STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2027-050
November 2026

INFORMATION TECHNOLOGY NETWORK SECURITY CONTROLS

At Selected State Agencies



Sherrill F. Norman, CPA
Auditor General

State Agency Heads and Commissioners

The State Constitution and Florida Statutes establish the various State agencies and provide the title and selection process for the head of each State agency. The table below shows the three State agencies included in the scope of this information technology operational audit and the respective agency heads and commissioners, as applicable, who served during the period of our audit.

State Agency	Established by	State Agency Heads and Commissioners
Department of Business and Professional Regulation	Section 20.165, Florida Statutes	Melanie S. Griffin, Secretary
Department of Health	Section 20.43, Florida Statutes	Dr. Joseph A. Ladapo, State Surgeon General and State Health Officer
Fish and Wildlife Conservation Commission	Section 20.331, Florida Statutes, and Article IV, Section 9 of the State Constitution	Roger Young, Executive Director Commissioners: Rodney Barreto, Chair Preston Farrior Steven Hudson Joshua Kellam Gary Lester Albert Maury Gary Nicklaus Sonya Rood

The Auditor General conducts audits of government 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.

The team leader was Benjamin Ho, CISA, 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

INFORMATION TECHNOLOGY NETWORK SECURITY CONTROLS

At Selected State Agencies

SUMMARY

This operational audit focused on evaluating selected information technology (IT) network security controls at the Department of Business and Professional Regulation (DBPR), the Department of Health (DOH), and the Fish and Wildlife Conservation Commission (FWCC). Our audit disclosed the following:

Finding 1: Certain network security controls at the DBPR, the DOH, and the FWCC need improvement to ensure the confidentiality, integrity, and availability of agency data and IT resources.

BACKGROUND

Management designs information technology (IT) control activities to support the entity's information systems and automated business processes. The control activities are fundamental components of an entity's internal control system and apply broadly across the IT environment. IT general controls are the overarching policies and procedures that apply to all or a large segment of an entity's information systems and influence the effectiveness of application controls and other specific controls within an entity's IT environment. General controls help ensure the proper operation of information systems by creating an environment for the appropriate operation of application and user controls. General controls help mitigate information security risks and are designed to help entity management achieve the information security objectives of:

- Confidentiality, thereby preserving authorized restrictions on information access and disclosure.
- Integrity, thereby guarding against improper information modification or destruction.
- Availability, thereby ensuring timely and reliable access and use of information and IT resources.

Network security is one of the most fundamental parts of an entity's IT infrastructure environment, and strong network security controls are vital to protect entity IT resources and data. Malicious cyber actors routinely exploit weak network security controls to compromise an entity's IT systems. Strong network security controls include implementing multi-factor authentication for all network access, restricting administrative level account access, and routinely performing vulnerability scanning, analysis, and remediation. Network security risks are potential vulnerabilities, threats, and weaknesses in the network infrastructure that malicious cyber actors can exploit. Such risks include unauthorized access attempts, malware infections, data breaches, denial of service, and configuration faults in network devices. Our audit evaluated selected network security controls at the Department of Business and Professional Regulation (DBPR), the Department of Health (DOH), and the Fish and Wildlife Conservation Commission (FWCC).

The DBPR was created and organized consistent with State law[1] to license and regulate businesses and professionals operating in the State. The DBPR operates through 11 divisions to carry out the Department's varied responsibilities.

Pursuant to State law,[2] the purpose of the DOH is to protect and promote the health of all residents and visitors in the State through organized State and community efforts, including cooperative agreements with counties. The DOH protects the public health by monitoring diseases, preventing their spread, managing health data, preparing for emergencies, ensuring access to quality care, and regulating both environmental activities and health practitioners to safeguard the public's well-being.

The State Constitution[3] specifies that the FWCC is responsible for exercising regulatory and executive powers of the State with respect to wild animal life, freshwater aquatic life, and marine life. The mission of the FWCC is to manage fish and wildlife resources for their long-term sustainability and the benefit of people.

FINDING AND RECOMMENDATION

Finding 1: Network Security Controls

Network security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain network security controls at the DBPR, the DOH, and the FWCC need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising those agencies' data and IT resources. However, we have notified appropriate DBPR, DOH, and FWCC management of the findings in the areas needing improvement.

Without appropriate network security controls, the risk is increased that the confidentiality, integrity, and availability of DBPR, DOH, and FWCC data and IT resources may be compromised.

Recommendation: We recommend that DBPR, DOH, and FWCC management improve certain network security controls to ensure the confidentiality, integrity, and availability of agency 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 January 2026 through July 2026 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

[1] Section 20.165, Florida Statutes.

[2] Section 20.43, Florida Statutes.

[3] Article IV, Section 9 of the State Constitution.

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 network security controls at the Department of Business and Professional Regulation (DBPR), the Department of Health (DOH), and the Fish and Wildlife Conservation Commission (FWCC) during the period July 2025 through May 2026 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations.
- 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:

- Interviewed DBPR, DOH, and FWCC personnel and reviewed applicable agency laws, rules, policies and procedures, and other guidelines to obtain an understanding of the agencies' organizational structures, statutory requirements, and operational processes.

- Reviewed DBPR, DOH, and FWCC records and obtained an understanding of the agencies' network domain infrastructures, including purpose, users, and access methods.
- Reviewed DBPR, DOH, and FWCC records and obtained an understanding of the agencies' vulnerability management processes.
- Observed, examined, and evaluated the adequacy of DBPR, DOH, and FWCC processes and records related to the agencies' network authentication and security controls.
- Observed, examined records related to, and evaluated the adequacy of DBPR, DOH, and FWCC vulnerability management controls, including the timely performance of authenticated scans and analysis and remediation of identified vulnerabilities. Specifically, we evaluated vulnerability scans performed by the agencies to determine whether vulnerabilities identified as critical or high on the Common Vulnerabilities and Exposures list were timely remediated.
- 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 finding and recommendation included in this report describing the matters requiring corrective actions. Management responses are included in this report under the heading ***MANAGEMENT RESPONSES***.

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

dbpr

Ron DeSantis, Governor
Melanie S. Griffin, Secretary

November 13, 2026

Sherrill F. Norman
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-450

Dear Auditor General Norman,

In accordance with Section 11.45(4)(d), Florida Statutes, I have enclosed our response to the preliminary and tentative audit findings and recommendations included in your Information Technology Network Security Controls review.

We appreciate the time, energy, and dedication put forth by your staff, as well as your continuing efforts to improve the operations of state government.

If you have any questions, please contact Rodney J. MacKinnon, Inspector General, at (850) 717-1576.

Sincerely,

Melanie S. Griffin

Melanie S. Griffin

cc: Sam Kerce, Chief of Staff
Robin Jordan, Acting Chief Information Officer
Rodney MacKinnon, Inspector General

Finding 1: Network security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain network security controls at the DBPR, the DOH, and the FWCC need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising those agencies' data and IT resources. However, we have notified appropriate DBPR, DOH, and FWCC management of the findings in the areas needing improvement.

Without appropriate network security controls, the risk is increased that the confidentiality, integrity, and availability of DBPR, DOH, and FWCC data and IT resources may be compromised.

Finding 1 Response:

DBPR acknowledges the recommendation and remains committed to strengthening network security controls to safeguard the confidentiality, integrity, and availability of agency data and IT resources.

Florida Fish and Wildlife Conservation Commission

Commissioners
Rodney Barreto
Chairman
Coral Gables

Steven Hudson
Vice Chairman
Fort Lauderdale

Preston Farrior
Tampa

Joshua Kellam
Palm Beach Gardens

Gary Lester
Oxford

Albert Maury
Coral Gables

Sonya Rood
St. Augustine

Office of the
Executive Director
Roger A. Young
Executive Director

Charles "Rett" Boyd
Assistant Executive Director

George Warthen
Chief Conservation Officer

Jessica Crawford
Chief of Staff

850-487-3796
850-921-5786 FAX

Managing fish and wildlife resources for their long-term well-being and the benefit of people.

620 South Meridian Street
Tallahassee, Florida
32399-1600
Voice: 850-488-4676

Hearing/speech-impaired:
800-955-8771 (T)
800-955-8770 (V)

MyFWC.com

November 10, 2026

Ms. Sherrill F. Norman, Auditor General
State of Florida Auditor General
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the Florida Fish and Wildlife Conservation Commission (FWC) respectfully submits the enclosed response to the preliminary and tentative audit finding and recommendation identified during the Information Technology Operational Audit of Network Security Controls at FWC. We are committed to addressing the finding and have initiated appropriate corrective actions to strengthen controls and ensure compliance with audit recommendations.

We appreciate the opportunity to review and respond to the audit finding and recommendation. If you have any questions or require additional information, please contact Percy Griffin, Inspector General, at (850) 488-6068.

Sincerely,

Jessica Crawford for

Roger Young
Executive Director

Attachment

cc: Rett Boyd, Assistant Executive Director
Jessica Crawford, Chief of Staff
George Warthen, Chief Conservation Officer
Percy Griffin, Inspector General

Florida Fish and Wildlife Conservation Commission
Response to Preliminary and Tentative Audit Findings
Auditor General IT Operational Audit

Finding 1: Certain network security controls at the DBPR, the DOH, and the FWCC need improvement to ensure the confidentiality, integrity, and availability of agency data and IT resources.

Recommendation: We recommend that DBPR, DOH, and FWCC management improve certain network security controls to ensure the confidentiality, integrity, and availability of agency data and IT resources..

Agency Response: FWCC acknowledges the recommendation and agrees that effective network security controls are essential to safeguarding agency data and information technology resources. FWC is developing a risk-based remediation plan to address the identified areas for improvement and will implement corrective actions in consideration of technical, operational, and resource requirements.

November 12, 2026

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

Dear Ms. Norman:

Enclosed is our response to the preliminary and tentative audit finding and recommendation made during the Office of the Auditor General's audit of *Network Security Controls at Selected State Agencies*, including the Department of Health, as required by section 11.45(4)(d), Florida Statutes.

Please contact Michael J. Bennett, CIA, CGAP, CIG, Inspector General, by calling 850-245-4141, should you have any questions.

Sincerely,

Joseph A. Ladapo, MD, PhD
State Surgeon General

JAL/akm

cc: Shay Gonzalez, BSN, MBA, Interim Chief of Staff
Antonio D. Dawkins, MPA, PMP, Deputy Secretary for Operations
Leonard D. Schoonover, II, Chief Information Officer, Office of Information Technology
Michael J. Bennett, CIA, CGAP, CIG, Inspector General

Florida Department of Health
Office of the State Surgeon General
4052 Bald Cypress Way, Bin A-00 • Tallahassee, FL 32399-1701
PHONE: 850-245-4210
FloridaHealth.gov

PHAB
Accredited Health Department
Public Health Accreditation Board

November 12, 2026

State of Florida
Management's Corrective Action Plan –
Florida Department of Health
For the Information Technology Network Security Controls Audit

Finding:	Certain network security controls at the Department of Business and Professional Regulation (DBPR), the Department of Health (DOH), and the Fish and Wildlife Conservation Commission (FWCC) need improvement to ensure the confidentiality, integrity, and availability of agency data and information technology (IT) resources.
Recommendation:	DBPR, DOH, and FWCC management improve certain network security controls to ensure the confidentiality, integrity, and availability of agency data and IT resources.
Planned Corrective Action:	DOH acknowledges the finding and is taking steps to strengthen network security controls to help ensure the confidentiality, integrity, and availability of agency data and IT resources. As part of this effort, we are reviewing and enhancing existing security practices to ensure they are applied consistently across the affected environments. This includes improving oversight of network configurations, refining access and authentication safeguards, and advancing measures that support more effective monitoring and timely response to potential security risks. We are also implementing process improvements designed to promote standardized governance, clearer accountability, and more reliable tracking of security related activities. These actions will be carried out in coordination with the impacted entities and will align with established statewide and industry security standards. DOH will continue to evaluate the effectiveness of these improvements and make adjustments as needed to maintain a strong and resilient security posture.
Anticipated Completion Date:	December 31, 2027
Responsible Contact Person:	Mark Stich and Michael James

Florida Department of Health
Office of the State Surgeon General
4052 Bald Cypress Way, Bin A-00 • Tallahassee, FL 32399-1701
PHONE: 850-245-4210
FloridaHealth.gov

Accredited Health Department
Public Health Accreditation Board