SOUTHWEST FLORIDA WATER MANAGEMENT DISTRICT

OFFICE OF
INSPECTOR
GENERAL

Cybersecurity Audit

Southwest Florida
Water Management District

Governing Board
September 24, 2024

TABLE OF CONTENTS

Southwest Florida Water Management District

2379 Broad Street, Brooksville, Florida 34604-6899
(352) 796-7211 or 1-800-423-1476 (FL only)
WaterMatters.org

An Equal Opportunity Employer

Bartow Office
170 Century Boulevard
Bartow, Florida 33830-7700
(863) 534-1448 or
1-800-492-7862 (FL only)

Sarasota Office
78 Sarasota Center Boulevard
Sarasota, Florida 34240-9770
(941) 377-3722 or
1-800-320-3503 (FL only)

Tampa Office
7601 U.S. 301 North
Tampa, Florida 33637-6759
(813) 985-7481 or
1-800-836-0797 (FL only)

September 24, 2024

Ms. Michelle Williamson, Chair
Southwest Florida Water Management District
2379 Broad Street
Brooksville, Florida 34604-6899

Dear Ms. Williamson:

In accordance with the Office of Inspector General (OIG) Charter Governing Board Policy and Section 20.055, Florida Statutes, the Inspector General shall conduct audits and prepare audit reports. The cybersecurity audit was conducted for the period of July 2024 through September 2024.

The OIG would like to thank District management and staff for their cooperation and assistance throughout the audit. I respectfully submit to you, the final audit report which presents the results of this audit which was conducted in accordance with Generally Accepted Government Auditing Standards (Yellow Book).

Sincerely,

Brian Werthmiller, CPA, CFE, CIG
Inspector General

cc: Finance/Outreach and Planning Committee
Remaining Members of the Governing Board
Mr. Brian Armstrong, Executive Director
Ms. Sherril Norman, State of Florida Auditor General

SOUTHWEST FLORIDA WATER MANAGEMENT DISTRICT
CYBERSECURITY AUDIT

SUMMARY

This operational audit focused on evaluating selected information technology (IT) controls applicable to IT infrastructure.

Finding 1: Certain District IT security controls related to information security, vulnerability management, and monitoring need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources. The District had a cybersecurity risk assessment completed in August 2023 that noted similar findings.

BACKGROUND

Authorized in 1972, the District protects and manages water resources in a sustainable manner for the continued welfare of the citizens across the 16 counties it serves. The District is one of five water management districts created under the Florida Water Resources Act of 1972[1] and includes all or part of Charlotte, Citrus, Desoto, Hardee, Hernando, Highlands, Hillsborough, Lake, Levy, Manatee, Marion, Pasco, Pinellas, Polk, Sarasota, and Sumter Counties. Governance lies with a thirteen-member Board which consists of representatives from specific geographic areas within District boundaries. Each member is appointed by the Governor and confirmed by the Senate. An Executive Director is appointed by the Board, subject to approval by the Governor and confirmation by the Senate.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls – Information Security, Vulnerability Management, and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of District data and IT resources. Audit procedures disclosed certain security controls related to information security, vulnerability management, and monitoring need improvement. Specific details of the issues in this report are not being disclosed to avoid the possibility of compromising District data and IT resources. However, management has been notified of the findings in these areas needing improvement.

[1] Chapter 373, Florida Statutes.

The District had a cybersecurity risk assessment completed in August 2023 that noted similar findings.

Without appropriate security controls related to information security, vulnerability management, and monitoring, the risk is increased that the confidentiality, integrity, and availability of District data and IT resources may be compromised.

Recommendation: To ensure the confidentiality, integrity, and availability of District IT data and resources, the District should improve IT security controls related to information security, vulnerability management, and monitoring.

PRIOR AUDIT FOLLOW-UP

There are no prior audit findings to follow-up on.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Office of Inspector General (OIG) conducted this operational audit in accordance with *Generally Accepted Government Auditing Standards* (GAGAS). Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objectives. The OIG believes that the evidence obtained provides a reasonable basis for findings and conclusions based on the audit objectives. In addition, the IG is independent per the GAGAS requirements for internal auditors.

This IT operational audit focused on evaluating selected IT controls applicable to IT infrastructure during the period July 2024 through September 2024. For those areas, the objectives of this operational audit were to:

- Evaluate the effectiveness of selected 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; and the safeguarding of IT resources.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those controls.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls significant to the audit objectives; instances of noncompliance with applicable laws, rules, regulations, contracts, and other guidelines; 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 judgement has been used in determining the significance and audit risk and in selecting particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of the audit, the audit work included, but was not limited to, communicating to management the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and related significant controls; identifying and evaluating internal controls significant to the audit objectives; 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; and reporting on the results of the audit as required by Governing Board policy, governing laws, and auditing standards.

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

In conducting the audit for the period of July 2024 through September 2024, the OIG:

- Reviewed applicable statutes, policies, procedures and interviewed District staff to gain an understanding of the District's operations and applicable internal controls and related requirements.
- Evaluated the effectiveness of District policies and procedures relating to certain IT systems, to determine whether internal controls were designed properly and operating effectively.
- Gained an understanding, examined, and evaluated certain IT systems relating to information security, vulnerability management, and monitoring.
- Communicated on an interim basis with applicable officials.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

Brian Werthmiller, CPA, CFE, CIG
Inspector General
2379 Broad Street Brooksville, Florida 34604-6899
Fraud and Compliance Hotline (352) 754-3482

MANAGEMENT'S RESPONSE

Southwest Florida Water Management District

2379 Broad Street, Brooksville, Florida 34604-6899
(352) 796-7211 or 1-800-423-1476 (FL only)
WaterMatters.org

An Equal Opportunity Employer

Bartow Office
170 Century Boulevard
Bartow, Florida 33830-7700
(863) 534-1448 or
1-800-492-7862 (FL only)

Sarasota Office
78 Sarasota Center Boulevard
Sarasota, Florida 34240-9770
(941) 377-3722 or
1-800-320-3503 (FL only)

Tampa Office
7601 U.S. 301 North
Tampa, Florida 33637-6759
(813) 985-7481 or
1-800-836-0797 (FL only)

September 23, 2024

Mr. Brian Werthmiller, C.P.A., C.I.G.
Inspector General
Southwest Florida Water Management District
2379 Broad Street
Brooksville, Florida 34604

Subject: Inspector General Audit Report – Cybersecurity Audit

Dear Mr. Werthmiller:

Thank you for taking the time to complete the Cybersecurity Audit. We are in receipt of the results of the audit, which focuses on evaluating selected information technology (IT) controls applicable to IT infrastructure.

We have finalized our review of the findings and recommendations. Please find our responses listed below.

Finding 1: Certain District IT security controls related to information security, vulnerability management, and monitoring need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources. The District had a cybersecurity risk assessment completed in August 2023 that noted similar findings.

Response: The Information Technology Bureau agrees that it will continue improving IT security controls around information security, vulnerability management, and monitoring as a part of the ongoing efforts to improve the District's cybersecurity posture and increasingly aligning to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Thank you for your services and recommendations

Sincerely,

Brian J. Armstrong, P.G.
Executive Director

BJA:tfh
cc: Amanda Rice
Brandon Baldwin