Department of Legal Affairs
Office of the Attorney General
Office of Inspector General

Follow-up to Auditor General Department of Legal Affairs, Department of Veterans' Affairs, and Fish and Wildlife Conservation Commission Mobile Device Security Controls Report No. 2017-201 OIG Audit Report #2017-09

Final Audit Report **October 20, 2017** **Assignment No. 2017-09**

Purpose

This follow-up report advises the Attorney General, the Auditor General, the Office of Program Policy Analysis and Government Accountability, and the Joint Legislative Auditing Committee of the status of corrective actions related to findings reported by the Auditor General Department of Legal Affairs (DLA), Department of Veteran's Affairs, and Fish and Wildlife Conservation Commission Mobile Device Security Controls Report No. 2017-201 dated April 2017.

Standards

Our work was performed in accordance with the *International Standards for the Professional Practice of Internal Auditing* as published by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope

The scope of this review was to determine the current status of corrective actions and/or management decisions related to the findings reported in the report mentioned above as of October 2017.

Background

The Auditor General's previous operational audit focused on evaluating selected Department of Legal Affairs (DLA), Department of Veterans' Affairs (DVA), and Fish and Wildlife Conservation Commission (FWCC) information technology (IT) controls applicable to managing and securing mobile devices connected to the agencies' networks or used to store confidential and sensitive agency data.

Methodology

As a part of this assignment, Office of Inspector General staff:

- Requested staff to assess current status of implementation of recommendations from the previous report; and
- Reviewed documents and made observations necessary to corroborate their assertions relating to the status of

audit findings reported in the previous report.

Conclusion: The status of the implementation of the recommendations is as follows:

1. Implemented
2. Not yet implemented
3. Implemented
4. Not yet implemented

The recommendations and previous audit responses are explained in greater detail as follows.

Finding Number One: Impact Analysis

The DLA, DVA, and FWCC lacked documentation that an impact analysis had been conducted prior to allowing the use of agency-owned and personally owned mobile devices in each respective agency's IT environment.

Recommendation One: We recommend that DLA, DVA, and 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.

DLA Management's Prior Response:

A Business Impact Analysis has been undertaken and a Statement will be available within 30 days.

DLA Management's Current Status (October 2017):

A Business Impact Analysis was prepared dated as of January 2017.

Auditor's Conclusion:
Implemented.

Finding Number Two: Mobile Device Policies and Procedures

DLA and FWCC security policies and procedures for mobile devices need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

Recommendation Two: To better protect the confidentiality, integrity, and availability of agency data and IT resources, we recommend that DLA and FWCC management enhance IT security policies and procedures for mobile devices.

DLA Management's Prior Response:
Policy revision is already underway as noted in the P&T and we anticipate the revisions needed in accordance with recommendations will be completed within 90 days.

DLA Management's Current Status (October 2017):

Policy revision began with a preliminary gap analysis. This indicated the scope of revisions needed had been significantly underestimated and management subsequently allocated a full-time position to assume the duties of the ISM including policy revisions. Due to the total overhaul required by additional regulatory and threat mitigation activities the projected completion of policy revisions is February 2018.

Auditor's Conclusion:
Not yet implemented.

Finding 3: Mobile Device Agreements
Controls related to mobile device agreements at the DLA, DVA, and FWCC need improvement to ensure that the agency and user responsibilities for personally owned mobile devices used to connect to the agency's network and IT resources are appropriately documented.

Recommendation 3: We recommend that DLA, DVA, and 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.

DLA Management's Prior Response:
We are in the process of revising the mobile device agreement which will be sent to all Citrix users for signature. We anticipate this will be completed within 60 days.

DLA Management's Current Status (October 2017):

All Citrix users must acknowledge a Terms and Conditions agreement before proceeding with logging into the Citrix portal.

Auditor's Conclusion: implemented.

Finding 4: Mobile Device Management
DLA and FWCC security controls for the management and administration of mobile devices need improvement to correspond to the complexity of the related mobile device environment.[1]

Recommendation No. Four: We recommend that DLA and 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.

DLA Management's Prior Response:
There are administrative controls in place in the form of policies, addressing some of the identified risks, that users must review and sign annually. If these controls are followed they help to mitigate the risks under discussion. While DLA has the capability of remotely wiping some DLA managed mobile devices using IBM Traveler, DLA is moving to a MDM solution in conjunction with enterprise and email modernization currently underway and will be operating in accordance with the recommendations within 6 months.

DLA Management's Current Status (October 2017):
The implementation of Outlook/Exchange was delayed due to circumstances outside IT control. Consequently, the projected start date of implementing Enterprise Mobility Security has been changed to 1/18.

Auditor's Conclusion: not yet implemented.

[1] Department of Legal Affairs, Department of Veterans' Affairs, and Fish and Wildlife

Inspector General's Statement

This engagement was conducted pursuant to Section 20.055, F.S. in accordance with *The International Standards for the Professional Practice of Internal Auditing*. This engagement was conducted by Judy Goodman, CPA, CIA, Director of Auditing.

The Office of Inspector General would like to thank management and staff for their assistance and cooperation extended to us during our audit.

Sincerely,

Steve Rumph
Inspector General