Florida Fish and Wildlife Conservation Commission
Office of Inspector General

Advisory Memorandum
IA-1911 AG 2019-209 Information Technolgy Operational Audit Follow-up
March 6, 2019

Executive Summary

The purpose of this memorandum is to report the progress and status of the Florida Fish and Wildlife Conservation Commission's (FWC/Agency/Commission) efforts to complete action items established to address issues identified in the State of Florida Auditor General's (AG) Operational Audit Report Number 2019-009.

Based on the results of our follow-up review, we determined that FWC's Office of Information Technology (OIT) management is in the process of taking actions to address the issues identified in the Auditor General's report. A Legislative Budget Request (LBR) has been forwarded for fiscal year (FY) 2019-2020 budget; OIT is also updating policies and procedures to address the security issues.

The FWC's Office of Inspector General (OIG) will conduct an additional follow-up review in six months.

Introduction and Background

In August of 2018, the Auditor General issued Information Technology Operational Audit Report Number 2019-009 regarding the Agency's information technology (IT) general controls. The AG report contained six findings and recommendations for strengthening and improving Agency controls.

Specifically, the AG's audit determined the following:

- The Commission had not established IT security policies and procedures to protect and manage IT boundaries and data communications;
- The Commission had not established procedures for comprehensive periodic access reviews and the access reviews performed were not documented;
- The Commission did not timely disable the network access privileges for some employees who separated from Commission employment;
- Commission backup policies and procedures need improvement;
- The Commission's computer security incident response policies and procedures need improvement to promote prompt and appropriate responses to cybersecurity events;
- Certain security controls related to logical access, user authentication, logging and monitoring, vulnerability management, configuration management, and network security settings need improvement to ensure the confidentiality, integrity, and availability of Commission data and IT resources.

Results of Follow-up Review

The following tables contain the AG findings, recommendations, and the FWC management's initial response/corrective action plans relating to the AG's operational audit [2019-009] In addition, the tables contain a status section detailing the current disposition of the findings and recommendations.

AG Finding Number	**1- IT Security Policies and Procedures**
AG Finding	The Commission had not established IT security policies and procedures to protect and manage IT boundaries and data communications.
AG Recommendation (R1)	We recommend that Commission management establish and implement IT security policies and procedures for protecting and managing IT boundaries and data communications, including managing the firewalls and e-mail security.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. We are currently updating our policies and procedures to address these issues. Specifically, OIT has begun work to revise our policies and procedures addressing patching to ensure the scope of the policy covers all areas of the IT boundaries and data communications. Additionally, a new OIT policy and procedure is being created to address email security.
Status	**Open:** Per OIT management, the IT policies and procedures are still being developed. **Anticipated Completion Date:** May 2019

AG Finding Number	**2 - Periodic Review of Access Privileges**
AG Finding	The Commission had not established procedures for comprehensive periodic access reviews and the access reviews performed were not documented.

AG Recommendation (R2)	We recommend that Commission management establish and implement procedures for conducting comprehensive periodic reviews of all user access privileges, including accounts with elevated access privileges, and retain documentation of the reviews conducted.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. OIT is currently developing policies and procedures to address these user access privilege issues. The policy will include a requirement for a documented, comprehensive periodic review of system user privileges, with a focus on accounts with elevated risks or requirements. The policy will also include definitions for elevated privileges, the focus of the review, frequency of the review, and any required documentation.
Status	**Open:** According to OIT management, the IT policies and procedures are still being developed. **Anticipated Completion Date:** June 2019

AG Finding Number	**3 - Timely Disabled Network User Accounts**
AG Finding	The Commission did not timely disable the network access privileges for some employees who separated from Commission employment.
AG Recommendation (R3)	We recommend that Commission management ensure that network user accounts are timely disabled upon an employee's separation from Commission employment. To demonstrate that the user accounts were timely disabled, Commission management should ensure that required forms are completed and retained.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. In conjunction with the FWC's Office of Human Resources (HR), we will continue to improve the process for the timely removal of user accounts due to the departure of an employee from the Agency. While recognizing there are limits to the automation of the process, staff will be provided with appropriate training and written procedures to improve the logging and retention of documentation required for this process.

Status	**Open:** Per OIT management, HR will provide messaging to supervisors as to the importance of timely account disabling. The FWC Employee Separation Checklist will be updated to indicate timely requirement of submission of form of account disabling and termination. An annual self-audit will be performed by OIT for review by management on timeliness of account disabling. The procedure and process changes are being modified. **Anticipated Completion Date:** June 2019

AG Finding Number	**4 - Backup Controls**
AG Finding	Commission backup policies and procedures need improvement.
AG Recommendation (R4)	We recommend that Commission management establish policies and procedures and related controls governing the backup process. Additionally, we recommend that the Commission store the weekly backup tapes at an off-site location and maintain records of the movement of the monthly backup tapes.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. These issues deal with the backup processes and procedures at the FWC's Fish and Wildlife Research Institute (FWRI) facility in St. Petersburg, Florida. We are in the process of implementing a new process that will mostly eliminate the need for the use of tapes. Under the new system, data will be replicated offsite. This new process will be documented; where any tapes are required to be moved offsite, that process will be reevaluated and improved to ensure proper documentation and logging.
Status	**Open:** According to OIT management, new data replication backup system at FWRI is nearing implementation. The new process will terminate the need for tapes to be stored offsite, except for annual backups. A SharePoint process will be implemented to track the annual tape shipment and storage. **Anticipated Completion Date:** June 2019

AG Finding Number	**5 - Computer Security Incident Response**
AG Finding	The Commission's computer security incident response policies and procedures need improvement to promote prompt and appropriate responses to cybersecurity events.
AG Recommendation (R5)	We recommend that Commission management ensure Computer Security Incident Response Team (CSIRT) member training is conducted on an annual basis, revise the Computer Security Incident Reporting and Response Policy to comply with the Florida Agency for State Technology (AST) computer security incident reporting requirements, and ensure that all computer security incidents are timely reported to the AST. Additionally, we recommend that the Commission utilize the response checklist when responding to all computer security incidents involving a virus or malware.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. The policy for the CSIRT process will be updated to comply with the Florida Administrative Code (F.A.C.) Chapter 74-2, Information Technology Security and Florida Statutes (F.S.) Chapter 282, Communications and Data Processing. Additionally, quarterly meetings of the CSIRT will include required annual training. With the changes to the policy and improvements being made to the incident reporting portal by AST, we will be able to improve the timeliness of the security incident reports. The team will also work to improve incident management and documentation.
Status	**Open:** Per OIT management, an updated Agency policy, Internal Management Policies and Procedures (IMPP) 3.8, Computer Security Incident Reporting and Response Policy has been drafted and is being reviewed. It will be submitted to FWC management for approval. The draft will reflect changes to AST rule 74-2 F.A.C. and Chapter 282 F.S. since it was first implemented. All other issues with CSIRT process have been addressed. **Anticipated Completion Date:** April 2019

AG Finding Number	**6 - Security Controls – Logical Access, User Authentication, Logging and Monitoring, Vulnerability Management, Configuration Management, and Network Security Settings**
AG Finding	Certain security controls related to logical access, user authentication, logging and monitoring, vulnerability management, configuration management, and network security settings need improvement to ensure the confidentiality, integrity, and availability of Commission data and IT resources.
AG Recommendation (R6)	We recommend that Commission management improve certain security controls related to logical access, user authentication, logging and monitoring, vulnerability management, configuration management, and network security settings to ensure the confidentiality, integrity, and availability of Commission data and other Commission IT resources.
FWC Initial Response and Corrective Action Plan	The Commission concurs with the finding. A Legislative Budget Request is being processed to improve our ability to identify and monitor these vulnerabilities. The LBR will include the acquisition of a Security Event Information Management (SEIM) system. At the end of fiscal year 2017-2018, we also acquired a tool to allow longer retention of systems logs, which will address several findings.
Status	**Open:** Per OIT management, the LBR is pending Legislature approval. **Anticipated Completion Date:** October 2019

Attachment One – Purpose, Scope, and Methodology

Section 20.055, Florida Statutes, requires the OIG to conduct audits, investigations and management reviews related to programs and operations of the Commission. This review was performed as part of the OIG's mission to promote accountability, integrity, and efficiency in government.

The **purpose** of this review was to monitor the disposition of recommendations communicated to functional management in the AG engagement number 2019-009, Information Technology General Controls.

Our **scope** included a review of the audit findings, recommendations, and status of corrective actions associated with the AG engagement number 2019-009, Information Technology General Controls.

To achieve our purpose, we used the following **methodology**:

- Reviewed findings, corrective actions, and recommendations from AG engagement number 2019-009, Information Technology General Controls;
- Reviewed applicable agency policies, procedures, and processes;
- Interviewed appropriate Agency personnel; and
- Reviewed other applicable documentation.

Attachment Two – Final Report Addressee and Distribution List

Addressee:
Eric Sutton, FWC Executive Director

Distribution List:
Thomas Eason, FWC Assistant Executive Director
Jennifer Fitzwater, FWC Chief of Staff
Glenda Atkinson, Chief Information Officer
Sherrill Norman, CPA, Florida Auditor General
Melinda Miguel, Florida Chief Inspector General

Attachment Three – Review Team and Statement of Accordance

This audit follow-up was conducted under the authority of Section 20.055, F.S. and in conformance with the International Standards for the Professional Practice of Internal Auditing published by the Institute of Internal Auditors as well as applicable Principals and Standards for Offices of Inspector General published by the Association of Inspectors General. This audit follow-up was conducted by the FWC OIG's Internal Auditor Donna Whittle, CIGA, FCCM and was supervised and directed by the FWC's Inspector General Mike Troelstrup, CIG, CIGI. Please address inquiries regarding this report to the Inspector General (Mike.Troelstrup@MyFWC.com).

Requests for copies of the final report may be made to FWC's Inspector General Mike Troelstrup, CIG, CIGI by email to Mike.Troelstrup@MyFWC.com, by telephone (850-488-6068), by FAX (850-488-6414), in person, or by mail at 620 South Meridian Street, Tallahassee, FL 32399.