STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-009
August 2018

FISH AND WILDLIFE CONSERVATION COMMISSION

Information Technology General Controls

Sherrill F. Norman, CPA
Auditor General

The Fish and Wildlife Conservation Commission and Executive Director

The Fish and Wildlife Conservation Commission is established by Article IV, Section 9 of the State Constitution and operates under the authority of Sections 20.331 and 379.1025, Florida Statutes. The seven Commissioners are appointed by the Governor, subject to confirmation by the Senate, for staggered 5-year terms. The Commissioners who served during the period of our audit were:

Adrien “Bo” Rivard	Chair from December 7, 2017
Brian S. Yablonski	Chair through December 6, 2017
Robert A. Spottswood	Vice Chair from January 12, 2018
Aliese P. “Liesa” Priddy	Vice Chair through December 1, 2017
Ronald M. Bergeron	Through December 1, 2017
Richard Hanas	Through January 12, 2018
Joshua Kellam	From February 2, 2018
Gary Lester	From January 12, 2018
Gary Nicklaus	From December 1, 2017
Sonya Rood	From December 1, 2017
Michael W. Sole	From May 12, 2017

The Executive Director is appointed by the Commission, subject to confirmation by the Senate, and serves at the pleasure of the Commission. The Executive Director supervises, directs, coordinates, and administers all activities necessary to fulfill the Commission’s constitutional and statutory responsibilities. The following individuals served as Executive Director during the period of our audit:

Eric Sutton	From December 8, 2017
Nick Wiley	Through December 7, 2017

The team leader was Clark Evans, CPA, CISA, and the audit was supervised by Hilda Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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

FLAuditor.gov

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

FISH AND WILDLIFE CONSERVATION COMMISSION

Information Technology General Controls

SUMMARY

This operational audit of the Fish and Wildlife Conservation Commission (Commission) focused on evaluating selected information technology (IT) general controls. Our audit disclosed the following:

Finding 1: The Commission had not established IT security policies and procedures to protect and manage IT boundaries and data communications.

Finding 2: The Commission had not established procedures for comprehensive periodic access reviews and the access reviews performed were not documented.

Finding 3: The Commission did not timely disable the network access privileges for some employees who separated from Commission employment.

Finding 4: Commission backup policies and procedures need improvement.

Finding 5: The Commission's computer security incident response policies and procedures need improvement to promote prompt and appropriate responses to cybersecurity events.

Finding 6: 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.

BACKGROUND

The Fish and Wildlife Conservation Commission (Commission) is tasked with a diverse set of responsibilities, ranging from law enforcement to research.[1] As of March 2018, the Commission's organizational structure included the Divisions of Law Enforcement, Hunting and Game Management, Habitat and Species Conservation, Freshwater Fisheries Management, and Marine Fisheries Management, as well as, the Fish and Wildlife Research Institute.

The Fish and Wildlife Research Institute's work includes assessment and restoration of ecosystems and studies of freshwater and marine fisheries, aquatic and terrestrial wildlife, imperiled species, and red tides. The Institute develops the information science required to analyze and disseminate research products and engages in outreach activities to complement all programs. As such, a Commission-owned and managed data center (Data Center) to support these research functions is maintained in St. Petersburg, Florida.[2]

The Commission also has regional administrative offices, and field offices and facilities throughout the State. The Commission's Office of Information Technology (OIT) is responsible for the administration of

[1] Section 20.331(4), Florida Statutes.

[2] Section 282.201(4), Florida Statutes.

the Data Center and the Commission-owned information technology (IT) resources located throughout the State.

FINDINGS AND RECOMMENDATIONS

Finding 1: IT Security Policies and Procedures

Effective IT security controls include documented security policies and procedures. A security policy is management's directives to create a computer security program, establish its goals, and assign responsibilities. Policies are written at a broad level and procedures provide the detailed steps to be followed to accomplish security-related tasks. Security policies and procedures include adequately protecting IT boundaries and data communications through controlled interfaces such as firewalls, proxies, routers, and switches. Agency for State Technology (AST) rules[3] require each agency to ensure that security policies and procedures are maintained and are used to manage protection of information systems and assets.

Our audit procedures disclosed that the Commission had not established and implemented IT security policies and procedures for protecting and managing IT boundaries and data communications. Specifically, the Commission had not established written policies and procedures for:

- Managing the firewalls with specific requirements for patch management, logical access, and traffic configuration rules.
- E-mail security that addressed filtering and scanning for malicious content.

Documented policies and procedures for protecting and managing IT boundaries and data communications help prevent intrusions through the firewalls or e-mail, thereby reducing the risk that Commission data and IT resources may be compromised.

Recommendation: 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.

Finding 2: Periodic Review of Access Privileges

AST rules[4] require agency control measures to address responsibilities of information stewards and facilitate periodic reviews of access rights with information owners. The frequency of the reviews must be based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit procedures disclosed that the Commission had not established procedures for comprehensive periodic reviews of user access privileges including accounts with elevated access privileges. In response to our audit inquiry, Commission management directed us to the user account clean-up process in the Commission procedure *Disposition of Network User Accounts* and identified this as the periodic

[3] AST Rule 74-2.003(5), Florida Administrative Code.

[4] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

access review procedure. The user account clean-up process provides methods to identify users who have separated from Commission employment and inactive user accounts so that the user accounts can be disabled. Specifically:

- Biweekly, Human Resources provides a separation report to OIT. OIT staff compare the report to the user access list, identify user accounts belonging to former employees, and initiate the process to disable the user accounts.
- Quarterly, OIT generates an expired user report showing user accounts with 60 days of inactivity (i.e., expired) and initiates the process to disable the user accounts on the expired user report.

According to Commission management, periodic reviews of user accounts with elevated access privileges are conducted every 6 to 8 months or as needed. However, there is not a formal process to document the review and Commission management was unable to provide documentation of such reviews during the period July 1, 2017, through June 12, 2018.

While the Commission had processes to help identify the user accounts of former employees and inactive users so that the accounts can be disabled, the processes did not represent a comprehensive periodic access review procedure. A comprehensive periodic access review procedure that requires the identification of the current access privileges of all users, evaluation of the access privileges necessary for each user's job responsibilities, and documentation that the access privileges granted reflect the appropriate access privileges, increases management's assurance that the user access privileges assigned are authorized and remain appropriate.

Recommendation: 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.

Finding 3: Timely Disabled Network User Accounts

AST rules[5] require agency control measures to ensure IT access is removed when an IT resource is no longer required. Prompt action to disable access privileges when a user separates from employment or no longer requires access to an IT resource is necessary to help prevent misuse of the access privileges. Commission procedures[6] require supervisors to submit a form when an employee separates from Commission employment to initiate the process for removing network user accounts and other IT resource access privileges. According to Commission staff, when the script to remove the network user account runs, the network account disablement dates are systematically recorded on the required form.

As part of our audit, we evaluated whether network access privileges were timely removed for 9 of the 36 employees who separated from Commission employment during November 2017. We found that for 1 of the 9 former employees neither the completed form nor other evidence of the date the network user account was disabled was maintained. For 3 of the 8 remaining former employees, the network user accounts were not timely disabled and remained active between 3 and 32 days after the users'

[5] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

[6] Commission OIT Operating Procedure Section OIT-2.1, *Disposition of Network User Accounts*.

employment separation dates. Additionally, although the network user account for another of the 8 former employees was timely disabled according to a manually recorded date, the form with the system-recorded date of disablement was not available.

Timely disabling network user accounts upon an employee's separation from Commission employment reduces the risk that the network access privileges may be misused by the former employee or others.

Recommendation: 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.

Finding 4: Backup Controls

Effective backup controls include written policies and procedures that provide guidance for an entity's backup processes, including the identification of the IT resources requiring back up, the frequency of backups, and the periodic testing for recoverability to prevent or minimize the damage to automated operations that can occur from unexpected events. AST rules[7] require each agency to develop procedures to prevent loss of data and to ensure that backups of information are conducted, maintained, and tested periodically. AST rules also require each agency to mirror data and software essential to the continued operation of critical agency functions to an off-site location or regularly back up a current copy for storage at an off-site location. Additionally, effective controls ensure that accurate records of the location and status of backup data are maintained and all backups are accounted for to strengthen an entity's ability to restore data files and minimize the risk of data loss that may occur due to an unexpected event.

Our audit procedures disclosed that Commission backup controls need improvement. Specifically, we found that:

- The Commission had not established policies and procedures governing the back up of data on Commission-managed servers and addressing backup frequency, periodic recoverability testing, and backup tape location records.
- Commission-managed backups were not periodically tested to ensure recoverability.
- Monthly backup tapes were created at the Data Center, stored in a vault in Tallahassee until expired, and returned to the Data Center for reuse or destruction. However, the Commission did not document the movement of the tapes as they went back and forth between the Data Center and the vault.
- Weekly backup tapes created at the Data Center were not stored off-site to ensure the availability of the backup tapes in the event of a disaster affecting the Data Center.

The lack of policies and procedures that establish effective backup controls limits the Commission's ability to timely and completely recover in the event of a loss of production data. Additionally, storing weekly backup tapes at the Data Center and the lack of records to identify the location of monthly backup tapes jeopardizes the availability of the backup tapes in the event of a disaster affecting the Data Center.

[7] AST Rules 74-2.006(1)(b) and (c) and 74-2.003(5)(d), Florida Administrative Code.

Recommendation: 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.

Finding 5: Computer Security Incident Response

AST rules[8] require agencies to establish and maintain response processes and procedures and validate execution capability to ensure timely agency response for detected cybersecurity events. Agencies are also required to establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents. Responsibilities of CSIRT members include, among other things, receiving training at least annually on cybersecurity threats, trends, and evolving practices. Additionally, as shown in Table 1, the AST has established timeframes for agencies to report incidents to the AST and the Cybercrime Office within the Department of Law Enforcement.

Table 1
Incident Reporting Timeframes

Rating	Initial Notification	Definition of Effect Rating
Minimal	Monthly aggregate	Effect on IT resources managed by internal process
Low	Weekly	Minimal effect on IT resources
Medium	1 business day	Moderate effect on IT resources
High	Within 4 hours	Severe effect on IT resources or delivery of services
Critical	Immediately	Severe effect on IT resources, believed to impact multiple agencies or delivery of services

Source: AST Rule 74-2.005(1)(a)5., Florida Administrative Code.

The Commission's computer security incident response policy[9] provides that periodic simulation exercises are to be conducted to offer initial training to CSIRT members and their backups, and annual refresher training thereafter.

Our audit procedures disclosed that the Commission computer security incident response policies and procedures need improvement. Specifically, we found that:

- CSIRT member training had not been held since 2013. While Commission management scheduled the CSIRT member training for October 11, 2017, the training was postponed for lack of attendance. Commission management subsequently stated that several tabletop exercises were performed at the CSIRT meeting held on May 8, 2018. Annual CSIRT member training would promote prompt and appropriate responses to cybersecurity events.
- The Commission's computer security incident response policy had not been revised since June 2011 and the reporting timeframes and classification of incidents referenced by the policy were not in compliance with AST rules. In response to our audit inquiry, Commission management stated that they are now reporting computer security incidents in compliance with AST rules and acknowledged the need to revise the policy. Should an incident occur that involves the potential or actual compromise, loss, or destruction of Commission data or IT resources, the lack of an up-to-date computer security incident response policy that is compliant with AST rules

[8] AST Rule 74-2.005(1), Florida Administrative Code.

[9] Commission Policy and Procedures Section 3.8, *Computer Security Incident Reporting and Response Policy*.

may result in Commission management's failure to take timely and appropriate actions to prevent further loss or damage to Commission data and IT resources.

- Computer security incidents were not always timely reported to the AST. Our review of documentation for nine computer security incidents that occurred during the period July 1, 2016, through December 20, 2017, with initial (three incidents) or final (six incidents) incident levels of medium or higher disclosed that six of the nine computer security incidents were not timely reported to the AST as required by AST rules. One of the six incidents was not reported to the AST at all, and the remaining five incidents were reported 8 to 21 days after the incident occurred.
- While the Commission established, as of August 25, 2016, a virus and malware response procedure checklist (response checklist) to document and streamline the response to viruses and malware, the checklist was not always completed as required. We reviewed documentation of the eight computer security incidents that occurred during the period August 26, 2016, through December 20, 2017, with an incident classification of virus or malicious software (widespread) and an incident description indicating a ransomware event and noted that a checklist was not completed for one of the eight computer security incidents.

Absent effective Commission computer security incident response policies and procedures that establish processes for responding to detected cybersecurity events and suspected computer security incidents, there is reduced assurance that the Commission will timely and appropriately respond to detected or suspected security events.

Recommendation: We recommend that Commission management ensure CSIRT member training is conducted on an annual basis, revise the *Computer Security Incident Reporting and Response Policy* to comply with 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.

Finding 6: Security Controls – Logical Access, User Authentication, Logging and Monitoring, Vulnerability Management, Configuration Management, and Network Security Settings

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, logging and monitoring, vulnerability management, configuration management, and network security settings need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Commission data and other Commission IT resources. However, we have notified appropriate Commission management of the specific issues.

Without appropriate security controls related to logical access, user authentication, logging and monitoring, vulnerability management, configuration management, and network security settings, the risk is increased that the confidentiality, integrity, and availability of Commission data and IT resources may be compromised.

Recommendation: 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.

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 November 2017 through April 2018 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 IT general and security controls applicable to the Commission during the period of July 2017 through April 2018, and selected actions prior and subsequent thereto.

The overall objectives of the audit were:

- To evaluate 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 at the Commission.
- 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 IT systems and 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 IT systems and 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 IT systems and 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 IT system 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 Commission personnel and reviewed related documentation to obtain an understanding of:
  - The patch management process for Commission-managed servers and Data Center servers, Commission end-user workstations, laptops, and firewall devices, and to identify key personnel responsible for the process.
  - The automated data backup process for servers utilized by the Commission, including procedures for ensuring all data is saved to locations protected by the backup process.
  - The security hardware and software in place to protect the Commission network and interconnected systems from external attacks and intrusions.
  - User provisioning processes and periodic review processes for logical access to Commission systems and the interconnected network.
  - Logging and monitoring capabilities at the Commission related to the capture and review of security events.
  - The Commission's computer security incident response plan and related legal requirements.
  - The process for planning, conducting, and documenting vulnerability testing of the Commission network and interconnected systems and remediation of issues noted.
- Evaluated the effectiveness of the Commission patch management processes for servers, high-risk network devices, and workstations. Specifically, we reviewed:
  - 10 of the 90 active Commission-managed servers as of December 12, 2017, to evaluate whether the Commission had timely installed vendor-supplied patches.
  - Five selected high-risk network devices to evaluate whether, as of January 29, 2018, and February 9, 2018, the Commission had timely installed vendor-supplied patches.
  - 42 of the 3,369 active Commission-managed workstations to evaluate whether, as of February 14, 2018, the Commission had timely installed vendor-supplied patches.
- Evaluated the effectiveness of the backup process for Commission-managed servers, including tape and disk backups, backup tape reconciliation processes, offsite tape rotation, and testing of recoverability. Specifically, we examined backup evidence for 11 of the 89 active Commission-managed servers not used for disaster recovery, as of January 19, 2018, and February 22, 2018, to determine whether daily backups to disk were performed.
- Evaluated the logical design, appropriateness, administration, and periodic review procedures for logical access privileges to the Commission network, systems, and IT resources. Specifically, we reviewed:
  - The appropriateness of access for network accounts with administrative access privileges as of December 12, 2017, for:
    - The 28 Active Directory accounts (19 service accounts and 9 user accounts) in the *Domain Admins* security group allowing administrative access privileges to the *fwc.state.fl.us* domain.

        - The 5 Active Directory accounts (3 service accounts and 2 user accounts) in the *Enterprise Admins* security group allowing administrative access privileges at the forest-level including the *fwc.state.fl.us* domain.
        - The 1 Active Directory user account with membership in the *Schema Admins* security group.
        - The 6 Active Directory accounts (5 service accounts and 1 user account) with membership in the *Administrators* security group allowing administrative access privileges to the *fwc.state.fl.us* domain.
    - The appropriateness of access privileges for a total of 65 administrative accounts with membership in the locally defined *Administrators* security group on each server, excluding the *Domain Admins* security group, for 9 of the 90 active Commission-managed servers as of December 19, 2017, to verify that access was appropriately assigned.
    - The appropriateness of access privileges for the 90 Active Directory accounts not disabled in the locally defined *Administrators* security group for Windows workstations as of December 20, 2017.
    - The appropriateness of access for the 28 administrative accounts among five selected high-risk network devices as of December 22, 2017, January 25, 2018, January 29, 2018, January 30, 2018, and February 14, 2018.
    - The effectiveness of periodic access review processes including the adequacy of periodic reviews of network user access.
    - Network access privileges for 9 of the 36 employees who separated from Commission employment during November 2017 to determine whether the privileges were timely disabled.
- Evaluated the effectiveness of the Commission network infrastructure user authentication controls. Specifically, we reviewed:
    - User authentication controls for the Commission network domain as of December 12, 2017.
    - User authentication controls for five selected high-risk network devices as of January 25, 2018, January 29, 2018, and February 12, 2018.
- Evaluated the effectiveness of Commission logging and monitoring controls related to network security events as of December 15, 2017, and December 22, 2017.
- Evaluated whether Commission policies and procedures for protecting and managing IT boundaries and data communications help to prevent intrusions through the firewalls or e-mail.
- Evaluated whether Commission computer security incident response policies and procedures were sufficient for responding to suspected computer security incidents. Specifically, we reviewed:
    - The Commission's *Computer Security Incident Reporting and Response Policy*.
    - Computer security incidents that occurred during the period of July 1, 2016, through December 20, 2017, to evaluate whether computer security incidents were timely reported to the AST in compliance with AST rules, including the three computer security incidents that occurred during 2017 with an initial incident level of medium or higher and the six computer security incidents that occurred during 2016 with a final incident level of medium or higher.
    - Documentation of the eight computer security incidents that occurred during the period of August 26, 2016, through December 20, 2017, with an incident classification of virus or malicious software (widespread) and an incident description indicating a ransomware event to determine whether the Commission's response checklist was completed as required.

- Evaluated the Commission's annual security awareness training documentation and the statement of understanding for the *Password Policy*[10] to determine whether Commission security risks and network user responsibilities were adequately addressed. Specifically, we reviewed:
  - Screen shots of the Commission's Security Awareness Training located on SharePoint.
  - Six non-Other Personal Services (non-OPS) Commission employees with initial hire dates between November 1, 2017, and November 30, 2017, to evaluate whether the employees timely completed security awareness training.
  - Six non-OPS Commission employees with initial hire dates between November 1, 2017, and November 30, 2017, to evaluate whether the employees accessing Commission IT resources had verified in writing that they would comply with the Commission IT security policies, specifically the *Password Policy*.
- Evaluated whether Commission procedures addressed vulnerability management including analysis and remediation of reported vulnerabilities on the Commission 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 ***MANAGEMENT'S 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

[10] Commission Policy and Procedures Section 3.3, *Password Policy*.

MANAGEMENT'S RESPONSE

Florida Fish and Wildlife Conservation Commission

Commissioners
Bo Rivard
Chairman
Panama City

Robert A. Spottswood
Vice Chairman
Key West

Joshua Kellam
Palm Beach Gardens

Gary Lester
Oxford

Gary Nicklaus
Jupiter

Sonya Rood
St. Augustine

Michael W. Sole
Tequesta

Office of the Executive Director
Eric Sutton
Executive Director

Thomas H. Eason, Ph.D.
Assistant Executive Director

Jennifer Fitzwater
Chief of Staff

Office of Inspector General
Mike Troelstrup
Inspector General
(850)488-6068

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

August 3, 2018

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

Dear Ms. Norman,

In compliance with section 11.45(4)(d), Florida Statutes, enclosed are the responses to your Information Technology audit of the Fish and Wildlife Conservation Commission (FWC or Commission).

We appreciate the opportunity to respond to your preliminary and tentative findings and recommendations. We found your staff to be professional and thorough, and always look forward to the opportunity to improve our operations.

If you have any questions regarding our response please contact Mike Troelstrup, FWC Inspector General, at (850) 488-6068.

Sincerely,

Eric Sutton
Executive Director

Attachment

Cc: Ms. Jennifer Fitzwater, Chief of Staff
Mr. Mike Troelstrup, Inspector General

Finding 1: IT Security Policies and Procedures

Agency Response: 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 policy/procedure addressing patching to ensure the scope of the policy covers all areas of the IT boundaries and data communications. Additionally, a new OIT policy/procedure addressing email security is being developed.

Finding 2: Periodic Review of Access Privileges

Agency Response: The Commission concurs with the finding.

Corrective Action: OIT is currently developing policies and procedures to address these user access privilege issues. This 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 include definitions for elevated privileges, the focus of the review, frequency of the review, and any required documentation.

Finding 3: Timely Disabled Network User Accounts

Agency Response: The Commission concurs with finding.

Corrective Action: In conjunction with our Human Resources Office, 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.

Finding 4: Backup Controls

Agency Response: The Commission concurs with the finding.

Corrective Action: These issues deal with the backup processes and procedures at our FWRI facility in St. Petersburg. 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 and where any tapes are required to be moved offsite, that process will be re-evaluated and improved to ensure proper documentation and logging.

Finding 5: Computer Security Incident Response

Agency Response: The Commission concurs with the finding.

Corrective Action: The policy for the CSIRT process will be updated to comply with FAC 74-2 and statute 282. 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.

Finding 6: Security Controls – Logical Access, User Authentication, Logging and Monitoring, Vulnerability Management, Configuration Management, and Network Security Settings

Agency Response: The Commission concurs with the finding.

Corrective Action: : A Legislative Budget Request (LBR) is being processed to improve our ability to identify and monitor these vulnerabilities. This LBR will include the acquisition of a SEIM (Security Event Information Management) system. At the end of FY17-18, we also acquired a tool to allow longer retention of system logs, which will address several findings.