, insurance adjuster, customer representative, service representative, or managing general agent unless he or she is currently licensed by the Department and appointed by an appropriate appointing entity or person. All licenses require an appointment, except for insurance agency licenses.

BOL consists of forty-two full-time positions comprising three units: The Education, Applications, and Analysis and Records. BOL responsibilities includes issuing and renewing licenses and appointments for regulated insurance agents and agencies. BOL is also responsible for overseeing the examination process for insurance representative. Additionally, BOL approves and monitors pre-licensing and continuing education providers, courses and instructors. The Automated Licensing Information System (ALIS) and Department of Insurance Continuing Education (DICE) applications, that store confidential data, are used to administer insurance agents' licensing and education requirements.

During FY 2019-20 BOL:

- Processed 125,288 new license applications and 2,061,738 appointment actions (new, renewals and terminations)
- Issued 115,816 new licenses
- Administered approximately 44,724 licensing examinations
- Approved and monitored 496,927 completed pre-licensing and continuing educations courses

Audit Objective and Scope

The audit objective and scope were to:

- Evaluate the effectiveness of general information technology (IT) controls to secure confidential data for BOL applications.
- The audit scope was from July 1, 2019 through June 30, 2020 and related activities through the end of fieldwork.

OBSERVATIONS AND RECOMMENDATIONS

Issue 1: Application Access Reviews

Florida Administrative Code[1] requires each agency to ensure access to IT resources is limited to authorized users and processes. Additionally, the Department's Access Control Policy require access privileges are assigned based on an employee's role and access is reviewed quarterly. The audit disclosed BOL did not conduct ALIS and DICE quarterly access reviews. Also, ALIS and DICE permissions were assigned to employees that were not required for their responsibilities and there were active service accounts[2] that were no longer required. Specifically, the audit identified:

- For 3 of the 10 BOL staff ALIS permissions reviewed, some permissions were assigned that were not required for their responsibilities
- For 4 of the 4 BOL staff that changed roles during the audit scope, some ALIS permissions were assigned that were not required for their responsibilities
- 10 BOL staff were assigned the ALIS Administer User Accounts permission that was not required for their responsibilities
- 9 ALIS service accounts were identified as obsolete
- 1 DICE user account was identified as obsolete

During audit fieldwork, BOL removed all ALIS permissions and the DICE user account, identified above, for staff, that were not required for their responsibilities. BOL also removed the obsolete ALIS service accounts during audit fieldwork.

The audit also disclosed that there are three ALIS roles, Work Queue Administrator, Work Queue Supervisor and Indexer Supervisor, that include ALIS Administer User Accounts permission as a default permission which is not required for staff that are assigned those roles.

Recommendation

The OIG recommends BOL develop and implement policy and procedures to conduct quarterly access reviews to identify and remove ALIS and DICE user permissions that are not required for their responsibilities and obsolete service accounts. Additionally, the OIG recommends the ALIS Administer User Accounts permission is removed from the ALIS Work Queue Administrator, Work Queue Supervisor and Indexer Supervisor roles.

Issue 2: Inactive ALIS and DICE Accounts

Based on the confidential data stored in ALIS and DICE, security standards[3] require organizations identify a timeframe for removing inactive accounts. Also, Department policy and procedures[4]

[1] FAC 60GG-2 Information Technology Security

[2] Service accounts are utilized to process background application functions.

[3] NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations; NIST Special Publication 800-53B, Control Baselines for Information Systems and Organizations, October 2020

[4] AP&P 4-03 Information Technology Security Policy

(Security Policy) require that accounts identified as being unused are assessed and where necessary, deactivated.

The Department does not have a policy that identifies a timeframe for when inactive accounts should be removed. Additionally, the audit disclosed BOL did not review ALIS inactive user accounts during the audit period. There were 29 ALIS user accounts that were not access for 6 months or longer. Specifically, the ALIS accounts were not accessed 244-4905 days. During the audit fieldwork, BOL removed 19 of the inactive ALIS accounts.

The audit also disclosed that DICE does not have a report that identifies the last login date for user accounts. Therefore, inactive DICE accounts could not be identified.

Recommendation

The OIG recommends OIT implement a defined timeframe standard for deactivating inactive accounts that are used to access confidential data. The OIG also recommends OIT develop a report that identifies DICE account last login dates that will allow inactive accounts to be identified and removed. Additionally, BOL should develop and implement policy and procedures to identify and remove ALIS and DICE inactive accounts.

Issue 3: Segregation of Duties

The Department's Access Control Policy requires a segregation of duties between the Access Control Administrator (ACA) that is responsible for providing application access and the staff responsible for routinely reviewing application access. The audit disclosed BOL ACA is performing some application access reviews.

Recommendation

The OIG recommends BOL assign application access reviews to staff that are not responsible for providing access to applications.

Issue 4: Shared ALIS Account

The Department's Access Control Policy states that users must not share a user account. The audit disclosed OIT shared a user account that had the ALIS Administer User Accounts permission.

Recommendation

The OIG recommends OIT remove the shared ALIS user account and assign individual ALIS user accounts for staff requiring access based on their responsibilities.

Issue 5: ALIS and DICE User Authentication

The Department Security Policy and security standards require certain authentication settings for ALIS and DICE. The audit disclosed that certain security controls related to user authentication need improvement. The specific details of the issues will be provided to appropriate Department leadership.

METHODOLOGY

This IT operational audit conforms with The International Professional Practices Framework (IPPF), published by The Institute of Internal Auditors. The IPPF requires the OIG to consider risk when planning to perform the audit and obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions that align with audit objectives. Additionally, the IPPF requires the auditors to meet objectivity requirements and possess necessary collective knowledge, skills and experience. The audit evidence obtained provides a reasonable basis for the OIG findings and conclusions.

To accomplish audit objectives, the OIG performed the following audit procedures:

- Reviewed specific Florida Statutes and Florida Administrative Code, National Institute of Standards and Technology (NIST) Security and Privacy Controls, DFS AP&Ps and AAS IP&Ps
- Conducted interviews with BOL leadership and staff
- Conducted testing of general IT controls

MANAGEMENT'S RESPONSE

The AAS BOL and OIT responses are provided as an attachment and the DFS OIG agrees with the response.

ACKNOWLEDGEMENTS

The OIG would like to thank AAS BOL and OIT leadership and staff for their input, cooperation and assistance throughout the performance of this engagement.

The Office of Inspector General performs audits, consulting activities, and reviews of Department of Financial Services' programs, activities, and functions to promote accountability, integrity, and efficiency in state government.

This consulting engagement was conducted in conformance with The *International Standards for the Professional Practice of Internal Auditing*, published by The Institute of Internal Auditors, Inc., pursuant to Section 20.055, Florida Statutes, and *Principles and Standards for Offices of Inspectors General*, published by the Association of Inspectors General. This engagement was conducted by Helene Muth, CIA, CISA, Senior Auditor, under the supervision of Debbie Clark, CPA, CISA, CIGA, Director of Audit.

Please address inquiries regarding this report to the DFS Office of Inspector General at 850-413-3112.

DISTRIBUTION LIST

Jimmy Patronis, Chief Financial Officer
Peter Penrod, Chief of Staff
Frank Collins, Deputy Chief Financial Officer
Greg Thomas, Director of Division of Insurance Agents & Agency Services,
Scott Stewart, Chief Information Officer, Office of Information Technology

ATTACHMENT

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Issue 1: Application Access Reviews

The audit disclosed BOL did not conduct ALIS and DICE quarterly access reviews. Also, ALIS and DICE permissions were assigned to employees that were not required for their responsibilities and there were active service accounts that were no longer required.

Recommendation: The OIG recommends BOL develop and implement policy and procedures to conduct quarterly access reviews to identify and remove ALIS and DICE user permissions that are not required for their responsibilities and obsolete service accounts. Additionally, the OIG recommends the ALIS Administer User Accounts permission is removed from the ALIS Work Queue Administrator, Work Queue Supervisor and Indexer Supervisor roles.

Response: BOL has updated and adopted the attached Division Application Access Control policy and procedures which include quarterly access reviews by the ACA to identify and remove ALIS and DICE user access and permissions that are not required for their responsibilities and to remove obsolete accounts which we define as accounts not accessed within the previous 90 days.

In addition, the updated policy and procedures include a quarterly audit every September, December, March, and June by the Assistant Division Director and a monthly audit of CJIS training and records to ensure user's biennial compliance.

The Division has requested OIT to develop and provide the monthly User Reports with the user details that are listed in the policy and procedures and are listed in the response to Issue 2 below.

In addition, the ALIS Administer User Accounts permission was removed on April 16, 2021 as an automatically enabled permission from the ALIS Work Queue Administrator, Work Queue Supervisor and Indexer Supervisor roles. The ALIS Administer User Accounts permission has been retained for the Access Control Administrator and their backups.

Expected Completion Date for Corrective Action: April 26, 2021

Issue 2: Inactive ALIS and DICE Accounts

The Department does not have a policy that identifies a timeframe for when inactive accounts should be removed. Additionally, the audit disclosed BOL did not review ALIS inactive user accounts during the audit period. There were 29 ALIS user accounts that were not access for 6 months or longer. Specifically, the ALIS accounts were not accessed 244-4905 days. During the audit fieldwork, BOL removed 19 of the inactive ALIS accounts.

The audit also disclosed that DICE does not have a report that identifies the last login date for user accounts. Therefore, inactive DICE accounts could not be identified.

Recommendation: The OIG recommends OIT implement a defined timeframe standard for deactivating inactive accounts that are used to access confidential data. The OIG also recommends OIT develop a report that identifies DICE account last login dates that will allow inactive accounts to be identified and removed. Additionally, BOL should develop and implement policy and procedures to identify and remove ALIS and DICE inactive accounts.

Response: BOL: Per the updated Division Application Access Control Policy & Procedure, attached, until OIT implements a department policy, the Division has implemented a policy and procedure in which to terminate inactive ALIS accounts after 90 days of inactivity.

The Division, though the policy was implemented on April 26, 2021, has reviewed all inactive accounts as defined by the updated policy and has terminated all inactive accounts.

The Division has requested OIT to develop and provide the monthly User Reports for the following user groups which include the following User Details. The initial reports have been created and submitted and are currently just being refined for ease of use.

User Groups Categories
1. Users with both an Active Role and an Active Permission
2. Users who became inactive or terminated within the previous 90 days.
3. Users who have had permissions or role modifications within the previous 90 days.

User Details
1. User ID
2. Last Name
3. First Name
4. Division
5. Role
6. Role Status
7. Permission
8. Permission Status
9. Last Login
10. Active Role Count
11. Inactive Role Count
12. Date Access Granted (Start, Creation Date)
13. Date Access Removed (if applicable)
14. Date Access Level Updated (ifapplicable)

OIT: OIT concurs. OIT has made revisions within the policy 4-05, Application Access Control. These revisions are in a draft form and under review by executive level management.

Expected Completion Date for Corrective Action: BOL**:** April 26, 2021, OIT: December 31, 2021

Issue 3: Segregation of Duties

The audit disclosed BOL ACA is performing some application access reviews.

Recommendation: The OIG recommends BOL assign application access reviews to staff that are not responsible for providing access to applications.

Response: Quarterly Audits and Monthly Audits, per the attached Division Application Access Control policy and procedures, will be performed by the Assistant Division Director who is not responsible for providing access to applications.

These audits will be in addition to the quarterly and monthly review performed by the ACA.

Expected Completion Date for Corrective Action: April 26, 2021

Issue 4: Shared ALIS Account

The audit disclosed OIT shared a user account that had the ALIS Administer User Accounts permission.

Recommendation: The OIG recommends OIT remove the shared ALIS user account and assign individual ALIS user accounts for staff requiring access based on their responsibilities.

Response: AAS**:** The shared OIT user account was terminated on March 9, 2021 and the respective OIT employees were assigned individual User Accounts. The attached Policy & Procedure requires individual employee User Accounts.

OIT: OIT concurs. OIT has removed the shared account and individual accounts for the OIT users needing the ALIS access have been created.

Expected Completion Date for Corrective Action: Complete

Issue 5: ALIS and DICE User Authentication

The audit disclosed that certain security controls related to user authentication need improvement.

Recommendation: The OIG recommends OIT improve ALIS and DICE authentication controls to comply with the Department Security Policy and security standards.

Response: BOL: The Division of Agent & Agency Services has submitted a remedy ticket requesting OIT program ALIS and DICE user authentications to comply with the Department's Security Policy and security standards. The programming that has been approved is a login verification for ALIS and DICE Internal using the internal Active Directory (Network) verification. OIT has determined that this authentication method is best and the preferred method and is in agreement with this request.

OIT: OIT concurs. Our primary goal is researching options for the best method of remediation as well as evaluating the cost-benefit of meeting the minimum requirements of the security controls under industry standards and requirements per NIST SP 800-53 and Rule Chapter 60GG-2, F.A.C.

Expected Completion Date for Corrective Action: AAS: Request sent to OIT on 4/21/2021. Completion contingent on when OIT can complete the system changes, currently in development. Each system is estimated to take 160 hours of programming to complete.

OIT: December 31, 2021