FDLE

Florida Department of
Law Enforcement

J. Mark Glass
Commissioner

Office of Inspector General
Post Office Box 1489
Tallahassee, Florida 32302-1489
(850) 410-7228
www.fdle.state.fl.us

Ron DeSantis, *Governor*
Ashley Moody, *Attorney General*
Jimmy Patronis, *Chief Financial Officer*
Wilton Simpson, *Commissioner of Agriculture*

MEMORANDUM

DATE: July 19, 2024

TO: J. Mark Glass, Commissioner
Office of Executive Director

FROM: Lourdes Howell-Thomas, Inspector General
Office of Inspector General (OIG)

SUBJECT: Six-Month Follow-Up Report
Auditor General Report Number 2024-111
Information Technology Operational Audit
FDLE Information Technology General Controls

The Auditor General completed an audit of the FDLE Information Technology General Controls in January 2024. The final report included four findings with recommendations for corrective action. In accordance with the provisions of s. 20.055(6)(h), Florida Statutes, the OIG conducted a six-month follow-up.

The attached *Six-Month Follow-up Status Report* details the latest implementation status as of July 2024. The Department has taken steps to address the recommendations; however, two of the findings remain open. The remaining recommendations will be re-evaluated at a future date.

We appreciate the assistance and cooperation provided by members of the Information Technology Services division during this project.

If further information is needed, please contact me at (850) 410-7241.

LHT/jd

Attachment

cc: Joint Legislative Auditing Committee
Matt Walsh, Deputy Executive Director, Office of Executive Director
Annie White, Assistant Commissioner, Office of Executive Director
Joey Hornsby, Director, Information Technology Services

Six-Month Status Report

Auditor General Report No. 2024-111 Information Technology Operational Audit

FDLE Information Technology General Controls

OIG Report Number FP-2324-01

Information Technology Services

Finding 1: Department cybersecurity incident response policies, procedures, and related documentation were out of date and did not include required notification procedures for Cybersecurity Incident Response Team (CSIRT) members. Additionally, CSIRT members did not receive required annual incident response training.

Recommendation: We recommend that Department management update incident response policies, procedures, and incident response plan scenarios documentation to incorporate the CSIRT notification procedures specified in DMS rules and ensure that CSIRT members receive annual incident response training in accordance with DMS rules.

FDLE Initial Response: Agree. FDLE will update policies and procedures to address this finding. FDLE is participating in the FLDS annual CSIRT training.

FDLE Six-Month Response: This has been completed.

Six-Month Status: Completed.

Finding 2: Department backup policies and procedures and processes, including periodic recoverability testing and off-site storage controls, need improvement.

Recommendation: We recommend that Department management enhance policies and procedures to require periodic recoverability testing and define the frequency and retention period for backups. We also recommend that Department management ensure that backups are periodically tested for recoverability and off-site backup media is stored in a location geographically separated from the primary operating location.

FDLE Initial Response: Agree. A procedure outlining backup frequency, retention and testing has been drafted and will be implemented.

FDLE Six-Month Response: This has been completed.

Six-Month Status: Completed.

Finding 3: Department disaster recovery processes need improvement, including conducting a business impact analysis, developing a disaster recovery plan, and completing annual testing.

Recommendation: To ensure the recoverability of critical Department systems in the event of a disaster or other interruption of service, we recommend that Department management:

- Conduct a BIA that documents the assessment of the criticality of all Department systems for DR purposes.
- Identify system dependencies for critical systems.
- Determine MTD, RPO, and RTO thresholds for critical systems.
- Develop and document a DR plan that includes Department personnel roles, responsibilities, and contact information, vendor information, and step-by-step recovery instructions for critical systems.
- Ensure that the DR plan is tested at least annually and documentation of live DR testing is maintained.

FDLE Initial Response: Agree. FDLE has submitted a legislative budget request (LBR) for security resources to enhance our information security program which includes disaster recovery.

FDLE Six-Month Response: Security staff for IT Security (including DR) was associated with a LBR request for FY 24-25. EOG requested we cut our request down to 3 FTEs and 1 contractor. These positions will be funded on 7/1/2024 and ITS has started the advertisement/hiring process. One FTE position will be assigned to Disaster Recovery however, ITS is submitting another LBR for FY 25-26 for the remaining positions.

Six-Month Status: In progress.

Finding 4: Certain security controls related to logical access, user authentication, vulnerability management, physical access, and configuration management need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, vulnerability management, physical access, and configuration management to ensure the confidentiality, integrity, and availability of Department data and IT resources.

FDLE Initial Response: Agree – FDLE will update policies and procedures to address this finding.

FDLE Six-Month Response: This has been completed. This refers to the confidential findings. All confidential findings have been completed except confidential findings 3 and 4, both are LBR issues similar to finding 3 above.

Six-Month Status: In progress.