Agenda Item #: 3CC-1

PALM BEACH COUNTY

BOARD of COUNTY COMMISSIONERS

AGENDA ITEM SUMMARY

==========

Meeting Date: **4/4/2023**

[X] Consent [ ] Regular
[ ] Public Hearing

Department:
Submitted By: County Internal Auditor's Office

==========

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to receive and file:

A. Audit report reviewed by the Audit Committee at its March 15, 2023 meeting as follows:
   1. 2023-03 Information Systems Services – *IT Systems Access Controls (2022-02)*
   2. 2023-04 Facilities Development and Operations – Electronic Services and Security – *Contractors and After-Hours (2021-05)*
   3. 2023-05 Fire Rescue – *Operations Reporting* (2021-02)

Summary: The County Code requires the County Internal Auditor to submit copies of final audit reports to the Board of County Commissioners and the Internal Audit Committee. At its meeting on March 15, 2023 the Internal Audit Committee reviewed the attached audit reports. We are submitting these reports to the Board of County Commissioners as required by the County Code. Countywide (DB)

Background and Justification: County Code Section 2-463(e3) requires the County Internal Auditor to submit copies of final audit reports to the Board of County Commissioners and the Internal Audit Committee. At its meeting on March 15, 2023 the Internal Audit Committee reviewed the attached audit reports. We are submitting these reports to the Board of County Commissioners as required by the County Code.

Attachments:

1. 2023-03 Information Systems Services – *IT Systems Access Controls (2022-02)*
2. 2023-04 Facilities Development and Operations – Electronic Services and Security – *Contractors and After-Hours (2021-05)*
3. 2023-05 Fire Rescue – *Operations Reporting* (2021-02)

==========

Recommended by: Joseph T Bergeron 2 March 2023
County Internal Auditor Date

Recommended by: _____ _____
County Administrator Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact:

Fiscal Years	2023	2024	2025	2026	2027
Capital Expenditures					
Operating Costs					
External Revenues					
Program Income (County)					
In-Kind Match (County)					
NET FISCAL IMPACT	None				
# ADDITIONAL FTE					
POSITIONS (Cumulative)					

Is Item Included In Current Budget? Yes _____ No _____
Does this item include the use of federal funds? Yes _____ No _____
Budget Account No.: Fund ____ Agency ____ Org. _____ Object ____
Program Number _____ Revenue Source _____

B. Recommended Sources of Funds/Summary of Fiscal Impact:

No fiscal impact

A. Department Fiscal Review:

_____

III. REVIEW COMMENTS:

A. OFMB Fiscal and/or Contract Administration Comments:

3/7/2023
JA 3/6 Budget/OFMB ESW 3-6-2023

3/7/23
Contract Administration 3/7/23

B. Legal Sufficiency:

3/8/2023
Assistant County Attorney

C. Other Department Review:

_____
Department Director

This summary is not to be used as a basis for payment.

INTERNAL AUDIT REPORT

COUNTYWIDE
IT SYSTEMS ACCESS CONTROLS AUDIT

W/P No. 2022-02
Report # 2023-03

TABLE OF CONTENTS

COUNTYWIDE
IT SYSTEMS ACCESS CONTROLS AUDI
REPORT #2023-03

AUDIT OBJECTIVES AND CONCLUSIONS

We performed this audit to answer the following objectives:

1. Did Departments ensure user access for terminated users (employees and non-employees) to all IT systems was immediately deprovisioned in accordance with Palm Beach County IT Security Policies PPM CW-O-059, and within the National Institute of Standards and Technology (NIST) guidelines [SP 800-53]?

2. Did Departments ensure user access to department controlled IT resources was reviewed and adjusted immediately when employees were transferred or reassigned to other functions in accordance with Palm Beach County's IT Security Policies PPM CW-O-059 and PPM CW-O-61 entitled, *"Access to the Palm Beach County Enterprise Network?"*

As to the audit objectives above, we concluded:

1. Departments did not ensure user access for terminated users (employees and non-employees) to all IT systems was immediately deprovisioned in accordance with Palm Beach County's IT Security Policies PPM CW-O-059, and within the National Institute of Standards and Technology (NIST) guidelines.

2. Departments did not ensure user access to department controlled IT resources was reviewed and adjusted immediately when employees were transferred or reassigned to other functions in accordance with Palm Beach County's IT Security Policies PPM CW-O-059 and PPM CW-O-61 entitled, *"Access to the Palm Beach County Enterprise Network."*

In addition, we noted three issues of a minor nature that we determined did not rise to the level of audit findings, but were reportable to management for their attention and possible action. We provided six suggestions for improvement for these issues. The issues included managing shared access to an outward facing application, integration of vendor procured applications to SIM (centralized directory), and updating security PPM to reflect ISS' position on the timeframe to deprovision user access. We further address these issues in our Management Letter.

FINDINGS AND RECOMMENDATIONS

Finding #1: Departments did not deprovision terminated employee SIM accounts when required

A Secure Identity Management (SIM) account is set up for employees, which provides for access to certain information technology systems in which permissions are granted.

Condition

Departments did not deprovision 90% (169 of 187) of terminated employee SIM accounts as required by PPM CW-O-059, and 73% (136 of 187) within one business day of an employee's termination date. The number of days to deprovision user access ranged from zero to 87 calendar days and zero to 59 business days of an employee's termination date.

Of 25 departments with terminated employees, 21 (or 84%) did not deprovision user access immediately, and 20 (or 80%) did not deprovision user access within one business day of the employee's termination date.

Effect or Risk

A delay in deprovisioning a terminated employee's SIM account allows a user to retain access that is no longer needed. Unauthorized access to information systems creates a vulnerability that could be exploited, and/or allows information to be obtained or changed in unwanted ways.

Cause

Departmental SIM Administrators did not take steps to deprovision user access when required, are unfamiliar with the County's IT Security Policies (PPM CW-O-059), and do not have written guidelines for deprovisioning user access. In addition, 50% of departments indicated they received SIM training in the past.

Criteria

PPM CW-O-059 entitled "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to immediately revoke access to all IT systems and information by terminated employees. Our position is that "immediately" means the same day, and without delay. The County's Chief Information Security Officer (CISO) indicated access should be revoked within one business day after an employee

terminates without cause. However, we believe that position is not consistent with the language of the policy.

Recommendations:
1. Departments should deprovision an employee's SIM account immediately upon termination.
2. The ISS Department should train departmental SIM Administrators on the PPM deprovisioning requirements, and on the capabilities of SIM (Centralize Directory) to support them.

Finding #2: Departments rely on a secondary tool, HRIS connector (PA process), to deprovision terminated employee SIM accounts

Condition
Of 21 departments that did not deprovision terminated employee SIM accounts as required by PPM CW-O-059, nine (or 43%) indicated they do not proactively deprovision terminated employee SIM accounts, but rely on the HRIS connector through the personnel action (PA) process to revoke user access.

For these nine departments, the number of days to deprovision an employee SIM account after the PA effective date (termination date) ranged from zero to 87 calendar days and zero to 59 business days, with an average of 11 calendar and seven business days to deprovision user access.

According to the County's CISO, the HRIS connector is a fail-safe process put in place to catch and disable terminated employee SIM accounts, which were not deprovisioned by one of the available direct methods.

Effect or Risk
A delay in deprovisioning a terminated employee's SIM account allows a user to retain access that is no longer needed. Unauthorized access to information systems creates a vulnerability that could be exploited, and/or allows for information to be obtained or changed in unwanted ways.

Cause
Departmental SIM Administrators and management did not know that the HRIS connector (PA process) is a secondary (not primary) tool to deprovision a user's SIM account, and were unaware of the direct methods available to revoke user access. In addition, they do not have written guidelines on deprovisioning user access, with 56% (five of nine) indicating that someone from their department received SIM training.

Criteria
PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to immediately revoke access to all IT systems and information by terminated employees; and Section 22 System Access, 22.4 Roles and Responsibilities requires ISS to develop, maintain, and publish policies, procedures, and standards to facilitate efficiency during deprovisioning.

Recommendations:
3. Departments should deprovision SIM accounts immediately utilizing one of the available direct methods.
4. The ISS Department should develop and provide training to all SIM Administrators on deprovisioning user access, which includes the available methods to disable a user's SIM account within the required timeframe.

Finding #3: Departmental SIM Administrators were not promptly informed of employee terminations

Condition
Of 21 departments that did not deprovision user access when required, the SIM Administrator [or staff person tasked to remove user access] for five departments (or 24%) were not informed of employee terminations prior to the PA effective date as follows:

- For 19% of departments (four of 21), the SIM Administrator did not receive notification of the termination until after the PA effective date
- For 5% of departments (one of 21), the SIM Administrator was never notified of the employee terminations

In addition, one department's representatives confirmed that they do not have an internal process in place to inform their SIM Administrator of employee terminations.

Effect or Risk
A delay in deprovisioning a terminated employee's SIM account allows a user to retain access no longer needed. Unauthorized access to information systems creates a vulnerability that could be exploited, and/or allows for information to be obtained or changed in unwanted ways.

Cause
Departmental procedures do not provide for SIM Administrators to be notified of employees leaving prior to the termination date. Departmental personnel processing PAs either do not inform SIM Administrators of employee

terminations prior to the effective date, or are not notified themselves by departmental supervisors of an employee leaving prior to the termination date.

Criteria
PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to immediately revoke access to all IT systems and information by terminated employees, and Section 22 System Access, 22.4 Roles and Responsibilities requires departments to promptly disable access for terminated employees to systems under departmental control and to promptly notify ISS when users terminate.

Recommendations:
5. Department SIM Administrators (or staff tasked to remove user access) should be informed of employee terminations prior to the effective date.
6. Departments should develop procedures to ensure SIM Administrators are informed of employee terminations prior to their effective date.

Finding #4: Departments change terminated employees' SIM passwords to preclude user access, and do not disable the SIM account as required

Condition
Departments change the SIM passwords for terminated employees to preclude further user access, and do not deprovision their SIM accounts immediately in order to allow departmental access to the former employee's files located in their personal drive and/or in-box.

Our conversations with two departments confirmed that they do not disable employee SIM accounts immediately after an employee's termination date, and instead, change an employee's SIM password to preclude further access to information systems through their SIM account.

Effect or Risk
Departmental personnel have full access, without ISS assistance, to all files stored in a former employee's personal drive, which could lead to potential privacy issues if sensitive documents have been stored in the drive.

Cause
Procedures for accessing a former employee's files, located in their personal drive and inbox, have not been communicated to departments. Departmental

personal believe the only way to access a terminated employee's files is to change their SIM password without disabling their SIM account.

Criteria
PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to immediately revoke access to all IT systems and information by terminated employees, and Section 22 System Access, 22.4 Roles and Responsibilities requires ISS to develop, maintain, and publish policies, procedures, and standards for user credentials to facilitate efficiency during deprovisioning.

According to the County's CISO, departments should disable a terminated employee's SIM account as required, and submit a work order to ISS to request access to a former employee's files located in the H drive and in-box.

Recommendations:
7. Departments should disable terminated employee SIM accounts when required.
8. The ISS Department should communicate to departments the procedures to be followed to access files located in a former employee's personal drive and/or inbox.

Finding #5: Departments did not deprovision student intern/seasonal employee SIM accounts immediately when access was no longer required

Condition
Departments that use student intern/seasonal employees did not deprovision their SIM accounts immediately as of their last workday.

Our conversations with representatives for three departments indicated they do not disable student/seasonal employee SIM accounts as of their last day of seasonal work if they anticipate they will return the following year. For one department, access for a student user was deprovisioned 59 business days after the last day worked when deemed they would not return.

One department director indicated they have an agreement with the Human Resources (HR) Department to keep seasonal employees in HRIS if they anticipate they will return the following year; and thus, do not disable their SIM accounts either. An HR Department official confirmed that HRIS accounts for seasonal employees are suspended (and not terminated) after their completion of seasonal work until the following year.

Effect or Risk
Users have access to IT resources when not needed. In addition, unauthorized access creates a vulnerability that could be exploited.

Cause
Due to the volume of seasonal employee users, departments have adopted a practice of not disabling user access at the end of the season if they anticipate they will return the following year. In addition, departments are not aware that a user's login can be temporarily disabled in SIM (without deletion of their account), and that ISS can assist with temporarily disabling multiple users in SIM. Lastly, ISS has not recently offered SIM Training to departments.

Criteria
PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to revoke access to all IT systems and information by terminated employees immediately, and Section 22 System Access, 22.4 Roles and Responsibilities requires departments to promptly notify ISS when users are impacted in a way, which would change their system access privileges. The County's ISS CISO indicated access should be revoked within one business day after an employee terminates without cause, which is not consistent with existing policy.

Recommendations:
9. Departments with students/seasonal employees should temporarily disable (login restricted) their system access as of their last day of seasonal work, and immediately when they terminate.
10. The ISS Department should provide guidance/training to departmental SIM Administrators to ensure they have the knowledge to temporarily disable user access (system-wide login restriction) for students/seasonal employees when they are not actively working.

Finding #6: Thirty-five percent of external users evaluated no longer needed access and were not deprovisioned when required

Condition
External users sponsored (authorized system access) by County departments through SIM were not deprovisioned as required when access was no longer needed as follows:

- Of 43 external users evaluated, 15 (or 35%) were confirmed to no longer need access, although, their SIM account was still active.
- Of 21 departments that sponsored external users, nine (or 43%) had external users with an active SIM account that no longer needed access.
- One department was unaware when the need for user access had expired for its five external users confirmed to no longer need access.

The ISS Senior Manager (SIM Team) indicated SIM allows for an external user's account to be set up with an expiration date, but most of these account types are not set up in SIM with an expiration date.

Effect or Risk

External users have access to County IT resources when no longer needed. In addition, unauthorized access creates a vulnerability that could be exploited or allows information to be obtained or changed in unwanted ways. Lastly, annual licensing fees are paid for users that do not need access.

Cause

Departments do not have procedures to periodically monitor if external users still need access to IT systems. In addition, the majority of external user accounts are not set-up in SIM with an expiration date.

Criteria

PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments to revoke access to all IT systems and information by terminated employees immediately, and Section 15 Network Access, 15.4 Roles and Responsibilities requires departments to promptly report employee or contractor terminations, or other changes in system access. In addition, the County's CISO indicated user access should be removed within one business day of a user terminating, which is not consistent with existing policy.

Recommendations:

11. Departments should immediately deprovision external users that no longer need access.
12. Departments should develop/implement procedures to ensure access for external users are deprovisioned as required when no longer needed. Procedures should include regular monitoring of external user access needs, and setting up external user accounts in SIM (centralized directory) with an expiration date.

Finding #7: Forty-seven percent of external users that no longer needed access were not identified in ISS' annual SIM review

ISS conducts an annual review of active SIM accounts to identify users that no longer require access and need to be deprovisioned.

Condition

From a selection of external users with an active SIM account, we confirmed 15 users no longer needed access; of which, seven (or 43%) no longer needed access prior to ISS' annual SIM review (May 2021). The seven external users that no longer needed access were not identified in ISS' annual SIM review as follows:

- For four external users, the sponsoring departments (two) were not included by ISS in the review
- For three external users, sponsored by three departments, access was not deactivated, nor ISS informed access was no longer needed when solicited

Effect or Risk

External users retain access to County IT resources when no longer needed. In addition, unauthorized access creates a vulnerability that could be exploited, or allows for information to be obtained or changed in unwanted ways. Lastly, annual licensing fees are paid for users that do not need access.

Cause

ISS's annual review (May 2021) did not include all departments with active external user accounts. In addition, departments do not have procedures in place to identify active external users with an expired access need, and to inform ISS of an external user's expired access need when solicited.

Criteria.

PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.3 Policy Provisions requires departments revoke access to all IT systems and information by terminated employees to immediately, and Section 5 Personnel Management, 5.4 Roles and Responsibilities requires departments to immediately request elimination of access authorizations for terminated employees. In addition, the County's CISO indicated user access should be removed within one business day of a user terminating, which is not consistent with existing policy.

Recommendations:

13. ISS annual SIM review should be conducted to detect active external users that no longer need access.

14. ISS should include all departments with active external users in the ISS annual SIM review to ensure external users with an expired access need are detected for prompt deprovisioning

Finding #8: Fifteen percent of SIM User Move Requests for transferred employees were completed after one business day of the Personnel action (PA) effective date

In response to a request, ISS processes a SIM User Move for employees that transfer to another department. Moving an employee's SIM account deprovisions access to the departing department's IT systems linked to a user's SIM account.

Condition
A SIM User Move was completed after one business day of the PA effective date for three of 20 (or 15%) transferred employees, which ranged from two to six business days.

For the three employee SIM accounts moved after one business day of the PA effective date, ISS or the receiving department, and not the departing department, initiated the move request.

Of 20 SIM User Moves completed by ISS, the departing department did not initiate the request for 15 (or 75%) of the moves.

Effect or Risk
A delay in moving an employee's SIM account allows the user to retain access to the departing department's IT systems when no longer needed.

Cause
Departments are not clear on the County's IT Security Policy with regard to departmental roles and responsibilities for removing system access for transferred employees. In addition, PPM CW-O-059 by ISS does not address procedures to follow for removing transferred employee user access. Lastly, ISS training to SIM Administrators has not been received by 50% of the County departments.

Criteria
PPM CW-0-059 "*Information Technology Security Policies,*" Section 22 System Access, 22.4 Roles and Responsibilities requires departments to promptly disable or delete system access for terminated and transferred employees for

systems under departmental control. According to the County's CISO, departments are to ensure user access is removed from IT resources when an employee transfers, with access deprovisioned within one business day, which is not consistent with existing policy.

Recommendations:
15. Requests to transfer a user's access to another department (remove access to IT resources) should be completed within the required timeframe.
16. ISS should develop and provide training to all SIM Administrators on their roles and responsibilities for removing transferred employee user access under the County's IT Security Policy.

Finding #9: Department procedures for deprovisioning user access to department-controlled applications do not provide for removing user access when required

Condition
Current procedures for two departments do not ensure user access is deprovisioned from department-controlled applications that are non-SIM integrated and accessible via internet when required as follows:

- One department director indicated they do not have procedures to notify ISS to remove user access to an outward facing and non-SIM integrated application [ArcGIS].
- One department representative indicated they rely on email notifications from HR, which are often sent after an employee's termination date, to manage user access to an outward facing and non-SIM integrated application [WebEOC].
- Our review of a sample email notification utilized for managing WebEOC access showed it was sent five days after the employee's termination date.

Effect or Risk
Users retains access to departmental resources via the internet when no longer needed.

Cause
Departments are unaware that current procedures do not provide for deprovisioning a terminated user's access within the required timeframe, as one department was unfamiliar with the required timeframes in the County's IT Security Policy, and another department assume all applications are integrated with SIM.

Criteria

PPM CW-0-059 "*Information Technology Security Policies,*" Section 5 Personnel Management, 5.4 Roles and Responsibilities requires departments to immediately review access authorizations for transferred or reassigned employees, and to request elimination of access authorizations for terminated employees. In addition, Section 22 System Access, 22.4 Roles and Responsibilities requires departments to promptly notify ISS when users are transferred, terminated, or otherwise impacted in a way that would change their system access privileges, and to disable/ delete system access for terminated and transferred employees for systems under departmental control.

Recommendations:

17. Department procedures should ensure user access to department-controlled applications are deprovisioned when required.
18. Departments should develop and implement procedures that ensure user access to department-controlled applications are deprovisioned within the required timeframe.

Management Comments and Our Evaluation

In replying to a draft of this audit report, the Chief Information Officer and the Chief Information Security Officer agreed with all nine findings and all 18 recommendations. We agree with their position.

MANAGEMENT AND AUDIT RESPONSIBILITIES

Management is responsible for establishing and maintaining effective internal controls to help ensure that appropriate goals and objectives are met; resources are used effectively, efficiently, and economically, and are safeguarded; laws and regulations are followed; and management and financial information is reliable and properly reported and retained.

Internal Audit is responsible for using professional judgment in establishing the scope and methodology of our work, determining the tests and procedures to perform, conducting the work, and reporting the results.

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Joseph F. Bergeron, CPA, CIA, CGAP
County Internal Auditor
January 11, 2023

BACKGROUND

The Audit Committee requested Internal Audit to conduct a countywide review of departmental user access to IT systems, which was approved under the FY2022 audit work plan.

Based on our initial evaluation of departmental user access to Information Technology (IT) Systems, we narrowed our review to managing user access to both department-controlled applications and to IT resources integrated with the County's Secure Identity Management (SIM) system.

After meeting with ISS management, reviewing department survey results, and evaluating the risks for managing user access to IT systems, we further narrowed our review to departmental deprovisioning of user access (employee and non-employee) in accordance with the County's security policies, which require immediate action upon termination, transfer or reassignment of County personnel.

We determined the highest risk to be a user retaining access to systems after they terminated from the County or transferred to another department, which also included external users retaining access to systems on the County network when no longer needed. We also determined that department-controlled applications that are not integrated with SIM and connected directly to the internet are at higher risk for unauthorized user access if not managed.

The Information Systems Services (ISS) department implemented the SIM system for managing user access to County IT resources. SIM is the County's primary solution for authenticating and authorizing user access to IT systems and resources. SIM provides for single sign-on to integrated systems and the automatic deactivation of access to integrated systems when a user's SIM account is disabled. For IT systems not integrated with SIM, user access is managed separately outside SIM.

The County's ISS SIM Team supports SIM, with departmental SIM administrators, performing day-to-day account management activities, which include deprovisioning user access. The primary methods available to deprovision user access through SIM are: 1.) SIM iManager, 2.) SIM ADEX Service Request, and 3.) SRS Work Order.

The SIM iManager is an administrative interface for managing user accounts and security groups in SIM. Departmental SIM administrators have access to accounts in their own agency. Both a SIM ADEX Service Request and SRS work

order are methods to contact the ISS SIM Team to request that a SIM operation be performed.

ISS implemented a secondary tool to deprovision user access for terminated employees not disabled by one of the primary methods. Through a connector to the HRIS system 'HRIS Connector', SIM picks up terminated employee records to move to a table for deactivation. An employee's status changes to terminated in HRIS only after a fully approved personnel action (PA) form is processed.

Lastly, the ISS SIM Team conducts an annual review of active SIM accounts to identify any users (i.e. external users) that need to be deprovisioned.

AUDIT SCOPE AND METHODOLOGY - GENERAL

The scope of the audit covered departmental deprovisioning of user access to both department-controlled systems and to IT resources integrated with SIM. It included a review of employee personnel actions (PA) [terminated, transferred, and/or reassigned] for 30 County departments with an effective date during the 3-month period from November 1, 2021 to January 31, 2022, as well as active external users as of January 31, 2022.

The 30 County departments included are: Airports, County Administration, County Attorney, Facilities Development & Operations (FDO), Financial Management & Budget (OFMB), Fire Rescue, Information Systems Services (ISS), Tourist Development Council (TDC), Community Services, Office of Equal Opportunity, Human Resources, Medical Examiner's Office, Purchasing, Criminal Justice Commission (CJC), Risk Management, Equal Business Opportunity (EBO), Housing & Economic Dev, Parks, Youth Services, Office of Community Revitalization, Engineering & Public Works, Environmental Resources (ERM), Planning Zoning & Building (PZB), Office of Resilience, County Co-op Extension, Libraries, Palm Tran, Public Affairs, Public Safety, and Water Utilities (WUD).

We conducted our fieldwork from May 2022 through August 2022.

To accomplish our audit objectives, our methodology included:

- Reviewing the County's IT Security Policies and other related ISS PPMs, as well as the National Institute of Security and Technology (NIST) special publication for access control.

- Distributing a preliminary questionnaire (survey) to all County departments to gather information on how they manage user access to IT systems.
- Interviewing the ISS Chief Information Security Officer, and the ISS Senior Manager (SIM Team) to discuss the process for deprovisioning employee/non-employee users in SIM when terminated and/or transferred.
- Evaluating departmental responses for deprovisioning user access for terminated, and transferred employees in SIM and to department-controlled systems. In addition, we interviewed other departmental personal to gather further information.
- Reviewing employee personnel action reports, obtained from both the County and Palm Tran human resources departments, to identify employee terminations, transfers, and reassignments.
- Reviewing reports obtained from ISS to identify active external users and SIM deprovision dates for disabled accounts.
- Randomly selecting non-employee users, across all departments from ISS reports, to verify status with departmental personnel, and to evaluate against ISS' annual SIM review for inclusion.
- Computing deprovisoning timeframes for all terminated employees by comparing the PA effective dates and associated SIM deprovision dates from reports obtained from both HR and ISS.
- Discussing user access deprovisioning delays with departmental SIM administrators and management, as well as with HR and ISS management and personnel.
- Evaluating SIM account user access information (obtained from ISS) for all employee transfers identified in reports obtained from HR.
- Gathering information on departmental applications to ascertain if they are SIM integrated, outward/inward facing, and accessible through the internet for further evaluation.

AUDIT METHODOLOGY – DETAIL BY AUDIT FINDING

Finding #1:

We obtained a Countywide Personnel action Report from PBC Human Resources, and a similar report from Palm Tran Human Resources, which captured all personnel actions (including terminations) during a 3-month period. From these reports, we identified 187 employee terminations for the 3-month period. In addition, we obtained reports from ISS that showed the SIM deprovision dates for terminated employees. Utilizing the information from both the HR and ISS reports, the number of days (calendar, business) between an employee's PA effective date (termination date) and the SIM deprovision date were calculated for each of 187 employee terminations.

From these calculations, we identified those with a SIM deprovision date more than one business day after the PA effective date for further evaluation, which included discussions with the respective departmental SIM Administrators and management, as well as HR and ISS.

Finding #2:

Through a questionnaire combined with discussions with departmental SIM Administrators and management, we gathered information on departmental processes for deprovisioning an employee's SIM account when they terminate from the County.

In addition, when we identified terminations with a SIM deprovision date more than one business day after the PA (termination) effective date, we evaluated the reason for the deprovisioning delays with the respective departments.

Findings #3, 4, 5:

For employee terminations identified with a SIM deprovision date more than one business day after the PA effective date, we evaluated the reason for the deprovisioning delays with the respective departments, as well as with ISS. In addition, we obtained relevant documentation from departmental representatives and ISS.

Finding #6:

We obtained a report from ISS that lists all active SIM accounts from which we identified external users and the sponsoring County departments. We

randomly selected 43 external users from across 21 County departments, and verified with the associated departments if access was still needed. From this information, we identified 15 active external users whose access need had expired.

Finding #7:

For each external user with an expired access need, the expired access date was obtained from the sponsoring department. In addition, the date of the annual SIM review was obtained from ISS, which was compared to the date access no longer needed for each of the 15 external users deem to no longer need access. For the external users with an expired access date prior to ISS' annual SIM review, we had conversations with both ISS and the responsible departments.

Finding #8:

We obtained a Countywide Personnel action Report from PBC Human Resources, and a similar report from Palm Tran Human Resources, that lists personnel actions (including employee transfers) for the 3-month period. From these reports, we identified 20 employees that transferred their SIM account to another department, and for each, obtained the associated 'move date' in SIM from ISS. From this information, we calculated the number of (calendar, business) days from the PA effective date (start date with new department) to the SIM account move date for each employee transfer. In addition, we obtained the documented request for each SIM move from ISS for further evaluation.

Finding #9:

We gathered information through a questionnaire and discussions with departments on department-controlled applications, with an emphasis on those that are not integrated with SIM and are accessible through the internet. For these applications, we had conversations with departmental personal on their procedures for deprovisioning user access when someone terminates and/or makes a change.

ADMINISTRATIVE RESPONSE

Information Systems Services

301 N. Olive Avenue, 8th Floor
West Palm Beach, FL 33401
(561) 355-2823
FAX: (561) 355-3482 (8th Floor)
FAX: (561) 355-4120 (4th Floor)

www.pbcgov.com

Interoffice Memorandum

TO: Joseph F. Bergeron
County Internal Auditor

FROM: Archie Satchell
Chief Information Officer, ISS

DATE: February 6th, 2023

SUBJECT: **ISS Response to Internal Audit Report Titled Countywide IT Systems Access Controls Audit**

A Summary of the audit findings, related recommendations, and ISS' responses are presented below.

Finding 1. Departments Did Not De-provision Terminated Employee SIM Accounts When Required

Audit Recommendation

1. Departments should de-provision an employee's SIM account immediately upon termination

2. The ISS department should train departmental SIM Administrators on the PPM's de-provisioning requirements and on and on the capabilities of SIM (Centralized Directory) to support them.

ISS Response

ISS agrees with the finding and recommendations.

ISS' Additional Comments

SIM training is currently being updated to include an emphasis on the findings. The material and training classes are expected to begin 06/2023

Finding 2. Departments Rely On a Secondary Tool to De-provision Terminated Employee SIM Accounts

Audit Recommendation

1. Departments should de-provision SIM accounts immediately utilizing one of the available direct methods.
2. The ISS Department should develop and provide training to all SIM Administrators on de-provisioning user access, which includes the available methods to disable a user's SIM account within the required timeframe.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

SIM training is currently being updated to include an emphasis on IA findings. The material and additional training classes are expected to begin 06/2023.

Finding #3 - Departmental SIM Administrators were not promptly informed of employee terminations

Audit Recommendations:

1. Department SIM Administrators (or staff tasked to remove user access) should be informed of employee terminations prior to the effective date.

2. Departments should develop procedures to ensure SIM Administrators are informed of employee terminations prior to their effective date.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

ISS will provide SIM admins with ISS internal template for processes/procedures. This template is expected 06/2023.

Finding #4 - Departments change terminated employees' SIM passwords rather than disable the SIM account

Audit Recommendations:

1. Departments should disable terminated employee SIM accounts when required.

2. The ISS Department should communicate to departments the procedures to be followed to access files located in a former employee's personal drive and/or inbox.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

ISS will provide departments with additional procedures to access term employee data. This procedure is expected 03/2023.

Finding #5 - Departments did not de-provision student intern/seasonal employee SIM accounts immediately

Audit Recommendations:

1. Departments with students/seasonal employees should temporarily disable (login restricted) their system access as of their last day of seasonal work, and immediately when they terminate.

2. The ISS Department should provide guidance/training to departmental SIM Administrators to ensure they have the knowledge to temporarily disable user access (system-wide login restriction) for students/seasonal employees when they are not actively working.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

SIM training is currently being updated to include an emphasis on IA findings. The material and additional training classes are expected to begin 06/2023.

Finding #6 - Thirty-five percent of external users evaluated no longer needed access and were not de-provisioned when required

Audit Recommendations:

1. Departments should immediately de-provision external users that no longer need access.

2. Departments should develop/implement procedures to ensure access for external users are de-provisioned as required when no longer needed. Procedures should include regular monitoring of external user access needs and setting up external user accounts in SIM (centralized directory) with an expiration date.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

Although the external users' passwords expire every ninety days, thus disabling access, ISS will provide departments with additional procedures to de-provision external users within the required timeframe by 3/2023.

Finding #7 – Forty-seven percent of external users that no longer needed access were not identified in ISS' annual SIM review

Audit Recommendations:

1. ISS annual SIM review should be conducted to detect active external users that no longer need access.

2. ISS should include all departments with active external users in the ISS annual SIM review to ensure external users with an expired access need are detected for prompt de-provisioning

ISS Response:

ISS agrees with the finding and recommendations

ISS Additional Comment:

Report will be generated and disseminated when ISS conducts its annual true-up audit with occurs June of each year.

Finding #8 – Fifteen percent of SIM User Move Requests for transfer employees were completed after one business day of the Personnel action (PA) effective date

Audit Recommendations:

1. Requests to transfer a user's access to another department (remove access to IT resources) should be completed within the required timeframe.

2. ISS should develop and provide training to all SIM Administrators on their roles and responsibilities for removing transferred employee user access under the County's IT Security Policy.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

SIM training is currently being updated to include an emphasis on IA findings. The material and additional training classes are expected to begin 06/2023.

Finding #9 - Department procedures for de-provisioning user access to department-controlled applications do not provide for removing user access when required

Audit Recommendations:

1. Department procedures should ensure user access to department-controlled applications are de-provisioned when required.

2. Departments should develop and implement procedures that ensure user access to department-controlled applications are de-provisioned within the required timeframe.

ISS Response:

ISS agrees with the finding and recommendations.

ISS Additional Comment:

ISS will notify the departments by 3/2023 of the requirements to have documented procedures for implementation by 6/2023 with ISS providing templates to assist.

AS/as

INTERNAL AUDIT REPORT

FACILITIES DEVELOPMENT AND OPERATIONS (FDO) DEPARTMENT

ELECTRONIC SERVICES AND SECURITY (ESS) DIVISION
SECURITY AND CARD ACCESS (ACCESS) SECTION

CONTRACTORS AND AFTER-HOURS AUDIT

W/P No. 2021-05
Report # 2023-04

INTERNAL AUDIT REPORT

FACILITIES DEVELOPMENT AND OPERATIONS DEPARTMENT (FDO)
ELECTRONIC SERVICES AND SECURITY (ESS) DIVISION
SECURITY AND CARD ACCESS (ACCESS) SECTION
REPORT #2023-04

CONTRACTORS AND AFTER-HOURS AUDIT

TABLE OF CONTENTS

AUDIT OBJECTIVE AND CONCLUSION

We performed this Contractor and After-hours audit to answer the following objective(s):

Did the Division Director ensure internal controls are in place so that access/I.D. cards provide:

1. Authorized access for non-employee vendors/contractors on active County projects;
2. Access is deactivated or rescinded when non-employee vendors/contractors are terminated, transferred, or project is complete;
3. Contractors access is continuously monitored;
4. Contractor and after-hours policies concisely explain the appropriate access levels, monitoring processes, and Departmental expectations.

As to Audit Objective related to Contractors and After-hours Access:

1. Except for the issues found in our testing, controls were in place to ensure non-employee vendors/contractors were authorized to work on active County projects;
2. No controls were in place for ESS to ensure that non-employee contractor access was deactivated or rescinded when non-employee contractor was terminated or project completed;
3. No controls were in place for ESS to ensure that contractor access was continuously monitored;
4. Except for the issues found in our testing related to monitoring processes, controls were in place to ensure contractor and after-hours policies concisely explain the appropriate access levels and Departmental expectations.

FINDINGS AND RECOMMENDATIONS

Finding #1 Project Managers are not ensuring compliance with security policies related to contractors

Project Managers (PMs) are assigned to work with vendors after a contract has been awarded by the county. They create new projects in eFDO (an application where contractor data is entered for the ESS Access Section to use in in their process to manage access), and work with vendors to get their employees (herein called contractors) appointments for Palm Beach County access cards or ID badges. PMs are responsible for picking up contractor badges once they are ready, as well as collecting and returning these badges to ESS once a contractor leaves a project or when the project has been completed. Contractors working in Critical or Criminal Justice Information Services (CJIS) facilities/areas must pass a Criminal History Records Check before starting work; contractors working in CJIS areas are required to be CJIS certified and are placed on a Palm Beach County Sheriff's Office (PBSO) monitoring list for the duration of their involvement with the project.

Condition

Contractor access card/ID badge expiration dates were not tied to relevant contract date; expiration dates of these cards/badges were set to one year from the date they were created regardless of contracted project date. Contractor access cards/ID badges were not returned to ESS at expiration date or when a contractor left a county project. CJIS-certified contractors that no longer worked for county vendors, and should therefore no longer be monitored, were being monitored by PBSO.

See Audit Methodology – Detail by Finding on page 12 for more information on Methodology.

Effect or Risk

When access cards/ID badges are not set to expire at the end of a contract date or are not collected when a contractor leaves a project, there is a risk that cards/badges may be used for unauthorized access. We did not test to determine if there were any instances of unauthorized access. Monitoring CJIS contractors that no longer work for the county results in unnecessary monitoring efforts made by PBSO.

Cause

According to Department Officials, training for project managers on their security responsibilities has not been conducted in several years and the training material has not been update since sometime before 2017.

Criteria

The ESS Access Section Operation Manual states that PMs are responsible for collecting contractor access cards/ID badges and submitting relevant surrender forms to notify ESS when cards/badges expire, projects are completed, or individual contractor termination occurs.

Recommendations:

The Division Director should:

1. Work with project managers to develop processes to:
    a. Tie contractor access cards/ID badges to end of work/contract date.
    b. Periodically request active contractor lists from project managers and compare them to the PBSO monitoring reports to ensure only active county contractors with CJIS certification are monitored.
2. Ensure that project manager responsibilities are clearly defined in countywide PPMs and implement a process to ensure all project managers are trained on required responsibilities.

Finding #2 Courthouse Security Procedures Need Refinement

Departments and Constitutional Offices requesting work to be done by contractors (employees of County vendors) after-hours at facilities which include courthouses must submit a Facilities Access Plan (FAP) work document indicating personnel, materials, tools, and equipment needed for the work prior to the start of each project.

Condition
Of the 27 contractors selected for testing, 22 contractors should have had FAPs on file as they signed into facilities with courthouses. Of the 22, we were provided with FAPs for eight of these contractors.

See Audit Methodology – Detail by Finding on page 12 for more information on Methodology.

Effect or Risk
The Security Management Team was unable to confirm that contractors who performed work without having FAPs on file were authorized to do so by ESS.

Cause
According to Department Officials, training for project managers on their security responsibilities related to facilities access plans has not been conducted in several years and the training material has not been update since sometime before 2017.

Criteria
Countywide PPM CW-L-007 *"After-Hour Access to Palm Beach County Facilities with a Human Security Presence"* (Procedure 1D. After-Hours Access by Contractors/Vendors) requires that Departments or Constitutional Offices submit FAPs to ESS for review and approval before after-hours work by contractors at a facility with a courthouse is initiated.

Recommendations:

3. The ESS Division Director should ensure that security guards confirm and enforce all contractors who sign in to work at courthouse locations have Facilities Access Plans on file with ESS.

4. The ESS Division Director should ensure project managers are trained on required Facilities Access Plan responsibilities.

Finding #3 Security Log Controls Need Improvement

Condition
Contract Security's Contractor, Vendor, & After-hours sign in logs are inconsistent among county buildings. Information on Security sign in logs is illegible and/or incomplete.

See Audit Methodology – Detail by Finding on page 12 for more information on Methodology.

Effect or Risk
Logs that are not complete and/or legible may not be useful to security or to security management team.

Cause
Security Officer Post Orders for two of three buildings selected for testing do not provide guidance as to what information is needed at sign in; Security Officers do not enforce legible and complete entry of information on logs.

Criteria
PPM CW-L-007 "*After-Hour Access to Palm Beach County Facilities with a Human Security Presence*" (Procedure 1D. After-Hours Access by Contractors/Vendors) requires vendors/contractors coming into county facilities with a human security presence to sign in and out on the facility log.

Recommendations:

5. The ESS Director should implement training and monitoring to ensure that Security Officers
    a. review or complete security sign in log entries at the time of individual sign in.
    b. Enforcing legible, complete sign in on logs that Security Officers are able to use in order to determine who is in the building at a particular point in time.

6. The ESS Director should update Post Orders to align with management expectation of security sign in (e.g., Security Officers are able to identify who is in a building in case of emergency using the log), standardize security logs among county buildings, and periodically review completed security sign in logs.

Finding #4 Sensitive Information Collected when not needed by ESS

When a new contract is awarded and requires the vendor's employees (contractors) to be badged, a Contract Evaluator/Project Manager will create a new project in Card Tracking System, available through eFDO. Once completed, information is sent to the vendor that allows them to enter information for individual contractors into the system under the relevant project. Vendors are required to enter specific individual contractor information into this system, including Social Security Number (SSN) and Date of Birth (DOB).

Condition
eFDO requires personally identifiable information (PII) to create a contractor record in order to schedule appointments with ESS. ESS officials stated they do not use PII from eFDO in their processes; Access Staff acquires all necessary information from paperwork that contractors submit when they come in for their background check appointment prior to receiving an access card/ID badge.

See Audit Methodology – Detail by Finding on page 12-13 for more information on Methodology.

Effect or Risk
Collecting PII electronically and in hard copy is a duplication of effort. Collecting PII electronically when it is not required to be collected electronically creates the potential for the electronic information to be accessed by unauthorized persons.

Cause
The eFDO program requires full SSN and DOB in order to create an individual record.

Criteria
PPM CW-O-059 "*Information Technology Security Policies*" (11. Data Security Restricted Information – 11.2 Policy Overview) explains that some categories of data are confidential and exempt from Sunshine Law, such as SSN.

Recommendations:

7. The ESS Director should review the badging process for contractors and determine where PII is needed and will be requested; ensure requested PII is destroyed, deleted, or secured after use.

8. The ESS Director should work with ISS to eliminate or limit the amount of PII needed to schedule a contractor appointment with ESS.

Finding #5 Policies out of date

Condition
PPMs CW-L-007 & FDO-038 were last updated in June 2015. The Access Operations Manual was last updated in 2016. Post Orders for Courthouses were last updated 2014-2015.

See Audit Methodology – Detail by Finding on page 13 for more information on Methodology.

Effect or Risk
Guidance provided in policies is outdated and no longer relevant to current needs.

Cause
Non-compliance with the requirements of PPM CW-O-001 due, at least in part, to management turnover within the Division over the last several years.

Criteria
PPM CW-O-001 "*Policies and Procedures Memoranda (PPMs)*" (Policies - General 4.) state that policies shall be kept current, and that Countywide PPMs must be reviewed at least every five years.

Recommendations:

9. The ESS Director should review and update policies to ensure they match the relevant processes.

10. The ESS Director should implement a process to ensure that policies are reviewed every five years or when actual policies/procedures change, whichever occurs first.

Management Comments and Our Evaluation

In replying to a draft of this audit report, the Department Director agreed with all of the findings and recommendations. We accept management's response without comment.

MANAGEMENT AND AUDIT RESPONSIBILITIES

Management is responsible for establishing and maintaining effective internal controls to help ensure that appropriate goals and objectives are met; resources are used effectively, efficiently, and economically, and are safeguarded; laws and regulations are followed; and management and financial information is reliable and properly reported and retained.

Internal Audit is responsible for using professional judgment in establishing the scope and methodology of our work, determining the tests and procedures to perform, conducting the work, and reporting the results.

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Joseph F. Bergeron, CPA, CIA, CGAP
County Internal Auditor
January 30, 2023

BACKGROUND

Our audit fieldwork consisted of three separate areas within the Access Section's responsibilities: (1) employee access/ID cards, (2) manual keys, and (3) monitoring of contractors and "after-hours" access. Due to the complexity of our audit and diversity of issues, we concluded with the FDO Department Director that we would provide three separate audit reports, one for each area we tested. Our third report (of three) identifies opportunities for improvement in monitoring contractors and "after-hours" access. The first report discusses issues with "*employee access/ID cards*", and the second report examines "*manual keys*" [physical, as opposed to electronic, keys].

The Electronic Services and Security Division (ESS or Division) is part of the Facilities Development & Operations Department. ESS was originally identified as medium risk during the 2019 audit planning process. In 2020, the ESS ranking was upgraded to high risk, based on results provided by management input, financials, and length of time since last audit. The Audit Committee approved the ESS audit for inclusion in the FY2021 audit plan.

Based on our initial evaluation of the Division, we reviewed and identified core operational objectives of ESS's seven sections. Of the seven sections, we narrowed our review to the Security & Card Access section (Section).

After meeting with the ESS Division Director, we met with the Internal Auditor and discussed our impression of the Control Environment, Risk Assessment, and Control Activities. We completed the Matrix columns on "Controls" and "Procedures". We concluded that there are few to no process level controls.

Our Entrance Conference took place on June 22, 2021. Our Audit Planning Memorandum and Audit Program were approved by the Internal Auditor on October 7, 2021. Our fieldwork concluded on August 17, 2022.

The ESS Division is responsible for the County's audio, video recording, fire alarm, security, radio, card access, closed circuit television, and integrated building and jail systems. Its customers include the departments under the Board of County Commissioners, constitutional officers, and other organizations by means of inter-local agreements.

AUDIT SCOPE AND METHODOLOGY - GENERAL

The scope of the audit covered the management and oversight of the ESS Division's Security and Card Access Section. It included a review of the Section's physical access monitoring functions, card access functions, and manual key processes for the period of January, 2021 – August, 2021; after-hours testing was instead conducted for the period of January 1 – March 31, 2022 in order to obtain more current data. We conducted our contractor and after-hours fieldwork both remotely and at the Electronic Services and Securities Division Access Section offices between October 2021 and August 2022.

To accomplish our audit objectives, our methodology included:

- Conducting a risk assessment of the ESS Division's Access Control section.
- Interviewing personnel in ESS, FDO, and ISS to determine the internal controls in place.
- Interviewing the Security Manager.
- Reviewing documentation used in processing contractor access cards and ID badges.
- Evaluating internal controls.

Contractor access cards not being deactivated appropriately, contractors being permitted unescorted access without an ID badge or after annual ID badge expired, and not getting county access cards/ID badges issued to contractors back were all ranked high risk by ESS Management on the "*Business Process Risk, Control and Audit Matrix*" (Risk Matrix).

Our discussions focused on the audit objectives, the associated risks, and ESS controls implemented to mitigate those risks. We considered areas of fraud as they related to our audit objectives and data reliance in our planning and in discussions with the Internal Auditor, ESS Divisional Management, and Access Section staff. We also reviewed and analyzed reports for compliance with Department policies, regulations, and other applicable laws.

AUDIT METHODOLOGY – DETAIL BY AUDIT FINDING

Finding #1: We obtained a list of 1201 non-employee appointments scheduled between January-August 2021; these entries were sorted alphabetically, and Rat Stats was used to select a sample of 60 (5% of the population). Of the 60 contractors sampled, 38 had access cards or ID badges that expired prior to the contract expiration date, 10 had ID badges that expired after the contract expiration date, and 11 did not show up for their appointment, were non-compliant, or did not collect their ID badge. ESS relies on project managers to monitor contracts, collect access cards and ID badges from contractors for return to ESS, and to notify ESS of the need to deactivate contractor access cards. Of 35 CJIS contractors selected for sampling, six contractors who were no longer with PBC vendors were still on the monitoring list with PBSO.

Finding #2: We obtained security sign in logs for January-March 2022 for six county facilities (Government Center Complex, Main Judicial Center, North County Government Center, Vista Center, South County Courthouse, and West County Courthouse), and judgmentally selected a sample of 27 contractors that signed in across these dates and facilities.

Finding #3: We reviewed security sign in logs for January-March 2022 from Government Center Complex, Vista Center, and Main Judicial Center. We compared sign in logs used to directions in Security Officer Post Orders. Each county building with a security officer presence has its own Post Orders, a document which explains both general and building-specific security procedures for the security officer(s) on duty. Government Center Complex and Vista Center Post Orders state that everyone entering after-hours must sign in and out, but do not state what information must be recorded. Main Judicial Center Post Orders include a sign in sheet template, but this does not match what was used by security for sign in. Log errors (illegible entries, incomplete entries, and entries missing information) were observed as follows:

- Government Center: Log errors were observed in 91 of 98 pages.
- Vista Center: Of 612 sign in entries, seven did not include a sign out time, one did not include a security officer name, and nine recorded a time in before a time out.
- Main Judicial Center: Log errors were observed in 60 of 60 pages.

Finding #4: While pulling information for contractor sampling for audit testing related to contractor access card monitoring and deactivation, we observed full social security numbers and birthdates in contractor records within eFDO. Inquiries with Access Section indicated that they do not need this information as they obtain it from paper background check forms obtained

when contractors come in for background checks before being issued an access card or ID badge.

Finding #5: We noted that policies requested related to testing were last revised over five years ago. PPMs CW-L-007 & FDO-038 were last updated in June 2015, the Access Operations Manual was last updated in 2016, and Security Officer Post Orders for Courthouses were last updated in 2014 and 2015.

ADMINISTRATIVE RESPONSE

DATE: February 13, 2023

TO: Joseph F. Bergeron, County Internal Auditor

FROM: Isamí C. Ayala-Collazo, Director
Facilities Development & Operations

SUBJECT: **Response to Final Draft Audit Report** #2023-03
FDO - Electronic Services & Security - Contractors and After-hours Audit

---

The Facilities Development & Operations (FDO) Department, Electronic Services and Security (ESS) Division, has developed the following responses to the findings and recommendations identified in the final draft of audit report #2023-03. As requested, our responses to each one of the ten recommendations follows.

Finding #1
Project managers are not ensuring compliance with policies related to contractors.

Recommendation #1 - The Division Director should work with project managers to develop processes to:

a. Tie contractor access cards/ID badges to end of work/contract date.
b. Periodically request active contractor lists from project managers and compare them to the PBSO monitoring reports to ensure only active county contractors with CJIS certification are monitored.

Recommendation #2 - Ensure that project manager responsibilities are clearly defined in countywide PPMs and implement a process to ensure all project managers are trained on required responsibilities.

Department Response: FDO/ESS agrees with recommendations #1 and 2. ESS will work with project managers to add badge collection as a step prior to project completion/contract end date. In order to successfully achieve project closeout, project managers will be required to collect badges and turn them into ESS. ESS will work with FDO, Capital Improvements Division (CID) to add this additional step to the project closeout checklist. ESS/Access Section will continue to review PBSO monitored contractors and compare to open projects in eFDO. PPM CW-L-033 and CW-L-041 are being revised and will be used to provide refresher training to project managers on roles and responsibilities. PPM revisions and refresher training to be completed by August of 2023

Finding #2
Courthouse security procedures need refinement.

Recommendation #3 - The ESS Division Director should ensure that security guards confirm and enforce all contractors who sign in to work at courthouse locations have Facilities Access Plans on file with ESS.

Facilities Development & Operations Department

2633 Vista Parkway
West Palm Beach, FL 33411

Telephone - (561) 233-0200
www.pbcgov.com/fdo

Recommendation #4 - The ESS Division Director should ensure project managers are trained on required Facilities Access Plan responsibilities.

Department Response: FDO/ESS agrees with recommendations #3 and 4. The facility access plan (FAP) training guide will be updated, adding a quick reference guide for judicial security guards and project managers alike. This training will be conducted by ESS staff for all new judicial security officers and project managers as part of their onboarding. Update to be completed in August of 2023.

Finding #3
Security log controls need improvement.

Recommendation #5 - The ESS Director should implement training and monitoring to ensure that Security Officers:

a. Review or complete security sign in log entries at the time of individual sign in.
b. Enforcing legible, complete sign in on logs that Security Officers are able to use in order to determine who is in the building at a particular point in time.

Recommendation #6 - The ESS Director should update Post Orders to align with management expectation of security sign in (e.g., Security Officers are able to identify who is in the building in case of emergency using the log), standardize security logs among county buildings, and periodically review completed security sign in logs.

Department Response: FDO/ESS agrees with recommendations #5 and 6. ESS will update the post orders to include clear direction on how logbook entries are memorialized. This includes the security officer, not the visitor, writing the information in the logbook both legibly and completely. ESS will ensure all logbooks are consistent throughout each building with a security presence. Updates to be completed in August of 2023.

Finding #4
Sensitive information collected when not needed by ESS.

Recommendation #7 - The ESS Director should review the badging process for contractors and determine where PII is needed and will be requested; ensure requested PII is destroyed, deleted, or secured after use.

Recommendation #8 - The ESS Director should work with ISS to eliminate or limit the amount of PII needed to schedule a contractor appointment with ESS.

Department Response: FDO/ESS agrees with recommendations #7 and 8. ESS will work with ISS to remove electronic requests in eFDO for full social security numbers and replace with the last four digits only. Full social security numbers will only be used on written forms at the time of fingerprint submission and remain stored in the access supervisors office until destroyed. Transition to be completed by August of 2023.

Finding #5
Policies out of date.

Recommendation #9 - The ESS Director should review and update policies to ensure they match the relevant processes.

Recommendation #10 - The ESS Director should implement a process to ensure that policies are reviewed every five years or when actual policies/procedures change.

whichever occurs first.

Department Response: FDO/ESS agrees with recommendations #9 and 10. PPMs CW-L-033 and CW-L-041 are currently under review with a completion date of August 2023. FDO/ESS will ensure adherence to PPM CW-O-001 and the review/revision timeline.

Please feel free to contact us at (561) 233-1447 should you require any additional information regarding this matter.

C: Jimmy Beno, Director, FD&O Operations
Gilbert Morales, Director, FD&O Electronic Services & Security

Attachment #3

INTERNAL AUDIT REPORT

FIRE RESCUE DEPARTMENT

OPERATIONS DIVISION
PLANNING SECTION

PERFORMANCE DATA ACCURACY AUDIT

W/P No. 2021-02
Report # 2023-05

INTERNAL AUDIT REPORT

FIRE RESCUE DEPARTMENT
OPERATIONS DIVISION
PLANNING SECTION
REPORT #2023-05

PERFORMANCE DATA ACCURACY AUDIT

TABLE OF CONTENTS

AUDIT OBJECTIVE AND CONCLUSION

We performed this audit to answer the following objective:

Did the Fire Administrator ensure that the Fire Rescue Operations performance data gathered and reported to the Office of Financial Management and Budget (OFMB) for Fiscal Year 2021 was accurate and reliable according to the OFMB Budget Instruction Manual?

Our conclusion on the objective:

The Fire Administrator did ensure controls were in place to ensure that the Fire Rescue Operations performance data gathered and reported to the Office of Financial Management and Budget (OFMB) for Fiscal Year 2021 was accurate and reliable according to the OFMB Budget Instruction Manual.

Other matters:

During the course of our engagement, we noted certain other minor issues related to Fire Rescue's CAD Review Process and the Disaster Recovery Plan. In our judgment, these issues did not rise to the level of audit findings. We issued a comment letter to Fire Rescue management concerning these issues. While our comment letter provides suggestions for improvement in the areas noted above, the letter is for informational purposes only. We do not conduct any follow-up review on suggestions for improvement made in our management comment letters.

FINDINGS AND RECOMMENDATIONS

There are no findings or recommendations.

MANAGEMENT AND AUDIT RESPONSIBILITIES

Management is responsible for establishing and maintaining effective internal controls to help ensure that appropriate goals and objectives are met; resources are used effectively, efficiently, and economically, and are safeguarded; laws and regulations are followed; and management and financial information is reliable and properly reported and retained.

Internal Audit is responsible for using professional judgment in establishing the scope and methodology of our work, determining the tests and procedures to perform, conducting the work, and reporting the results.

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Joseph F. Bergeron, CPA, CIA, CGAP
County Internal Auditor
February 21, 2023

BACKGROUND

Palm Beach County Fire Rescue is one of the largest Fire Departments in the State of Florida, responding to various emergencies throughout the year. With more than 1700 employees and 49 fire stations, Fire Rescue covers 1769 square land miles serving over 960,000 residents.

Fire Rescue provides a broad range of services including:

- Fire Protection
- Emergency Medical Services,
- ALS/BLS Transport (Advanced and Basic Life Support)
- Hazardous Materials Mitigation
- Special Operations
- Aircraft Firefighting
- 911 Dispatching
- Public Education
- Inspections
- Investigations
- Plans Review
- Community Assistance (CARES) Team
- Mobile Integrated Health (MIH)

The department is further broken down into divisions with each division assigned a portion of the above Fire Rescue services. Operations is responsible for the response to and mitigation of a wide variety of fire and medical emergencies including:

- Conducting suppression activity and/or providing pre-hospital care;
- Responding to hazardous materials incidents;
- Conducting pre-fire planning on all major target hazards;
- Providing a volunteer-based Community Assistance (CARES) Team to offer post-incident assistance such as bereavement, emotion, and social-service support to citizens.

In addition, the Fire Rescue Planning Section is tasked with pulling data from the CAD system using Crystal Reports (CR) for various daily, monthly, quarterly and yearly reports. The reports are provided to the chiefs and the different municipalities. Other reports are for the Annual Report and information for the Board.

We reviewed a sample of available reports, requesting only the ones needed for our program. They included:

- Palm Beach County Fire Rescue (PBCFR) # of Calls
- FY21 Palm Beach County Public Safety Report- Call Summary
- FY21 Not Available Report

- PBCFR Turnout- & over 1 minute 30 seconds
- PBCFR Response Time Average FY21
- AVL (Automatic Vehicle Locator) logs
- Station At a Glance

AUDIT SCOPE AND METHODOLOGY - GENERAL

The scope of the audit included a review of the procedures and the controls implemented in the process of capturing, reviewing, verifying, and reporting the performance measures for the period of October 1, 2020 – September 30, 2021. Our scope was limited to activities within the Fire Rescue Legal Service Area (LSA). The LSA includes the unincorporated County and 19 municipalities. Fire Rescue also provides dispatch services for 13 additional municipalities. We did not include the services for the 13 municipalities in our scope. In addition, for some of our steps we were not able to review data between October 1, 2020 and June 30, 2021, as Fire Rescue did not retain the information.

Our methodology included interviewing key personnel at Fire Rescue. We met with management and staff at Fire Rescue involved in the emergency response incident data verification and reporting. We also reviewed the methodology used to verify and report performance data of emergency response incidents. We reviewed the controls implemented in the verification and reporting of performance data of emergency response incidents.

We reviewed sample transactions of the following data within the above named reports for:

- Missing received time
- Duplicate event numbers
- Turnout Time
- Availability of first due units
- Total Response Time for PBCFR legal service areas
- Review and justification of any exceptions

Lastly, we referred to the Government Accounting Office's (GAO) *"Internal Control Management & Evaluation Tool.*