Audit of the Parking Access Revenue Control System at Port Everglades

Office of the County Auditor

Audit Report

Robert Melton, CPA, CIA, CFE, CIG
County Auditor

Audit Conducted by:
Kathie-Ann Ulett, CPA, CFE, Deputy County Auditor
Gerard Boucaud, CIA, CISA, CDPSE, Audit Manager
Luis Martinez, CISA, CFE, CDPSE, Audit Supervisor
Samuel Josepher, CPA, CIA, Audit Senior

Report No. 24-13
March 6, 2024

OFFICE OF THE COUNTY AUDITOR
115 S. Andrews Avenue, Room 520 • Fort Lauderdale, Florida 33301 • 954-357-7590 • FAX 954-357-7592

March 6, 2024

Honorable Mayor and Board of County Commissioners

Pursuant to the fiscal year (FY) 2022-2023 Annual Audit Plan, we conducted an audit of the Parking Access Revenue Control System (PARCS) at Port Everglades (Port).

Our audit objectives were to determine whether the Port is adequately managing the PARCS contract to ensure that TIBA Parking Systems, LLC (TIBA) maintains compliance with key contract requirements and whether Information Technology (IT) general and application controls effectively support the confidentiality, integrity, and availability of PARCS.

We conclude that, except as noted in this report, Port is adequately managing the PARCS contract to ensure that TIBA maintains compliance with key contract requirements. We conclude IT general and application controls do not effectively support the confidentiality, integrity, and availability of PARCS. Opportunities for Improvement are included in the report.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient and 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.

Our work on this project was limited by TIBA's lack of providing repeatedly requested information. As a result of these limitations, we were unable to fully evaluate all issues within the scope of our review. This report includes recommendations based on the evidence we were able to obtain as well as recommendations for TIBA to provide additional information to Port Management.

We appreciate the cooperation and assistance provided by the Port's Operations Division throughout our audit process.

Respectfully submitted,

Bob Melton
County Auditor

cc: Monica Cepero, County Administrator
Andrew Meyers, County Attorney
Kimm Campbell, Deputy County Administrator
Michael Ruiz, Assistant County Administrator
Glenn Wiltshire, Interim Director, Port Everglades

TABLE OF CONTENTS

INTRODUCTION

Scope and Methodology

The County Auditor's Office conducts audits of Broward County's entities, programs, activities, and contractors to provide the Board of County Commissioners, Broward County's residents, County management, and other stakeholders, unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

Pursuant to the fiscal year (FY) 2022-2023 Annual Audit Plan, we conducted an audit of the Parking Access Revenue Control System (PARCS) at Port Everglades (Port). Our audit objectives were to determine whether:

1. Port is adequately managing the PARCS contract to ensure that TIBA Parking Systems, LLC (TIBA) maintains compliance with key contract requirements.
2. Information Technology (IT) general and application controls effectively support the confidentiality, integrity, and availability of PARCS.
3. Opportunities for improvement exist.

Our audit included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was October 1, 2022, through September 30, 2023. However, transactions, processes, and situations reviewed were not limited by the audit period.

To determine whether the Port is adequately managing the PARCS contract to ensure that TIBA maintains compliance with key contractual requirements, we interviewed appropriate personnel, performed an observation of PARCS, and inspected documentation and transactions to evaluate managements' oversight of the PARCS contract. Not all information requested was made available.

To determine whether IT general and application controls effectively support the confidentiality, integrity, and availability of PARCS, we reviewed policies and procedures governing physical and logical security, change management, and backup and recovery. We observed the physical controls around PARCS for adequacy and obtained evidence to support the logical access controls in place for PARCS. We also made inquiries with management and

the vendor regarding system hardening, backup and recovery and privileged access. Not all information requested was made available.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient and 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.

Our work on this project was limited by TIBA's lack of providing repeatedly requested information. As a result of these limitations, we were unable to fully evaluate all issues within the scope of our review. This report includes recommendations based on the evidence we were able to obtain, as well as recommendations for TIBA to provide additional information to Port Management.

Our audit included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was October 1, 2022, through September 30, 2023. However, transactions, processes, and situations reviewed were not limited by the review period.

Overall Conclusion

We conclude that, except as noted in this report, Port is adequately managing the PARCS contract to ensure that TIBA maintains compliance with key contract requirements. We conclude IT general and application controls do not effectively support the confidentiality, integrity, and availability of PARCS. Opportunities for Improvement are included in the report.

Background

The parking facilities at the Port provide nearly 4,000 parking spaces, primarily for cruise ship passengers. In 2020 the County entered into an agreement with TIBA Parking Systems, LLC (TIBA) to provide all necessary equipment, software, and services, including ongoing support and maintenance, for a comprehensive Parking Access Revenue Control System (PARCS) solution. PARCS includes electronic gates, license plate readers, parking machines and pay-on-foot stations that integrates with a credit card merchant to collect revenues which are remitted to the County. PARCS also includes the software that allows the Port to monitor parking transactions and control the parking equipment.

In addition to the agreement with TIBA, the County entered a contract with SP Plus Corporation (SP Plus) to provide parking management services for all parking operations at the Port including the PARCS equipment and software provided by TIBA.

The Port's Contract Administrator is responsible for broad oversight over the parking operation, working closely with both TIBA and SP Plus to ensure contract requirements are being met and that the operation is managed effectively. The Contract Administrator's responsibilities include monitoring PARCS to ensure it is in working order, escalating any unresolved issues to TIBA, ensuring that revenue is collected, and reports are sent to Port's Finance Division daily, and managing access to PARCS.

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. Contract Administration of the TIBA Agreement Should Be Enhanced

Oversight of services provided by TIBA requires enhancement. During our review, we identified three areas where oversight can be enhanced. Specifically:

A. Management does not analyze transaction reports for unusual activity related manual overrides. Management generates "Daily Reports" that capture manual overrides and changes made to fees; however, these reports are not reviewed for unusual transactions. While the ability to perform high-risk transactions in PARCS is limited by the principle of least privilege and adequately segregated, high-risk transactions should be periodically monitored for appropriateness. Monitoring acts as both a deterrent and a detective control. Without periodic monitoring of high-risk activity, erroneous and(or) inappropriate activity may remain undetected.

B. Management does not evaluate whether system support and maintenance response time requirements are consistently being met in accordance with the contract. Page 56 of 105 of the County's agreement with TIBA states;

> *"At the request of County, Provider shall provide monthly reports of the foregoing records as well as statistics of Provider's average monthly compliance with the Required Response Times.*
>
> *<u>Failure to Meet Required Response Times.</u> If Provider fails to meet the Required Response Times, County may offset against any sums due Provider up to 25% for each hour that Provider's average response time in the preceding month exceeds the Required Response Times."*

Additionally, the agreement requires the Provider to maintain records of its Support and Maintenance Services and provide the County with online access to an Event ticketing system.

Although oversight over support and maintenance services is adequate in ensuring that the PARCS system is working as expected; enhancements can be made to ensure that TIBA is providing timely service in accordance with their contract. Without adequate monitoring of TIBA's support and maintenance services, management is unable to determine whether TIBA resolves issues within their contractually required response times and is also unable to take remedial action against TIBA, such as offsetting sums owed to TIBA for poor performance. During our audit, management requested the support and maintenance services reports from TIBA. TIBA did not provide the reports and was unresponsive to the request.

C. The County does not have access to the PARCS server and has not identified user roles and the corresponding level of access required to monitor TIBA's compliance with their contractual requirements.

As stated in the contract with TIBA, Exhibit A, Section C- Statement of Work:

> *"Certain users will be required to have access to the server. As part of Provider's onsite analysis and critical design review, County will identify user roles and the corresponding level of server access required per role and Provider will, as part of its final configuration of the server, incorporate such roles and access levels. Provider is solely responsible for the server, including applying patches and updates to the server."*

The County should have server access to ensure PARCS server is adequately secured. Per County Administrative Policies and Procedures (CAPP) ETS Volume 7, Chapter 3, section 2.1.C, server security measures apply to *"All server equipment, that is owned, operated, or leased by the County, or registered under a County-owned internal network domain."*

Without server access, the County is not be able to ensure that TIBA is applying patches and updates to the server as required and are unable to monitor the performance of the server. Additionally, the County does not have the ability to detect whether the security logs they receive, or underlying transactional data pulled by the reports the Port uses to reconcile transactions have been altered.

We recommend management:

A. Implement procedures to periodically monitor high risk transactions for appropriateness. High risk transactions may include setting prices, adjusting parking fees or unusual activity related to parking validation or proximity card usage.

B. Evaluate whether system support and maintenance response time requirements are consistently being met in accordance with the contract.

C. Identifies user roles and the corresponding level of server access required to monitor relevant activity on PARCS servers. Ensure TIBA creates and grants the County access to these roles and develop standard operating procedures that allow them to effectively monitor key activities that may include patch management and parking transactions.

2. Security Assessments for PARCS and its Network Have Not Been Performed

We noted that PARCS and its network have not been subject to security assessments required by County Administrative Policies and Procedures and the County's contract with TIBA Parking Systems, LLC (TIBA). Specifically, we noted the following assessments have not been performed:

A. Vulnerability Assessments - Security assessments are required by the County Administrative Policies and Procedures (CAPP). Volume 7, Chapter 3, Section 8.1, F states:

> *"All new or modified applications are required to be scanned for vulnerabilities prior to promotion to production."*

B. Payment Card Industry Data Security Standard (PCI DSS) Assessments – The County is required to comply with payment card industry whenever accepting credit Card payment. In addition, Exhibit I of the County's agreement with TIBA Exhibit I requires that:

> *"annually the Provider shall provide to County: A copy of their Annual PCI DSS Attestation of Compliance ("AOC")."*

Failure to perform scans and security assessments hinders management's ability to identify, assess, and remediate risks to the County's information infrastructure in a timely manner. Failure to perform assessments to ensure PCI DSS compliance may lead to substantial fines per incident should a breach occur as well as additional costs and reputational damage resulting from notification requirements.

We recommend management:

A. Perform vulnerability assessments of PARCS and its network as required by the County Administrative Policies and Procedures.

B. Perform PCI DSS Assessments of PARCS and its network by either enforcing contractual requirements within the TIBA contract or performing an independent assessment and seeking legal remedies from TIBA for lack of compliance with contract terms.

3. Physical Security Controls Require Enhancement for PARCS and its Network.

During our review, we noted the following components which require improvement to align with Volume 7, Chapter 3 of CAPP and industry best practices:

A. Physical access management procedures are informal. Access changes are informally communicated between SP Plus staff and the Contract administrator which increase the risk of error. For example, the Contract Administrator informed us that during the monthly employee payroll review, if staffing changes are noted, access will be revoked, where appropriate. However, during our review we noted that for one of the two (50%) employees terminated during the audit period, management did not immediately revoke physical access to the Parking Office by changing the keypad code to the Parking Office. The keypad code securing access to the Parking Office was changed approximately 54 days after employee termination.

> *Section 13.2.e requires that the responsible agency must authorize access to the data center by submitting an Access Request Form. County access request forms require management to define the access being requested, a justification for the access and requires multiple levels of authorization to formally approve access prior to it being granted.*
>
> *Section 13.2.H, requires that, "Access rights to secure areas should be revoked immediately for personnel who were terminated or who no longer require access. Combinations to locks must be changed."*

Lack of formal access management procedures may increase the risk of inappropriate access.

B. A permanent log is not used to record all individuals accessing the server room.

> *"Section 13.2.C states that "Individuals accessing a data center must present a government issued or employer photo ID, have their name, date, time of entry and departure recorded in a permanent log and observe all local security measures of the facility."*

Insufficient monitoring controls (entry log and integrated cameras) increase the probability that inappropriate access may go undetected.

C. Physical Keys and Keypad codes are used without adequate monitoring controls. During our review, we noted the following:

   i. The Parking Office and server room door are secured by a keypad and physical key, respectively. While keypads and physical keys provide a layer of security, keypad codes are easily shared, and physical keys are easily replicable which weakens security. As a result of these weaknesses, physical keys and keypads require additional controls, such as camera surveillance (See ii below), to ensure effective monitoring over access to the server room in line with industry best practices.

   ii. While cameras have been deployed in the server room, they are not integrated as part of an intrusion detection solution that would compensate for the monitoring control weakness inherent with physical keys (See i above). Camera footage is currently archived and only reviewed if an incident has occurred. To detect unauthorized or inappropriate activity timely, the camera footage would have to be monitored continually in line with industry best practice.

D. The PARCS server is not physically secured by a locked rack as required by CAPP. The server rack panels, and door were disassembled.

   Section, 13.2.G states that, "All servers, storage, backup, remote access switches, networking and security equipment racks must be physically secured within locked racks or cages."

   Failure to properly secure PARCS servers may increase the risk of unauthorized access adversely impacting confidentiality, integrity, and availability of the system and its network.

We recommend management:

A. Establish a formal procedure to authorize, modify and revoke physical access to the PARCS facility using access request forms consistent with the CAPP. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

B. Implement a permanent log designed to track the name, date, time of entry and departure into the server room.

C. Consider the implementation of a key card entry system to the server room or implement a stronger combination of physical security controls designed to detect, notify, and monitor access to PARCS servers. Improvements may include the implementation of intrusion detection devices such as smart cameras and motion sensors.

D. Ensure PARCS servers are physically secured within locked racks or cages.

4. Policies and Procedures Should be Established to Ensure Environmental Security Controls Are Adequate for Server Rooms and Data Centers.

Countywide policies and procedures outlining baseline environmental security controls over server rooms and data centers have not been established. Through inquiry with Enterprise Technology Services (ETS) and Facilities Management (FMD) divisions, we noted that baseline environmental controls for server rooms and data centers have not been established.

Further, while overall, we noted that Port management implemented reasonable environmental controls to protect PARCS, we were unable to obtain evidence that the environment had been approved by ETS consistent with CAPP Volume 7, Chapter 3, Section 2.2.H.p requiring that:

> *"Servers must be physically located in a secure, access controlled ETS approved environment."*

The National Institute of Standards and Technology's ("NIST") Physical and Environmental Security Handbook identifies key control areas that should be considered to protect systems from their physical environment. The handbook discusses key areas of environmental security, including fire safety, supporting utilities such as air-conditioning, and plumbing leaks.

Without a baseline, the PARCS physical environment (as well as other County IT environments) may not be setup consistently to mitigate the risks related to the physical environment. IT systems may be exposed to an increased risk related to inappropriate temperatures, fire hazards, and water damage.

We recommend County Administration establish baseline environmental control requirements for server rooms/or data centers for inclusion in the CAPP and ensure that server rooms and/or data centers are evaluated and approved by ETS.

5. Logical Access Controls Require Enhancement for PARCS and its Network.

During our review, we noted the following components which require improvement to align with Volume 7, Chapter 3 of CAPP, and industry best practices:

A. Management does not have a formal procedure in place to authorize access to the PARCS Application. While the informal process is reasonable and is being followed, management should develop formal policies and procedures should be formally documented and distributed throughout the organization to ensure that they are followed consistently. Without a formal process, access may not be consistently provisioned.

B. The PARCS application account and password security controls do not comply with the CAPP Volume 7, Chapter 2, Section 7.1. During our review we noted that the application allowed users to create single character passwords. The Contract Administrator informed us that they were unaware of any configuration settings within the application that allowed minimum password requirements to be strengthened. Repeated attempts were made to TIBA to determine whether the system had the capability to require complex passwords and additional security settings consistent with the CAPP; however, no response has been received to date. Without strong password and account security requirements, the PARCS application is not compliant with County minimum security requirements increasing the risk of inappropriate or unauthorized access.

C. The user access review process is not formal and is not adequately designed to ensure that access to PARCS remains commensurate with user job responsibilities. The Contract Administrator performs a user access review monthly; however, this review is designed to detect changes in the vendor's employee payroll list which is included in the vendor's invoice. If the Contract Administrator detects that an employee from the previous payroll is no longer included on the current file, access is revoked. The review does not evaluate whether each user's access aligns with the authorized access requested and that each user continues to require the access granted based on job responsibilities.

   CAPP Volume 7 Chapter 2, Section 7.1 includes the following user access review requirement:

> *"All user access rights must be reviewed for accuracy by the agency Security Point of Contact (SPOC) and the data owner to determine if the access rights are correct or must be revised or revoked. Access rights include physical, network, server, and application privileges."*

Access review procedures should be formally documented and distributed throughout the organization to ensure they are consistently followed and allow for continuity of operations when organizations experience turnover in key positions. Without formal and appropriately designed access review procedures, inappropriate or unauthorized user access may remain undetected, increasing the risk of unauthorized activity.

We recommend management:

A. Establish a formal procedure to authorize, modify and revoke logical access to PARCS. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

B. Work with the vendor to implement account and password security controls for PARCS consistent with the CAPP.

C. Establish formal procedures to review user access to ensure that access rights remain commensurate with user job responsibilities. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

6. PARCS Updates Are Not Tested by Management Prior to Promotion to Production

During our review, we noted the following components which require improvement to align with Volume 7, Chapter 3 of CAPP, and industry best practices:

A. Management has not established formal change management procedures to ensure consistency and alignment with the CAPP.

B. PARCS system updates and software releases are not tested prior to promotion to production. In addition, we were unable to determine whether testing environments where changes can be evaluated prior to implementation have been established due to a lack of response from TIBA after repeated attempts.

CAPP, Volume 7, Chapter 3, Section 9, includes requirements to ensure software releases are adequately planned, tested, and signed off by appropriate parties prior to their promotion to

production environments. These requirements include testing software updates in non-production environments to ensure that any new features perform as expected, and existing functionality on County systems and in the County's environment is not impacted by the new release.

Management has taken some measures to reduce risk, such as making sure software updates are not scheduled for release on high traffic days to limit business disruptions related to software deployments; however, failure to establish formal change management policies and test software updates has led to business disruptions. For example, we were informed by management that the PARCS system received a software release that was deployed directly to production without testing. This release caused an operational disruption that impeded management's ability to pull reports from the application for each parking location. The issue persisted for three weeks until a correction was implemented.

We recommend management:

A. Establish a formal procedure to manage software releases and updates to PARCS consistent with CAPP. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

B. Ensure that software is tested in an environment separate from production.

7. Backup and Recovery Policies Have Not Been Developed

We noted that Port Management has not developed a backup and recovery strategy plan for PARCS that establish key business requirements including maximum acceptable data loss during network / system downtown, the maximum tolerable amount of time that can pass before system outages seriously impede normal business operations, and annual testing to ensure data files and programs can be recovered. Additionally, we were unable to obtain information regarding the implementation of backup and recovery schedules covering the Port's PARCS systems due to a lack of response from TIBA after repeated attempts.

Per County Administrative Policies and Procedures (CAPP) ETS Volume 7, Chapter 3, Section 14 includes backup and recovery requirements which include but are not limited to the following:

- Backup strategy plans are required of every agency, including enterprise agencies, with testing schedules.

- Procedures for recovery and restoration of backed up systems and data must be documented.

- ❖ Annual testing must be performed to ensure data files and programs can be recovered.

- ❖ Off-site storage sites must be secure locations distant from the primary data center.

Without policies and procedures governing backup and recovery, system backups schedules may not be in alignment with the Port's business requirements. This increases the chance that management may lose an unacceptable amount of data and/or experience a business disruption that seriously impedes the normal business operation.

We recommend management:

A. Develop a backup and recovery strategy plan designed to minimize the operation impact in the event of an incident affecting PARCS systems. Backup and recovery strategy plans should establish the maximum acceptable data loss, maximum amount of tolerable downtime before operations are impacted and annual testing to ensure data files and programs can be recovered. The backup and recovery strategy plan should be in alignment with CAPP requirements.

B. Work with the vendor to verify that PARCS backup and recovery policy and procedures are implemented in alignment with their strategic plan and that any relevant technical requirements established by the CAPP are followed.

8. The Vendor Was Not Responsive to Port Management's Requests for Information.

During the audit, Port management was unable to obtain information from the vendor that addressed various aspects of operational risk relevant to our audit. As a result, management is unable to assess whether adequate controls are in place to safeguard the Port's parking operations and transactional data upon which they rely for revenue. In addition, we were unable to perform our audit analysis to the extent planned as described throughout this report in various sections above.

TIBA is contractually obligated to respond to information requests from Port management, which include audit requests. The County's general right to audit is detailed in the TIBA agreement:

> *"Provider and its subcontractors shall preserve and make available, at reasonable times within Broward County for examination and audit by County, all financial records, supporting documents, statistical records, and any other documents pertinent*

to this Agreement for a minimum period of three (3) years after expiration or termination of this Agreement or until resolution of any audit findings, whichever is longer. County audits and inspections pursuant to this section may be performed by any County representative (including any outside representative engaged by County). County reserves the right to conduct such audit or review at Provider's place of business, if deemed appropriate by County, with seventy-two (72) hours' advance notice."

We recommend management work with the County Attorney to evaluate remedies for non-compliance with contract terms. In addition, we recommend management evaluate the risk created by a lack of information related to the scope of services provided by the vendor and take appropriate action.

MANAGEMENT'S RESPONSE

Michael W. Ruiz, Assistant County Administrator
115 S. Andrews Avenue, Room 409 • Fort Lauderdale, Florida 33301 • 954-357-7333 • FAX 954-357-7360

MEMORANDUM

DATE: March 5, 2024

TO: Robert Melton, County Auditor

FROM: Michael W. Ruiz, Assistant County Administrator Michael W. Ruiz

RE: Management Response to County Auditor's Report on Audit of the Parking Access Revenue Control System at Port Everglades

---

The Port Everglades Department has reviewed the Office of the County Auditor's Report on the Audit of the Parking Access Revenue Control System (PARCS) at Port Everglades and submits the following as Management's response.

In summary, Management concurs with the Auditor's overall conclusion that additional controls are required to address Information Technology (IT) general and application controls for the PARCS contract with TIBA Parking Systems, LLC (TIBA). The Port Everglades Department has implemented additional controls as further noted in the Management Response and will continue working on other improvements with the assistance of the Enterprise Technology Services (ETS) division.

Importantly, the Port acknowledges that the contract in question holds TIBA to the same standards as a County department, with respect to information technology, servers, applications, and security. Therefore, the distinctions commonly made in County Administrative Policies and Procedures (CAPP) between County-controlled systems versus vendor-controlled systems, do not apply. In such cases, based on the TIBA contract language, TIBA is held to the CAPP standard as if it were a County entity.

Detailed responses to the Opportunities for Improvement and Recommendations noted in the Auditor's report begin on page two.

Opportunity for Improvement 1 (OFI 1): Contract Administration of the TIBA Agreement Should Be Enhanced.

Recommendation A: Implement procedures to periodically monitor high risk transactions for appropriateness. High risk transactions may include setting prices, adjusting parking fees or unusual activity related to parking validation or proximity card usage.

Recommendation B: Evaluate whether system support and maintenance response time requirements are consistently being met in accordance with the contract.

Recommendation C: Identify user roles and the corresponding level of server access required to monitor relevant activity on PARCS servers. Ensure TIBA creates and grants the County access to these roles and develop standard operating procedures that allow them to effectively monitor key activities that may include patch management and parking transactions.

Management's Response to OFI 1

A. Management concurs: The Port's parking management contractor, SP Plus, reviews the daily reports for unusual transactions, but their Standard Operating Procedures are being modified to ensure that they alert the Port's Project Manager if any unusual transactions are identified. In addition, Port staff have implemented a review of the TIBA monthly reports and parking management monthly reconciliation reports. The Project Manager will compare reports and follow up on any unusual activity with upper management.

B. Management concurs: Port staff has created and will maintain a log listing details of service calls and tracking response times. The Project Manager is working with the County Attorney's Office to address additional steps to ensure TIBA complies with the contract provisions.

C. Management concurs: TIBA has provided the Port Project Manager with a User ID and password for County staff to gain access to the server. The Project Manager will work with TIBA to establish the Standard Operation Procedures to access and monitor appropriate activities on the PARCS server.

Opportunity for Improvement 2 (OFI 2): Security Assessments for PARCS and its Network Have Not Been Performed

Recommendation A: Perform vulnerability assessments of PARCS and its network as required by the County Administrative Policies and Procedures.

Recommendation B: Perform PCI DSS Assessments of PARCS and its network by either enforcing contractual requirements within the TIBA contract or performing an independent assessment and seeking legal remedies from TIBA for lack of compliance with contract terms.

Management's Response to OFI 2

A. Management concurs: The Responsibility Matrix in the contract with TIBA provides that TIBA will perform internal vulnerability scans of network components that are being managed by the vendor on the PARCS segment of the network. Port IT staff will work with ETS to perform a vulnerability scan on the County-managed network environment as required by the County CAPP.

B. Management concurs: The Project Manager is working with the County Attorney's Office to address additional steps to ensure TIBA complies with PCI requirements as outlined in the Responsibility Matrix in the contract.

Opportunity for Improvement 3 (OFI 3): Physical Security Controls Require Enhancement for PARCS and its Network.

Recommendation A: Establish a formal procedure to authorize, modify and revoke physical access to the PARCS facility using access request forms consistent with the CAPP. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

Recommendation B: Implement a permanent log designed to track the name, date, time of entry and departure into the server room.

Recommendation C: Consider the implementation of a key card entry system to the server room or implement a stronger combination of physical security controls designed to detect, notify, and monitor access to PARCS servers. Improvements may include the implementation of intrusion detection devices such as smart cameras and motion sensors.

Recommendation D: Ensure PARCS servers are physically secured within locked racks or cages.

Management's Response to OFI 3

A. Management concurs: Port staff has implemented a Standard Operating Procedure for facility access.

B. Management concurs: Port staff has implemented a sign-in log for access to the server room.

C. Management concurs: A video camera has been installed in the server room to monitor the room, detect any movement, and notify the Parking Management contractor, SP Plus if the room is accessed. This is in addition to the physical key and sign-in log required to access the server room. SP Plus will have it connected to the Internet within 90 days to provide access monitoring.

D. Management concurs: Port staff has connected all but one panel to the locked rack. The one exception is the panel on the back of the rack, against the wall, which provides insufficient space for installation. The Project Manager will work with ETS to ensure the network room meets ETS specifications.

Opportunity for Improvement 4 (OFI 4): Policies and Procedures Should be Established to Ensure Environmental Security Controls Are Adequate for Server Rooms and Data Centers.

Recommendation A: We recommend County Administration establish baseline environmental control requirements for server rooms and/or data centers for inclusion in the CAPP and ensure that server rooms and/or data centers are evaluated and approved by ETS.

Management's Response to OFI 4

A. Management concurs: County staff will work with ETS to review, establish, update, and verify that environmental standards for server rooms/data centers, including those of the Port, meet the operational and security needs of the County.

Opportunity for Improvement 5 (OFI 5): Logical Access Controls Require Enhancement for PARCS and its Network.

Recommendation A: Establish a formal procedure to authorize, modify and revoke logical access to PARCS. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

Recommendation B: Work with the vendor to implement account and password security controls for PARCS consistent with the CAPP.

Recommendation C: Establish formal procedures to review user access to ensure that access rights remain commensurate with user job responsibilities. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

Management's Response to OFI 5

A. Management concurs: Port staff has implemented a Standard Operating Procedure and created an access form to document system access requests.

B. Management concurs: Port staff has implemented a Standard Operating Procedure for password requirements and password privacy since the TIBA system does not provide password restrictions meeting County requirements.

C. Management concurs: Port staff has implemented a Standard Operating Procedure that includes the Project Manager reviewing employee access lists and roles each quarter.

Opportunity for Improvement 6 (OFI 6). PARCS Updates Are Not Tested by Management Prior to Promotion to Production

Recommendation A: Establish a formal procedure to manage software releases and updates to PARCS consistent with CAPP. These procedures should include the retention of documentary evidence demonstrating the performance of this activity.

Recommendation B: Ensure that software is tested in an environment separate from production.

Management's Response to OFI 6

A. Management concurs: The Responsibility Matrix in the contract requires TIBA to comply with change management procedures relating to PCI compliance. The Project Manager will follow up with TIBA to develop and implement the required procedures.

B. Management concurs: The Project Manager will pursue options with TIBA and SP Plus to comply with PARCS system changes and network updates relating to PCI requirements as outlined in the contract Responsibility Matrix. Vendor will be asked to provide evidence of software testing prior to deployment.

Opportunity for Improvement 7 (OFI 7). Backup and Recovery Policies Have Not Been Developed

Recommendation A: Develop a backup and recovery strategy plan designed to minimize the operation impact in the event of an incident affecting PARCS systems. Backup and recovery strategy plans should establish the maximum acceptable data loss, maximum amount of tolerable downtime before operations are impacted and annual testing to ensure data files and programs can be recovered. The backup and recovery strategy plan should be in alignment with CAPP requirements.

Recommendation B: Work with the vendor to verify that PARCS backup and recovery policy and procedures are implemented in alignment with their strategic plan and that any relevant technical requirements established by the CAPP are followed.

Management's Response to OFI 7

A. Management concurs: Within the next 90 days, the Project Manager will work with TIBA to establish an offsite backup solution to minimize any data loss and create a recovery strategy plan.

B. Management concurs: After the backup and recovery strategy plan is completed, the Project Manager will provide, review, and implement the plan with TIBA and SP Plus.

Opportunity for Improvement 8 (OFI 8). The Vendor Was Not Responsive to Port Management's Requests for Information.

> Recommendation A: We recommend management work with the County Attorney's Office to evaluate remedies for non-compliance with contract terms. In addition, we recommend management evaluate the risk created by a lack of information related to the scope of services provided by the vendor and take appropriate action.

Management's Response to OFI 8

> A. Management concurs: The Port's Project Manager made a number of informal requests to TIBA for information related to the audit, but they were not responsive to the requests. Port staff is working with the County Attorney's Office to review the findings and recommendations in the audit and any other contract non-compliance issues to prepare a formal notice to TIBA.

Thank you again for the opportunity to provide Management's comments. Should you have any questions, please do not hesitate to contact me or Glenn Wiltshire, Interim Director of Port Everglades.

cc: Monica Cepero, County Administrator
Kimm Campbell, Deputy County Administrator
Kevin Kelleher, Assistant County Administrator
Glenn Wiltshire, Interim Director, Port Everglades
Andrew J. Meyers, County Attorney
Kathie-Ann Ulett, Deputy County Auditor
Gerard Boucaud, Audit Manager