STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2024-111
January 2024

DEPARTMENT OF LAW ENFORCEMENT

Information Technology General Controls

Sherrill F. Norman, CPA
Auditor General

Executive Director of the Department of Law Enforcement

The Department of Law Enforcement is established by Section 20.201, Florida Statutes. The head of the Department is the Governor and Cabinet. The Executive Director of the Department is appointed by the Governor, subject to a majority vote of the Governor and Cabinet, with the Governor on the prevailing side. The appointment is subject to confirmation by the Senate. Mark Glass served as Executive Director during the period of our audit.

The team leader was Cara Hill and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

DEPARTMENT OF LAW ENFORCEMENT

Information Technology General Controls

SUMMARY

This operational audit of the Department of Law Enforcement (Department) focused on evaluating selected significant information technology (IT) general controls. Our audit disclosed the following:

Finding 1: Department cybersecurity incident response policies, procedures, and related documentation were out of date and did not include required notification procedures for Cybersecurity Incident Response Team (CSIRT) members.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

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

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

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.

BACKGROUND

Pursuant to State law,[1] the mission of the Department of Law Enforcement (Department) is to promote public safety and strengthen domestic security by providing services in partnership with local, State, and Federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. In carrying out this mission, the Department is charged with delivering investigative, forensic, law enforcement information, criminal justice training, and protective services to the State's criminal justice community. The Department provides these services through five divisions: Executive Direction and Business Support; Criminal Investigations and Forensic Science; Criminal Justice Information; Criminal Justice Professionalism; and the Florida Capitol Police.

Within the Department, the Information Technology Services (ITS) Division is responsible for securing Department data, information, and IT resources, and providing and supporting the IT capabilities critical to the Department and the State's law enforcement community. ITS provides network services, hardware, software, programming, technical support, systems analysis, Web design, host and server support, end-user computing, and field system support for Department systems and databases, and manages the daily operations of the Department's data center and other ITS-secured areas. ITS also supports and serves as the steward for Florida's Criminal Justice Network, the network supporting all criminal justice agencies in the State and the gateway to other state, Federal and international agencies.

[1] Chapter 943, Florida Statutes.

FINDINGS AND RECOMMENDATIONS

Finding 1: Cybersecurity Incident Response

Department of Management Services (DMS) rules[2] require State agencies to establish and maintain response processes and procedures and validate execution capability to ensure timely response to detected cybersecurity incidents. DMS rules also require State agencies to establish a Cybersecurity Incident Response Team (CSIRT) to respond to cybersecurity incidents and specify that agency security incident reporting processes must include notification procedures established pursuant to State law.[3] CSIRT members are responsible for determining the appropriate response required for each cybersecurity incident and are to receive incident response training annually as part of the agency's information security program.

To evaluate the adequacy of Department cybersecurity incident response controls, we inquired of Department personnel and reviewed Department incident response policies[4] and procedures,[5] incident response plan scenarios documentation, and CSIRT meeting and training records. Our audit procedures found that:

- As of May 26, 2023, contrary to DMS rules, neither the Department incident response plan scenarios documentation nor related policies and procedures included incident response notification requirements, such as the types of cybersecurity incidents CSIRT members were to be notified of and when (time frame). In response to our audit inquiry, Department management indicated that the cybersecurity incident notification requirements for CSIRT members were inadvertently not specified and that the policies, procedures, and incident response plan scenarios documentation were out of date.
- CSIRT members had not received the required annual incident response training. According to Department management, annual incident response training for CSIRT members was not conducted because Department management was unaware of what the training should entail; however, training was conducted for the IT personnel responsible for remediating technical issues in the event of an incident.

Absent compliance with DMS rules requiring the establishment of cybersecurity incident notification procedures for CSIRT members and the receipt of annual incident response training, the risk is increased that cybersecurity incidents will not be timely and appropriately responded to and corrected.

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.

[2] DMS Rule 60GG-2.005(1)(a), Florida Administrative Code.

[3] Sections 282.318 and 501.171, Florida Statutes.

[4] Department Policy No. 2.5, *Information Security*.

[5] ITS Procedure 8.300, *Computer Security Incident Handling*.

Finding 2: Backup Controls

Effective backup controls include policies and procedures for routinely duplicating or backing up data files and computer programs, ensuring off-site backup media storage locations are geographically separated from the primary operating locations, and establishing a recovery and restoration capability, including periodically testing backup media so that data and computer programs can be recovered and restored after a disruption or failure. DMS rules[6] require State agencies to ensure that backups of information are conducted, maintained, and tested.

ITS personnel were responsible for performing server backups of Department-managed servers located in the Department's data center. As part of our audit, we interviewed Department personnel, reviewed Department backup policies[7] and desktop procedures, and evaluated Department backup processes. Our audit procedures found that, as of May 19, 2023, Department policies and procedures did not require periodic recoverability testing or define the frequency of data backups or the retention schedule for backup media. Additionally, the Department did not perform recoverability testing to help ensure the useability of backup data in the event of a disaster or other unexpected event. According to Department management, Department policies and procedures were out of date due to personnel turnover and that they were unaware that periodic recoverability testing of backup media was necessary.

Further, we evaluated Department off-site backup media storage controls and found that the off-site location used by the Department for the storage of backup media for Department production servers was in the same city as the servers. In response to our audit inquiry, Department management indicated that, due to the large volume of tapes, the backup media was stored locally to provide the Department the ability to quickly restore in the event of disaster or other interruption in service.

The absence of updated and comprehensive policies and procedures specifying frequency and retention requirements for recoverability testing and the maintenance of backup media; the absence of periodic recoverability testing; and storing off-site backup media near the primary operating location increases the risk that data on Department-managed server backups will not be readily recoverable and available when needed in response to a disaster or other unexpected events.

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.

Finding 3: Disaster Recovery

Disaster recovery (DR) planning is intended to facilitate the timely recovery of critical applications, data, and services in the event of a disaster or other interruption in service. A business impact analysis (BIA) helps identify and prioritize IT systems that are critical to supporting the organization's mission and includes determining the maximum tolerable downtime (MTD) for each system and the recovery point

[6] DMS Rule 60GG-2.003(5)(d), Florida Administrative Code.

[7] Department Policy No. 2.5, *Information Security*.

objective (RPO) and recovery time objective (RTO) for each critical system in the event of a disaster or other interruption in service. The DR plan should be based on a BIA and contain detailed guidance and procedures for restoring damaged systems, including recovery personnel and related contact information. Testing the DR plan helps ensure that critical systems can be restored in the event of a disaster or other interruption in service by validating recovery capabilities and identifying gaps in the DR plan. DMS rules[8] require State agencies to develop and implement a DR plan, test the DR plan at least annually, and document the results of the test, including DR plan procedures that were successful and any modifications required to improve the DR plan. Additionally, Department policies[9] required the Department to maintain DR plans for information systems identified as critical to continuity of operations in the event of a disaster and test DR plans at least annually.

Our review of Department disaster recovery processes found that the Department had not conducted a BIA to identify and prioritize the IT systems critical to supporting the Department's mission, the order of recovery in the event of a disaster, the MTD, RPO, and RTO for each critical system, and system dependencies. Additionally, the Department had neither developed a comprehensive entitywide DR plan nor conducted a live DR test to ensure that the Department could recover all critical Department systems in the event of a disaster or other interruption in service. According to Department management, a BIA, DR plan, and testing had not been completed due to other priorities.

Conducting a BIA that includes a review of the criticality of all Department systems for DR purposes, identifying system dependencies, defining MTD, RPO, and RTO thresholds, and documenting step-by-step instructions for the recovery of each critical application in an entitywide IT DR plan will help ensure that Department data and IT resources will be readily recoverable and available when needed. Additionally, conducting and documenting comprehensive live DR plan exercises annually for all critical systems decreases the risk that critical Department applications will not be timely and orderly resumed in the event of a disaster or other interruption in service.

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.**

[8] DMS Rule 60GG-2.006(1), Florida Administrative Code.

[9] Department Policy No. 2.5, *Information Security*.

Finding 4: Security Controls – Logical Access, User Authentication, Vulnerability Management, Physical Access, and Configuration Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, vulnerability management, physical access, and configuration management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the six findings in the five areas needing improvement.

Without appropriate security controls related to logical access, user authentication, vulnerability management, physical access, and configuration management, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

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.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from April 2023 through August 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant IT general controls applicable to Department of Law Enforcement (Department) operations during the period July 2022 through May 2023 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate the effectiveness of selected significant IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems

so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines, and interviewed Department personnel to obtain an understanding of the Department's organizational structure, statutory requirements, operational processes, and selected significant general controls.
- Obtained an understanding of the Department's network domain infrastructure, including the purpose and users of the various network domains and Department processes for: authorizing, assigning, disabling, and periodically reviewing administrative-level access to Department network domains; authenticating to the network domains and high-risk network devices; physically protecting access to the Department's data center and other sensitive IT areas; cybersecurity incident response; data backup; disaster recovery; configuration management, including patching for servers and other high-risk network devices; vulnerability management; and logging and monitoring of access to the Department data center and other sensitive IT areas.
- Evaluated logical access controls, including policies, procedures, and processes for authorizing, assigning, disabling, and periodically reviewing administrative-level user and service accounts for the Department network domains. Specifically, we evaluated:
    - Department procedures and examined Department records to determine whether periodic access reviews of the appropriateness of access to the Department network domains were performed.
    - The appropriateness, as of April 11, 2023, of the three administrative-level user accounts and one administrative-level service account for one Department network domain and the ten administrative-level user accounts and seven administrative-level service accounts for the other Department network domain.

- The appropriateness of interactive log on capabilities as of April 26, 2023, for the one administrative-level service account for one Department network domain and the seven administrative-level service accounts for the other Department network domain.
- The adequacy of security controls for the default *Administrator* account for the two Department network domains as of April 27, 2023.

- Evaluated the adequacy of user identification and authentication controls for the two Department network domains and high-risk network devices.
- Evaluated the adequacy of Department vulnerability management policies and procedures and the effectiveness of vulnerability management processes, including the timely performance of authenticated scans, analysis and remediation of identified vulnerabilities for the Department network infrastructure, and the routine performance of penetration testing. Specifically, we evaluated vulnerability scans performed in May 2023 for 13 network segments to determine whether vulnerabilities identified as critical or high on the Common Vulnerabilities and Exposures list were timely remediated.
- Evaluated the appropriateness of physical access controls to the Department's data center and telecommunications rooms housing sensitive IT resources, including the adequacy of policies, procedures, and processes established to protect sensitive Department IT resources and data. Specifically, we:
  - Observed physical access controls to the Department's data center and telecommunications rooms on April 17, 2023.
  - Evaluated the appropriateness of physical access privileges to the Department's data center and telecommunications rooms assigned to 94 individuals as of April 19, 2023.
  - Evaluated logging and monitoring controls over access to the Department's data center and telecommunications rooms.
  - Examined Department records to determine the adequacy of the annual review of physical access privileges to the Department's data center and telecommunications rooms.
- Evaluated the adequacy of the Department's cybersecurity incident response policies, procedures, and related documentation and examined Cybersecurity Incident Response Team (CSIRT) membership, meeting, and training records to determine whether the Department complied with Department of Management Services Rule 60GG-2.005(1)(a), Florida Administrative Code, for establishing and maintaining incident response processes and procedures.
- Evaluated the adequacy of Department disaster recovery controls, including Department policies and procedures, disaster recovery plan and related business impact analysis, and annual disaster recovery testing.
- Evaluated the adequacy of Department backup policies and procedures and evaluated backup processes for ensuring the recoverability of data in the event of a disaster or other interruption in service, including the regular performance of server backups, periodic recoverability testing of backup media, and storage of off-site backup media. Specifically, we evaluated daily backup server reports as of May 12, 2023, to determine whether Department-managed server backups were timely completed, and backup job errors were timely investigated and resolved.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.

- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

FDLE

Florida Department of Law Enforcement

J. Mark Glass
Commissioner

Office of Executive Director
Post Office Box 1489
Tallahassee, Florida 32302-1489
(850) 410-7001
www.fdle.state.fl.us

January 12, 2024

Ms. Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building
Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, I am providing the enclosed response to the preliminary and tentative audit findings and recommendations on the operational audit of:

Florida Department of Law Enforcement
Information Technology General Controls

I appreciate the efforts you and your staff provided to assist us in improving our operations. If you require further information, please contact Inspector General Lourdes Howell-Thomas at 850-410-7241.

Sincerely,

J. Mark Glass
Commissioner

JMG/lht

Service • Integrity • Respect • Quality

Auditor General
Information Technology Operational Audit
Florida Department of Law Enforcement
Information Technology General Controls
Preliminary and Tentative Audit Findings and Recommendations
Agency Response

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.

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

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.

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

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.

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

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.

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