

**DEPARTMENT OF LEGAL AFFAIRS,  
DEPARTMENT OF VETERANS' AFFAIRS,  
AND  
FISH AND WILDLIFE CONSERVATION  
COMMISSION**

Mobile Device Security Controls



Sherrill F. Norman, CPA  
Auditor General

## State Agency Heads and Commissioners

The Florida Statutes establish the various State agencies and provide the title and selection process for the head of each State agency. The table below shows the three State agencies included in the scope of this information technology operational audit and the respective agency heads and commissioners, as applicable, who served during the period of our audit.

State Agency	Established by Florida Statutes	Agency Heads and Commissioners
Department of Legal Affairs	Section 20.11	Pam Bondi, Attorney General
Department of Veterans' Affairs	Section 20.37	Glenn Sutphin, Executive Director
Fish and Wildlife Conservation Commission	Section 20.331 and Article IV, Section 9 of the State Constitution	Nick Wiley, Executive Director Brian Yablonski, Chair Ronald M. Bergeron, Commissioner Richard Hanas, Commissioner Aliese P. "Liesa" Priddy, Commissioner Bo Rivard, Commissioner Charles W. Roberts III, Commissioner Robert A. Spottswood, Commissioner

The team leader was Jimmy Chien and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at [arthart@aud.state.fl.us](mailto:arthart@aud.state.fl.us) or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

[www.myflorida.com/audgen](http://www.myflorida.com/audgen)

Printed copies of our reports may be requested by contacting us at:

**State of Florida Auditor General**

**Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722**

**DEPARTMENT OF LEGAL AFFAIRS,  
DEPARTMENT OF VETERANS' AFFAIRS, AND  
FISH AND WILDLIFE CONSERVATION COMMISSION**

**Mobile Device Security Controls**

## ***SUMMARY***

---

This 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. Our audit disclosed the following:

**Finding 1:** 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.

**Finding 2:** 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.

**Finding 3:** 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.

**Finding 4:** 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.

## ***BACKGROUND***

---

Mobile devices<sup>1</sup> have become an integral part of the information technology (IT) infrastructure. Mobile devices may be owned by the employing entity or personally owned by the employee. Some entities permit the use of personally owned or *bring your own device* (BYOD) to conduct work-related tasks. Mobile devices, unlike traditional desktop computing configurations, are typically not physically connected to an entity's computing environment or network and can be used from any place in the world to connect to an entity's computing environment over the publicly accessible Internet. Convenience and availability are the major advantages of using mobile devices; however, these attributes also present additional risks to an entity.<sup>2</sup> Specifically, the use of mobile devices increases the risk of:

- Information interception, resulting in a breach of sensitive data, enterprise reputation, adherence to regulation, and legal action.
- Malware propagation, which may result in data leakage, data corruption, and unavailability of necessary data.

---

<sup>1</sup> Mobile devices are portable devices, such as laptops, smartphones, and tablets, that allow storage and transmittal of entity data.

<sup>2</sup> *Mobile Computing Security Audit/Assurance Program*, ISACA (formerly known as the Information Systems Audit and Control Association), 2010.

- Device corruption, lost data, call interception, and possible exposure of sensitive information.
- Lost devices or unauthorized access to unsecured devices allowing exposure of sensitive data, resulting in damage to the enterprise, customers, or employees.

Given these risks, the National Institute of Standards and Technology (NIST) recommends that entities establish a mobile device security policy that describes, among other things, how the entity will manage the configuration and security of each mobile device before allowing a mobile device to access entity data and IT resources.<sup>3</sup> An impact analysis should be conducted prior to allowing the use of mobile devices and entities should implement a standard security awareness training program regarding mobile devices, which should clearly define the expectations of both the user and the entity.

We included three State agencies (Department of Legal Affairs, Department of Veterans' Affairs, and Fish and Wildlife Conservation Commission) in the scope of this IT operational audit. Each of the three agencies has unique responsibilities and policies and procedures related to the use of agency-owned and personally owned mobile devices.

### **Department of Legal Affairs**

State law<sup>4</sup> specifies that the Department of Legal Affairs (DLA) is responsible for providing all legal services required by State agencies, unless otherwise provided by law. The DLA's other statutory responsibilities include enforcing State consumer protection, antitrust, and civil rights laws; prosecuting criminal racketeering; operating the State's Medicaid Fraud Control Unit; and administering programs to assist victims of crime.

During the period September through December 2016, the DLA allowed employees to access the DLA network and e-mail using both DLA-owned and personally owned mobile devices.

### **Department of Veterans' Affairs**

The Department of Veterans' Affairs (DVA) assists all former, present, and future members of the Armed Forces of the United States and their dependents in preparing claims for and securing such compensation, hospitalization, career training, and other benefits or privileges to which such persons are, or may become, entitled to under Federal or State law or regulation by reason of their service in the Armed Forces of the United States.<sup>5</sup>

During the period September through December 2016, DVA policies allowed employees to access the DVA network and e-mail using both DVA-owned and personally owned mobile devices. DVA-owned mobile devices consist of laptops and smartphones. DVA-owned laptops may access both the network and e-mail, whereas DVA-owned smartphones only have access to e-mail. Although personally owned mobile devices are permitted at the DVA, during the period September through December 2016, no employees were using personally owned mobile devices to access the DVA network and e-mail.

---

<sup>3</sup> NIST Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013.

<sup>4</sup> Section 16.015, Florida Statutes.

<sup>5</sup> Section 292.05(1), Florida Statutes.

## **Fish and Wildlife Conservation Commission**

The State Constitution<sup>6</sup> specifies that the Fish and Wildlife Conservation Commission (FWCC) is responsible for exercising regulatory and executive powers with respect to wild animal life, freshwater aquatic life, and marine life in order to ensure the long-term sustainability of fish and wildlife resources. The responsibilities of the FWCC include law enforcement to protect fish and wildlife, keeping waterways safe for boaters, and cooperating with other law enforcement agencies that provide homeland security; researching and managing fish and wildlife populations and conservation; and conducting outreach programs to encourage participation and responsible citizenship and stewardship of the State's natural resources.

During the period September through December 2016, the FWCC allowed both FWCC-owned and personally owned mobile devices to access the FWCC network and e-mail.

## ***FINDINGS AND RECOMMENDATIONS***

---

### **Finding 1: Impact Analysis**

An effective risk management program includes an impact analysis that ensures the entities' priorities and risk tolerances are established and used to support operational decisions. An impact analysis should be conducted prior to allowing the use of mobile devices to help identify security requirements, aid in designing the mobile device solution, and incorporate the necessary security controls needed to meet the security requirements of each mobile device type. Agency for State Technology (AST) rules<sup>7</sup> require each State agency to, prior to introducing new IT resources or modifying current IT resources, perform an impact analysis to assess the effects of the technology or modifications on the existing IT environment and ensure that IT resources conform to agency standard configurations prior to implementation into the production environment.

Our audit procedures disclosed that the DLA, DVA, and 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.

An impact analysis allows the agency to identify security requirements and to design IT security controls necessary to meet those requirements to protect the confidentiality, availability, and integrity of agency data and IT resources.

**Recommendation: 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.**

---

<sup>6</sup> Article IV, Section 9 of the State Constitution.

<sup>7</sup> AST Rule 74-2.002(5)(g), Florida Administrative Code.

## Finding 2: Mobile Device Policies and Procedures

Effective IT security controls include documented security policies and procedures. When introducing new IT resources or modifying current IT resources, security policies and procedures should be designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems. Security policies and procedures for mobile devices should include IT security requirements pertaining to device encryption, current standard configuration, patching, anti-virus protection, incident response procedures, and passcode protection. In addition, AST rules<sup>8</sup> require agencies to ensure that security policies, processes, and procedures are maintained and used to manage the protection of information systems and assets, and include a current baseline configuration of information systems. Baselines must specify standard hardware and secure standard configurations.

Our audit procedures disclosed that IT controls related to mobile device policies and procedures at the DLA and FWCC need improvement. Specifically, we noted that:

- The DLA lacked a policy requiring encryption and patching of personally owned mobile devices. In addition, although DLA policies<sup>9</sup> specified that personally owned mobile devices must meet certain minimum requirements for hardware and software, including but not limited to approved operating systems, the policies and procedures did not specify the approved operating systems for personally owned mobile devices other than laptops. Also, the minimum operating system specified for personally owned laptops was included in a DLA policy that had not been updated since September 26, 2011,<sup>10</sup> and allowed an operating system that was no longer supported by the vendor. In response to our inquiry, DLA management stated that the policy was updated on December 12, 2016, to no longer allow the unsupported operating system.
- Although the FWCC established policies and procedures addressing security requirements for personally owned mobile devices, the policies and procedures were not sufficiently detailed to address specific security requirements such as device encryption, user patching requirements, passcode requirements, and minimum operating systems. Similarly, the FWCC did not have policies and procedures in place that specified the minimum operating system requirements for FWCC-owned smartphones.

Documented policies and procedures addressing security controls for mobile devices help ensure the confidentiality, integrity, and availability of agency data and IT resources.

**Recommendation: 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.**

## Finding 3: Mobile Device Agreements

Effective mobile device security program controls include appropriate documentation (e.g., mobile device agreement forms) that clearly defines the responsibilities of the entity and the user when mobile devices are used to connect to an entity's network and IT resources. NIST guidelines<sup>11</sup> recommend that entities educate users on the importance of security measures, such as encryption, patching, passcodes, and

<sup>8</sup> AST Rule 74-2.003(5), (5)(a), and (5)(a)1., Florida Administrative Code.

<sup>9</sup> *IT Network Access and Security Policy and Procedure Manual 9.04.04.*

<sup>10</sup> *Home PCs and Remote Access*, revised September 26, 2011.

<sup>11</sup> NIST Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013.

incident response, and define users' responsibilities for implementing these measures within mobile device agreements. Additionally, AST rules<sup>12</sup> require that employees verify in writing that they will comply with agency IT security policies and procedures prior to accessing agency IT resources.

Our audit procedures disclosed that the controls related to mobile device agreements at the DLA, DVA, and FWCC need improvement. Specifically, we found that:

- DLA users approved for remote access were required to electronically sign a mobile device agreement (either a *Remote Computing Device* form or an *Authorization to Use Personal Mobile Device (BYOD)* form) to document the user's acknowledgement of their responsibilities regarding the use of mobile devices. We inspected a list of all DLA users with remote access capabilities as of November 16, 2016, and determined there were 609 unique active user IDs. We compared the electronic files containing all signed user agreements as of November 17, 2016, to the list of active users, and determined that the DLA did not have a user agreement on file for 583 active remote users. In response to our inquiry, DLA management stated that a *Remote Computing Device* form or an *Authorization to Use Personal Mobile Device (BYOD)* form was not always provided to the user for electronic signature when remote access was provided.
- The DVA required users to complete and sign an *Acceptable Use Notification Record (Record)* to document the users' acknowledgement of their responsibilities regarding remote access. We requested the completed and signed *Records* for 6 of the 54 users granted access to use DVA-owned mobile devices remotely as of October 12, 2016. Our review disclosed that for 1 of the 6 users, the DVA was unable to provide a completed and signed *Record*. According to DVA management, some forms had been misplaced or were missing.
- Although the FWCC required new employees to certify in writing that they read the *Internal Management Policies and Procedures (Procedures)* on the FWCC's intranet site upon hire, the *Procedures* did not address the specific responsibilities of the FWCC or the employees regarding personally owned mobile devices. In addition, 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.

Absent appropriately completed and signed mobile device agreement forms or other related documentation applicable to the authorized use of mobile devices, users may not be aware of the security risks and their responsibilities, thereby increasing the risk of data loss.

**Recommendation:** 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.

#### **Finding 4: Mobile Device Management**

Mobile device security best practices include security controls that require a complete inventory of mobile devices authorized to connect to an entity's environment, operating system updates for mobile devices, enforcement of authentication requirements including passcodes before accessing the entity's resources, 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

---

<sup>12</sup> AST Rule 74-2.003(3)(f)., Florida Administrative Code.

devices.<sup>13</sup> In addition, AST rules<sup>14</sup> require encryption of mobile device IT resources that store, process, or transmit confidential or exempt information.

Our audit procedures disclosed that security controls at the DLA and FWCC related to mobile devices need improvement. For the DLA we found that:

- The DLA did not maintain a complete inventory of personally owned mobile devices authorized to connect to DLA's environment thereby limiting user provisioning,<sup>15</sup> the prevention and detection of unauthorized mobile device access to the network, and incident response in the event of a lost or stolen device.
- The DLA did not enforce operating system updates, the use of security passcodes, or encryption of mobile device data for personally owned mobile devices. Additionally, the DLA did not prohibit remote users from saving confidential and sensitive data locally on personally owned mobile devices. While the remote access software had a setting that prevented users from saving data locally on the mobile device, as of November 9, 2016, that setting was not configured to globally prohibit saving files locally.
- The ability to remotely wipe lost or stolen DLA-owned laptops and personally owned mobile devices did not exist as of November 9, 2016.

For the FWCC we found that:

- 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.

A lack of security controls that promote the effective management and administration of mobile devices increases the risk that unauthorized personnel may access agency resources and confidential and sensitive agency data without timely detection.

**Recommendation:** 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.

---

<sup>13</sup> NIST Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013.

<sup>14</sup> AST Rule 74-2.003(4)(b)4., Florida Administrative Code.

<sup>15</sup> A business process for creating, managing, and deactivating access to resources in an IT system.



## **OBJECTIVES, SCOPE, AND METHODOLOGY**

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2016 through December 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected security controls applicable to the internal controls for managing and securing mobile devices for the Department of Legal Affairs (DLA), Department of Veterans' Affairs (DVA), and Fish and Wildlife Conservation Commission (FWCC) during the period September 2016 through December 2016 and subsequent actions thereto.

- To determine the effectiveness of selected IT controls in achieving management's control 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.
- Effectiveness of the internal controls for managing and securing mobile devices connected to the agency's network.
- Effectiveness of the internal controls for managing and securing mobile devices storing confidential and sensitive data.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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

As described in more detail below, for the security controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the security controls; 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; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of security controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

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

In conducting this audit, we:

- Interviewed DLA, DVA, and FWCC personnel and reviewed mobile device security related documentation to obtain an understanding of:
  - The organizational structure and related job duties, responsibilities, and activities of personnel responsible for managing and securing mobile devices.
  - The risk management process for mobile devices.
  - The security controls utilized by the agency to manage mobile devices connected to the network or that store sensitive and confidential data.
- Evaluated the ongoing risk management processes including whether an impact analysis, as it relates to mobile devices connected to the respective agency's network or for storing sensitive and confidential data including planning, conducting, and documenting the impact analysis, was conducted prior to the implementation of a mobile device program that allows users to remotely access DLA, DVA, and FWCC data and IT resources.
- Inspected initial and annual security awareness training documentation and mobile device user agreements at the DLA, DVA, and FWCC to determine whether mobile device security risks and responsibilities for agency-owned and personally owned devices were addressed.
- Evaluated the effectiveness of the authorization controls for DLA-owned mobile devices and personally owned devices. Specifically, we compared the list of all 609 active user IDs granted remote access to DLA resources to the user agreements on file as of November 17, 2016, to determine whether a user agreement existed for all active users.
- Evaluated the effectiveness of the authorization controls for DVA-owned mobile devices. For 6 of the 54 DVA active remote users assigned agency-owned devices as of October 12, 2016, we requested user agreements to determine whether users acknowledged their responsibilities regarding access prior to using DVA-owned mobile devices for remote access.
- Evaluated the effectiveness of the authorization controls for FWCC-owned mobile devices for 25 of the 1,512 FWCC active remote users assigned agency-owned devices as of September 12, 2016, to determine whether users were authorized prior to using FWCC-owned mobile devices for remote access.
- Evaluated the appropriateness of remote access privileges including timely deactivation of access privileges of former DLA employees for 13 users assigned agency-owned laptops and 5 users utilizing personally owned devices for the purpose of remotely accessing DLA data and IT resources from a listing of 609 active user IDs with remote access privileges as of November 10, 2016.
- For FWCC, evaluated the appropriateness of remote access for 40 employees including the deactivation of remote access privileges for employees who were no longer employed by the FWCC as of November 14, 2016.

- Evaluated the effectiveness of the mobile device policies and procedures at the DLA, DVA, and FWCC, including whether the policies and procedures included required security components for agency-owned and personally owned mobile devices and the responsibilities for both the agency staff and the user assigned to the device. Specifically, we determined whether the policies and procedures addressed:
  - Standard configuration, including minimum operating systems for laptops, smartphones, and tablets.
  - Patch management.
  - Malware protection.
  - Mobile device and connection encryption.
  - User provisioning.
  - Incident response.
- Evaluated the effectiveness of DLA, DVA, and FWCC security controls used for user provisioning, data loss prevention, inventory management, to manage agency-owned and personally owned mobile devices.
- Evaluated the effectiveness of DLA, DVA, and FWCC authentication controls used to access agency-owned and personally owned mobile devices.
- Evaluated the effectiveness of DLA, DVA, and FWCC security controls for preventing unauthorized mobile devices from accessing the network.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENTS' RESPONSE**.

## ***AUTHORITY***

---

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA  
Auditor General

# MANAGEMENTS' RESPONSE

---



**PAM BONDI**  
**ATTORNEY GENERAL**  
**STATE OF FLORIDA**

**OFFICE OF THE ATTORNEY GENERAL**  
**Inspector General**

Steve Rumph  
PL 01, The Capitol  
Tallahassee, Florida 32399-1050  
Telephone (850) 414-3300  
Fax (850) 922-3854, SunCom 292-3854

---

April 21, 2017

Ms. Sherrill Norman, CPA  
Auditor General  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Enclosed is the audit response to your preliminary and tentative audit findings and recommendations from the Mobile Device Security Controls audit.

**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.**

**Department of Legal Affairs Audit Response:** A Business Impact Analysis has been undertaken and a Statement will be available within 30 days.

**Recommendation 2: 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.**

**Department of Legal Affairs Audit 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.

**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.**

**Department of Legal Affairs Audit 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.

**Recommendation 4:** 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.

**Department of Legal Affairs Audit 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.

If you have any questions, please call Judy Goodman at (850) 414-3456.

Sincerely,

A handwritten signature in blue ink, appearing to read 'SR', with a long horizontal flourish extending to the right.

Steve Rumph  
Inspector General



**Glenn Sutphin**  
Executive Director

State of Florida  
**DEPARTMENT OF VETERANS' AFFAIRS**  
**Office of the Executive Director**  
The Capitol, Suite 2105, 400 South Monroe Street  
Tallahassee, FL 32399-0001  
Phone: (850) 487-1533 Fax: (850) 488-4001  
[www.FloridaVets.org](http://www.FloridaVets.org)

**Rick Scott**  
Governor  
**Pam Bondi**  
Attorney General  
**Jeff Atwater**  
Chief Financial Officer  
**Adam Putnam**  
Commissioner of Agriculture

March 31, 2017

Sherrill F. Norman, CPA  
Auditor General  
Claude Pepper Building, Suite G74  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

This letter is in response to your letter dated 22 March 2017, outlining the findings from the Mobile Device Security Audit of the Florida Department of Veterans' Affairs (FDVA). Pursuant to Section 11.45(4)(d) of the Florida Statutes, we are providing our response to the preliminary and tentative Mobile Device Security Audit findings and recommendations.

FDVA, IT in particular, is taking measures to improve the areas identified during the Auditor General's Mobile Security Audit. The agency strives for the continued improvement of our processes so that we may continue to provide excellent service and appreciates your efforts in assisting us with this goal.

On behalf of FDVA, I would like to thank your staff for their professionalism and expertise during the audit process. If you have any questions, please contact the Office of Inspector General at 727-518-3202 extension 5570.

Sincerely,

Glenn W. Sutphin, Jr.  
Lieutenant Colonel, U.S. Army (Retired)  
Executive Director

*"Honoring those who served U.S."*

**Finding No. 1: Impact Analysis**

The DLA, FDVA, 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:**

That DLA, FDVA, 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.

**Response:**

FDVA will document all of the security requirements/IT security controls necessary to meet the AST requirements. On a regular basis, FDVA will review the analysis and make changes as necessary.

**Finding No. 3: Mobile Device Agreements**

Controls related to mobile device agreements at the DLA, FDVA, 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:**

We recommend that DLA, FDVA, 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.

**Response:**

FDVA will coordinate the review of the Acceptable Use Notification Record with the HR office and check off the review on a bi-annual basis. FDVA will maintain documentation of the reviews.



Florida Fish and Wildlife Conservation Commission

Commissioners

Brian Yablonski
Chairman
Tallahassee
Aliese P. "Liesa" Priddy
Vice Chairman
Immokalee

Ronald M. Bergeron
Fort Lauderdale

Richard Hanas
Oviedo

Bo Rivard
Panama City

Charles W. Roberts III
Tallahassee

Robert A. Spottswood
Key West

Executive Staff

Nick Wiley
Executive Director

Eric Sutton
Assistant Executive Director

Jennifer Fitzwater
Chief of Staff

Office of the
Executive Director

Nick Wiley
Executive Director

(850) 487-3796
(850) 921-5786 FAX

Managing fish and wildlife
resources for their long-term
well-being and the benefit
of people.

620 South Meridian Street
Tallahassee, Florida
32399-1600
Voice: (850) 488-4676

Hearing/speech-impaired:
(800) 955-8771 (T)
(800) 955-8770 (V)

MyFWC.com

April 20, 2017

Ms. Sherrill F. Norman, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Our responses to your preliminary and tentative audit findings, and recommendations from your recent information technology audit of the Mobile Device Security Controls at the Florida Fish and Wildlife Conservation Commission (FWC), are included below:

Finding 1: The FWC 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: We recommend that FWC 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.

Response: The FWC will conduct and document an impact analysis as recommended. Anticipated completion date: September 2017.

Finding 2: FWC security policies and procedures for mobile devices need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

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

Response: 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.

Finding 3: Controls related to mobile device agreements at the FWC 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: We recommend that FWC 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.



**Response:** *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: September 2017.*

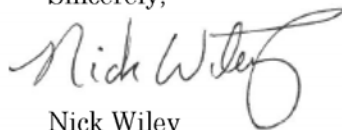
**Finding 4:** FWC security controls for the management and administration of mobile devices need improvement to correspond to the complexity of the related mobile device environment.

**Recommendation:** We recommend that FWC 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.

**Response:** *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.*

We welcome the information provided by your staff and the recommendations for improvements included in this report. If further information is required, please contact Mike Troelstrup, Inspector General, at (850) 488-6068.

Sincerely,



Nick Wiley  
Executive Director