Florida Fish and Wildlife Conservation Commission
Office of Inspector General

Advisory Memorandum
IA-1806 AG OIT Operational Audit Follow-Up
February 27, 2018

Executive Summary

The purpose of this memorandum is to report on the progress and status of Agency efforts to complete action items identified in Auditor General (AG) Operational Audit Number 2017-201, Mobile Device Security Controls.

Based on the results of our follow-up review, we determined that management is in process of taking actions to address the issues identified in the Auditor General's report. A Legislative Budget Request (LBR) has been forwarded for the Fiscal Year 2018-19 budget covering security issues. Once approved, the issues presented in the audit will be addressed and resolved.

Introduction and Background

The Auditor General's audit addressed Mobile Device Security Controls at three agencies namely, The Department of Legal Affairs, the Department of Veteran's Affairs, and the Fish and Wildlife Conservation Commission (FWCC). This follow-up addresses those issues that are specific to the Commission, and excludes the names of the other agencies jointly mentioned in the Auditor General findings and recommendations. Additionally, their findings are presented with the descriptive detail specified in the body of the report rather than the abbreviated descriptions provided in their summary section.

Finding 1 - Impact Analysis. FWCC lacked documentation evidencing that an impact analysis was conducted prior to allowing both agency-owned and personally owned mobile devices to access agency data and IT resources.

Finding 2 - Mobile Device Policies and Procedures. Policies and procedures for personally owned mobile devices were not sufficiently detailed to address specific security requirements such as device encryption, user patching requirements, passcode requirements, and minimum operating systems. The FWCC did not have policies and procedures in place that specified the minimum operating requirements for FWCC owned smartphones.

Finding 3 - Mobile Device Agreements. Procedures do not address the specific responsibilities of the FWCC or the employees regarding personally owned mobile devices. The FWCC did not use a mobile device agreement form or other related documentation for personally owned mobile devices that specified the responsibilities of the FWCC and the user when personally owned mobile devices are used to connect to the FWCC's network and IT resources.

Finding 4 – Mobile Device Management.
The FWCC did not maintain a complete inventory of personally owned mobile devices authorized to connect to FWCC's environment thereby limiting user provisioning, the prevention and detection of unauthorized mobile device access to the network, and incident response in the event of a lost or stolen mobile device.

Operating system updates, the use of passcodes, and encryption of mobile device data were not enforced for both FWCC-owned smartphones, FWCC-owned non-Windows tablets, and all personally owned mobile devices.

The ability to remotely wipe lost or stolen FWCC-owned and personally owned mobile devices did not exist as of October 28, 2016.

Results of Follow-up Review

The following tables contain findings, recommendations, and management's initial response/corrective action plans relating to the Auditor General Report No. 2017-201. In addition, the tables contain a status section which presents the current disposition of the Auditor General's findings and recommendations.

Finding Number	1
Finding	**Impact Analysis**. FWCC lacked documentation evidencing that an impact analysis was conducted prior to allowing both agency-owned and personally owned mobile devices to access agency data and IT resources.
Recommendation	We recommend that FWCC management assess the impact of allowing mobile devices to access agency IT environments, and identify and design required IT security controls to protect the confidentiality, availability, and integrity of agency data and IT resources.
FWC Initial Response and Corrective Action Plan	The FWC will conduct and document an impact analysis as recommended. Anticipated completion date: September 2017.
Status	**Open:** We reviewed industry standards and developed a comprehensive security plan. We have sought internal approval and submitted a Legislative Budget Request to obtain funding for mobile device software to manage our Mobile Device Management (MDM) environment resulting from this plan. The software will enforce that plan and address the issues in this Auditor General's finding. We will then design our impact analysis. The latest information available shows this LBR is part of both the House and Senate budgets as they head to conference. The LBR represents our assessment of the most beneficial, thorough, and comprehensive solution to address the audit findings. If funding does not materialize, we will attempt to apply alternate possibilities. Anticipated Completion Date: November 30, 2018

Finding Number	2
Finding	**Mobile Device Policies and Procedures**. Policies and procedures for personally owned mobile devices were not sufficiently detailed to address specific security requirements such as device encryption, user patching requirements, passcode requirements, and minimum operating systems. The FWCC did not have policies and procedures in place that specified the minimum operating requirements for FWCC owned smartphones.
Recommendation	To better protect the confidentiality, integrity, and availability of agency data and IT resources, we recommend that management enhance IT security policies and procedures for mobile devices**.**
FWC Initial Response and Corrective Action Plan	The FWC will continue the process of enhancing IT security policies and procedures for mobile devices. A formal agency policy for mobile device use and management is currently being created and is expected to be completed by September 2017.
Status	**Open:** We reviewed industry standards and developed a comprehensive security plan. We have sought internal approval and submitted a Legislative Budget Request to obtain funding for mobile device software to manage our Mobile Device Management (MDM) environment. The software will enforce that plan and address the security issues in the Auditor General's finding. The latest information available shows this LBR is part of both the House and Senate budgets as they head to conference. Once we have funding approval, we will move forward with evaluating and choosing a product that will meet our requirements and develop an impact analysis. We have had meetings to discuss the overall MDM and security and should begin software/vendor evaluations this month. The LBR represents our assessment of the most beneficial, thorough, and comprehensive solution to address the audit findings. If funding does not materialize, we will attempt to apply alternate possibilities. Anticipated Completion Date: November 30, 2018

Finding Number	**3**
Finding	**Mobile Device Agreements.** Procedures do not address the specific responsibilities of the FWCC or the employees regarding personally owned mobile devices. The FWCC did not use a mobile device agreement form or other related documentation for personally owned mobile devices that specified the responsibilities of the FWCC and the user when personally owned mobile devices are used to connect to the FWCC's network and IT resources.
Recommendation	We recommend that FWCC management improve controls to ensure that all users are informed of the security risks and document acknowledgement of their responsibilities prior to accessing agency data and IT resources remotely.
FWC Initial Response and Corrective Action Plan	The FWC will develop and enhance communication, training, and information process for all mobile device users, and document user acknowledgement of their responsibilities. Anticipated completion date is September 2017.
Status	**Partially Complete:** Procedures now address the responsibilities of the FWC employees. A mobile device agreement form is in draft stage. It awaits final approval and implementation Anticipated Completion Date: March 31, 2018
Finding Number	**4**
Finding	**Mobile Device Management**. The FWCC did not maintain a complete inventory of personally owned mobile devices authorized to connect to FWCC's environment thereby limiting user provisioning, the prevention and detection of unauthorized mobile device access to the network, and incident response in the event of a lost or stolen mobile device. Operating system updates, the use of passcodes, and encryption of mobile device data were not enforced for both FWCC-owned smartphones, FWCC-owned non-Windows tablets, and all personally owned mobile devices.

	The ability to remotely wipe lost or stolen FWCC-owned and personally owned mobile devices did not exist as of October 28, 2016.
Recommendation	We recommend that FWCC management improve security controls that correspond to the complexity of the related mobile device environment to ensure the complete inventory of mobile devices authorized to connect to an agency's environment is maintained, the performance of required operating system updates for mobile devices, the enforcement of authentication requirements including passcodes before accessing the agency's resources, the encryption of mobile device data, the ability to remotely wipe data from lost or stolen mobile devices, and the restriction of unnecessary storing of confidential or exempt data locally on personally owned mobile devices.
FWC Initial Response and Corrective Action Plan	The FWC will evaluate tools that will assist in setting the proper controls, as described, for the resulting environment. The selection and implementation of these tools and services will occur during Fiscal Year 2017-18.
Status	**Open**: We have sought internal approval and submitted a Legislative Budget Request to obtain funding for mobile device software to manage our Mobile Device Management (MDM) environment. We will be evaluating various software solutions so that we will have this portion of the business completed prior to funding. This software will allow for inventory of mobile devices, minimum operating systems, minimum operating system requirements for FWCC owned smartphones, passcode requirements, patching requirements, device encryption, and the ability to wipe data from lost or stolen mobile devices etc. The LBR represents our assessment of the most beneficial, thorough, and comprehensive solution to address the audit findings. If funding does not materialize, we will attempt to apply alternate possibilities. Anticipated Completion Date: November 30, 2018

Attachment One – Purpose, Scope, and Methodology

Section 20.055, Florida Statutes, requires the FWC OIG to conduct audits, investigations and management reviews related to programs and operations of the Commission. This review was performed as part of the FWC 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 resulting from AG operational audit number 2017-201, Mobile Device Security Controls.

Our **scope** included a review of the audit findings, recommendations, and status of corrective actions associated with AG engagement number 2017-201, Mobile Device Security Controls.

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

- Reviewed findings, corrective actions, and recommendations from AG engagement number 2017-201, Mobile Device Security 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
Ignacio Sanchez, Chief Information Officer
Sherrill Norman, CPA, Auditor General
Eric Miller, Chief Inspector General

Attachment Three – Review Team and Statement of Accordance

This review 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 Internal Auditor, Charles Mohamete and was supervised and directed by the Director of Auditing, Susan Horn, CPA, MBA, CFE. Please address inquiries regarding this report to the Director of Auditing (Susan.Horn@MyFWC.com).

Requests for copies of the final report may be made 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.