

OFFICE OF
INSPECTOR
GENERAL

IT Access Privileges Follow-Up Audit

September 30, 2019 to February 28, 2020

TABLE OF CONTENTS

	<u>Page No.</u>
LETTER TO THE BOARD.....	1
SUMMARY	2
BACKGROUND	2
FINDINGS AND RECOMMENDATIONS	3
PRIOR AUDIT FOLLOW-UP	3
OBJECTIVES, SCOPE, AND METHODOLOGY.....	3



An Equal Opportunity Employer

Southwest Florida Water Management District

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

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 (Fort King Highway)
Tampa, Florida 33637-6759
(813) 985-7481 or
1-800-836-0797 (FL only)

- Mark Taylor**
Chair, Hernando, Marion
- Michelle Williamson**
Vice Chair, Hillsborough
- Joel Schielcher**
Secretary, Charlotte, Sarasota
- Kelly S. Rice**
Treasurer, Citrus, Lake, Levy, Sumter
- Jack Blapham**
Manatee
- Roger Germann**
Hillsborough
- James G. Murphy**
Polk
- Rebecca Smith**
Hillsborough, Pinellas
- Seth Weigman**
Pasco
- Brian J. Armstrong, P.C.**
Executive Director

April 28, 2020

Mr. Mark Taylor, Chair
Southwest Florida Water Management District
2379 Broad Street
Brooksville, Florida 34604-6899

Dear Mr. Taylor:

In accordance with F.S. 20.055 and the Office of Inspector General (OIG) Charter Governing Board Policy, the Inspector General (IG) shall monitor the implementation of the District's response to any audit issued by the Auditor General (AG).

On July 9, 2018, the AG released report No. 2019-001 on the operational audit of the Southwest Florida Water Management District (District). Included in this report was a finding regarding IT access privileges. The AG recommended the District should ensure that assigned access privileges restrict employees to only those functions necessary for their assigned job responsibilities and enforce an appropriate separation of incompatible duties. To help monitor assigned access privileges, the District should establish procedures to periodically review the appropriateness of such privileges to ensure that employees do not access IT resources and functions that are incompatible with their assigned job responsibilities. In addition, if an employee only requires occasional access to perform back-up duties, the access should be granted only for the time needed.

In accordance with the Audit Plan, approved by the Governing Board, a follow-up audit on IT access privileges was performed and the OIG has concluded the District has taken corrective actions. The OIG would like to thank the Management Services Director, Employee and External Relations Director, and their staff for their cooperation and assistance throughout the audit. I respectfully submit to you, the final audit report which was conducted in accordance with *Generally Accepted Government Auditing Standards*.

Sincerely,

Brian Werthmiller, CPA, CIG
Inspector General

- cc: Finance/Outreach and Planning Committee
- Remaining Members of the Governing Board
- Mr. Brian Armstrong, Executive Director
- Ms. Mandi Rice, Assistant Executive Director
- Mr. John Campbell, Management Services Director
- Mr. Michael Molligan, Employee and External Relations Director
- Ms. Sherril Norman, State of Florida Auditor General
- Mr. James Halleran, James Moore & Company CPA's Legislative Auditing Committee

SOUTHWEST FLORIDA WATER MANAGEMENT DISTRICT IT ACCESS PRIVILEGES FOLLOW-UP AUDIT

SUMMARY

This is a follow-up audit to the IT access privileges finding from the AG Report No. 2019-001 released July 2018 for the District. The AG recommended the District should ensure that assigned access privileges restrict employees to only those functions necessary for their assigned job responsibilities and enforce an appropriate separation of incompatible duties. To help monitor assigned access privileges, the District should establish procedures to periodically review the appropriateness of such privileges to ensure that employees do not access IT resources and functions that are incompatible with their assigned job responsibilities. In addition, if an employee only requires occasional access to perform back-up duties, the access should be granted only for the time needed. The OIG follow-up audit disclosed the District has taken corrective actions.

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 1972¹ 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.

District Governing Documents² require, on an annual basis, a review of access privileges in the financial, human resources, and payroll systems. The District uses CGI Skyward to process and report its finance transactions and UltiPro to process and report its human resources and payroll transactions. Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, creation, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, change, add, or delete data.

¹ Chapter 373, Florida Statutes.

² Governing Document – Least Privilege

FINDINGS AND RECOMMENDATIONS

This report contains no findings or recommendations.

PRIOR AUDIT FOLLOW-UP

Based upon the objectives, scope, and methodology as documented below, the District has taken corrective actions for the IT access privileges finding per the AG in Report No. 2019-001.

OBJECTIVES, SCOPE, AND METHODOLOGY

The OIG conducted this follow-up audit for the period of September 30, 2019 to February 28, 2020 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.

The objectives of this operational audit were to:

- Evaluate management's performance in establishing and maintaining internal controls in accordance with applicable statutes, laws, rules, regulations, contracts, grant agreements, and other guidelines.
- 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, the safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective action for, or was in the process of correcting, the AG's IT access privileges finding from report No. 2019-001.

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

Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

In conducting the audit for the period of September 30, 2019 to February 28, 2020, the OIG:

- Reviewed applicable statutes, policies, procedures and interviewed District staff to gain an understanding of the District's operations and internal controls over IT access privileges.
- Gained an understanding of the information systems for the CGI Advantage and UltiPro applications.
- Evaluated the effectiveness of District policies and procedures relating to IT access privileges, to determine whether internal controls were designed properly and operating effectively.
- Examined the District's periodic reviews of access privileges assigned within the CGI Advantage and UltiPro applications.
- Reviewed user access privileges assigned within the CGI Advantage and UltiPro applications to determine whether any employees who had separated from the District had access as of September 30, 2019.
- Reviewed District procedures for maintaining and reviewing employee access to IT data and resources. Examined access privileges to selected critical functions for 30 employees who had access to the CGI Advantage and UltiPro applications as of September 30, 2019 to determine the appropriateness and necessity of the access based on the employees' job duties and user account functions and whether the access prevented the performance of incompatible duties. Also, examined mitigating controls in place to determine the appropriateness of access.
- 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, CIG
Inspector General

2379 Broad Street Brooksville, Florida 34604-6899

Phone: (352) 796-7211 X4100 ♦ Fraud and Compliance Hotline (352) 754-3482