CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

OFFICE OF INSPECTOR GENERAL
REPORT IA 22-504

CYBERSECURITY CONTINUOUS MONITORING

Division: Office of Information Technology

Subject: Audit of Cybersecurity Continuous Monitoring for the Florida Planning, Accounting, and Ledger Management (PALM) by the Office of Information Technology

Conclusion: The OIG concluded that the DFS' internal controls related to the cybersecurity monitoring for the Florida PALM were generally adequate and compliant with Rule 60GG-2.004(2), Florida Administrative Code, Security Continuous Monitoring, regarding IT resource monitoring to identify cybersecurity events, for the period July 1, 2021, through January 31, 2022.

Auditors: Tingting Fan, Crista Hosmer, Jasmine London

David T. Harper, Inspector General
Office of Inspector General
Florida Department of Financial Services
May 26, 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Financial Services (DFS), Office of Inspector General (OIG) conducted a compliance audit of the DFS' cybersecurity continuous monitoring within the Office of Information Technology (OIT) for the Florida Planning, Accounting, and Ledger Management (PALM).[1] This audit focused on the internal controls that the DFS had implemented for continuous monitoring of its information technology (IT) resources to identify cybersecurity events. The audit reviewed the DFS' cybersecurity practices from July 1, 2021, through January 31, 2022.

The OIG determined that the DFS had implemented adequate controls over the cybersecurity monitoring for the Florida PALM to identify cybersecurity events. Additionally, the DFS' IT resource monitoring practices were compliant with Rule 60GG-2.004(2), Florida Administrative Code (F.A.C.).

[1] The Florida Planning, Accounting, and Ledger Management (PALM) is the Florida Financial Management Information System, as provided in sections 215.90 – 215.96, Florida Statutes (F.S.). It is developed to replace the current Florida Accounting and Information Resource (FLAIR) and Cash Management System (CMS) with an integrated, enterprise financial management solution that will allow the state to organize, define, and standardize its financial management processes. This information is available on the Florida PALM website: https://www.myfloridacfo.com/floridapalm/.

INTRODUCTION

The DFS OIG conducted a compliance audit of the DFS' cybersecurity continuous monitoring within the OIT for the Florida PALM, a unified system providing fiscal, management, and accounting support for state decision-makers.[2] This audit was based on the OIG's fiscal year (FY) 2021-2022 Annual Audit Work Plan and in response to the legislative mandate.[3] The scope of the audit was limited to the DFS' internal controls over the cybersecurity continuous monitoring of the Florida PALM. The OIG's review included the DFS monitoring policies, procedures, activities, and processes from July 1, 2021, through January 31, 2022.

BACKGROUND

The DFS OIT has a total of 208 positions located within five sections.[4] The OIT manages a total of 217 solutions,[5] 773 components, 89 database servers, and 216 application servers, according to the OIT Application Inventory System (AIS) as of May 12, 2022. The OIG review of the solutions identified zero solutions with a Federal Information Processing Standard (FIPS)[6] impact level of high, nine with an impact level of moderate, and two with an impact level of low. The remaining 206 solutions were not classified.

The Information Security Manager (ISM) resides in the Audit & Compliance Office within the OIT. According to the ISM Designation Memo,[7] the ISM is responsible for the following functions:

- Development of a strategic information security plan and associated operational information security plan
- Development and implementation of agency security policies, procedures, standards, and guidelines
- Direction and management of the agency information security awareness program
- Coordination of the agency information security risk management process
- Coordination of the agency Computer Security Incident Response Team
- Coordination of Information Technology Disaster Recovery planning and support of the agency Continuity of Operations Plan
- Serving as the agency's internal and external point of contact for all information security matters

[2] Section 215.91(2), F.S., identifies the purpose of establishing the Florida Financial Management Information System.
[3] Per section 20.055(6)(i), F.S., the agency inspector general shall develop long-term and annual plans that include a specific cybersecurity audit plan.
[4] Per the OIT Organizational Chart, updated on May 2, 2022, the OIT comprises five sections: Bureau of Enterprise Applications, Office of Enterprise Financial Support Services, Administrative Services, Bureau of Distributed Infrastructure, and the Audit & Compliance Office.
[5] Per Gartner Information Technology Glossary, a solution is an implementation of people, processes, information, and technologies in a distinct system to support a set of business or technical capabilities that solve one or more business problems. This definition is available on the Gartner website: https://www.gartner.com/en/information-technology/glossary/solution.
[6] Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, issued by the National Institute of Standards and Technology (NIST) in February 2004, establishes security categories for both information and information systems within the Federal Government. FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity, and availability; rating each system as low, moderate, or high impact in each category.
[7] DFS ISM Designation Memo, effective July 9, 2021, specifies the duties of the ISM.

- Reporting directly to the agency head in all information security duties
- Otherwise complying with applicable law for information security as well as the rules, policies, procedures, and best practices promulgated by the Division of State Technology[8]

The OIT completed the most recent Risk Assessment Tool[9] in July 2020, providing a department-wide assessment of all functions identified in the Florida Cybersecurity Standards, Rule 60GG-2, F.A.C., including an assessment of security continuous monitoring. Additionally, the DFS adopted the Florida Cybersecurity Standards requiring security continuous monitoring of its IT resources to identify cybersecurity events and verify the effectiveness of its protective measures.[10]

The Florida PALM housed in the DFS is replacing the current Florida accounting and cash management systems, which have been outpaced by the state's needs, with a cloud-based financial management solution.[11] It is a state-wide system with multiple layers of external connections and is by far the largest project in DFS. This system is an integrated, enterprise financial management solution that allows the state to organize, define, and standardize its financial management processes. The DFS initiated its multi-year endeavor, the Florida PALM Project, in July 2014 and executed a contract in July 2018 to design, build, and implement the Florida PALM. As of July 6, 2021, all state agencies transitioned to the Florida PALM for cash management services functionality.[12]

RESULTS OF REVIEW

The OIG concluded that the DFS' internal controls related to the cybersecurity monitoring for the Florida PALM were generally adequate and compliant with Rule 60GG-2.004(2), F.A.C., Security Continuous Monitoring, regarding IT resource monitoring to identify cybersecurity events, for the period July 1, 2021, through January 31, 2022.

[8] Chapter 2020-161, Laws of Florida, effective July 1, 2021, removes the Division of State Technology from the Department of Management Services (DMS) and creates the Florida Digital Service (FLDS) housed in DMS. The state Chief Information Officer administers the FLDS and is appointed by the DMS Secretary.
[9] Florida Cybersecurity Standards (FCS) Risk Assessment Tool (v2.3) is to offer state agencies a uniform way to comply with risk assessment requirements outlined in section 282.318, F.S., and the FCS, Rule 60GG-2, F.A.C. State agencies are required to complete it tri-annually. The risk assessment tool is available for download on the DMS website: https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council/cybersecurity_resources.
[10] DFS Administrative Policies and Procedures (AP&P) 4-03, Information Technology Security, effective June 28, 2021.
[11] Florida PALM operates on Oracle® PeopleSoft 9.2, leveraging a Service Oriented Architecture (SOA), hosted by Oracle Cloud Infrastructure and connected via MyFloridaNet-2. It is a web-based single sign-on experience. This information is available on the Florida PALM website: https://myfloridacfo.com/docs-sf/florida-palm-libraries/financials-wave/project-history.pdf?sfvrsn=412fc7_2.
[12] Per the Florida PALM Project Timeline, the project has a timeline that is broken down into distinct periods: CMS Wave – (Completed) – all agencies transitioned to Florida PALM for CMS functionality; Financial Wave – all agencies will transition to Florida PALM for Central and Departmental FLAIR functionality and for historical Information Warehouse (IW) data -TBD; Payroll Wave – all agencies will transition to Florida PALM for Payroll functionality – TBD. The timeline information is available on the Florida PALM website: https://myfloridacfo.com/floridapalm/implementation/resources/timeline.

PURPOSE, SCOPE, OBJECTIVES, AND METHODOLOGY

The purpose of the audit was to evaluate the DFS' controls over the cybersecurity monitoring of the Florida PALM for compliance with the Florida Cybersecurity Standards, Rule 60GG-2.004(2), F.A.C., Security Continuous Monitoring, regarding IT resource monitoring to identify cybersecurity events.

The scope of the audit focused on the DFS' cybersecurity continuous monitoring policies, procedures, activities, and processes for the Florida PALM for the period July 1, 2021, through January 31, 2022.

The audit objectives were to assess the DFS's cybersecurity practices in the following areas:

- Monitoring the network to detect potential cybersecurity events
- Monitoring the physical environment to detect potential cybersecurity threats
- Monitoring user activity to detect potential cybersecurity events
- Monitoring for malicious code
- Monitoring for unauthorized mobile code
- Monitoring for external service provider activity to detect potential cybersecurity events
- Monitoring for unauthorized personnel, connections, devices, and software
- Performing vulnerability scans which are part of the System Development Life Cycle

This 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 the audit objectives. Additionally, the IPPF requires the auditors to meet objectivity requirements and possess the necessary collective knowledge, skills, and experience. The OIG believes that the audit evidence obtained provides a reasonable basis for the OIG findings and conclusions.

To accomplish the audit objectives, the OIG:

- Reviewed applicable rules, laws, standards, and the DFS policies and procedures
- Conducted interviews with appropriate DFS staff regarding the processes and controls implemented in the IT resource monitoring
- Reviewed the OIT procedural documents and the system artifacts of the Florida PALM
- Performed testing of controls related to the Florida PALM security monitoring

ACKNOWLEDGEMENTS

The OIG would like to thank the OIT leadership and the Florida PALM team for their input, cooperation, and assistance throughout the performance of this engagement.

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

This 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 the OIG audit team, including Tingting Fan, CISA, Senior Auditor and Auditor-in-Charge, Crista Hosmer, CIA, CIGA, CIGE, FCCM, Senior Auditor, and Jasmine London, CIGA, FCCM, Auditor, under the supervision of Debbie Clark, CPA, CIA, CISA, CIGA, CGAP, Director of Audit.

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

DISTRIBUTION LIST

Scott Stewart, Chief Information Officer
Jimmy Cox, Director, the Florida PALM Office
Michael Kyvik, Information Security Manager
Scott Fennell, Deputy Chief Financial Officer
Susan Miller, Deputy Chief of Staff
Peter Penrod, Chief of Staff
Jimmy Patronis, Chief Financial Officer
Melinda M. Miguel, Chief Inspector General
Sherrill F. Norman, Florida Auditor General