

INTERNAL AUDIT REPORT

Operational Audit
Recovery Effort – Data Integrity - Maritime

August 2024 - August 2025

Issue Date: December 4, 2025
Report No. 2025-24

This report is a matter of public record, and its distribution is not limited. Additionally, in accordance with the Americans with Disabilities Act, this document is available in alternative formats on our website.

TABLE OF CONTENTS

Executive Summary..... 3

Background 4

Audit Scope and Methodology..... 5

Appendix A: Risk Ratings..... 6

Executive Summary

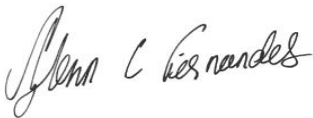
Internal Audit (IA) completed an audit titled Recovery Effort – Data Integrity - Maritime for the period August 2024, through August 2025. Based on internal discussions and scoping decisions, the audit solely focused on Maritime. The audit was performed to gain an overall understanding and to determine whether the Port's processes, specifically related to revenue billing and payroll, operated effectively during and immediately after the cyber event. IA tested the flow and transfer of information from each respective department to Accounting and Financial Reporting (AFR) Billing.

The Maritime Division oversees the cruise business, four recreational marinas, Terminal 91, Fishermen's Terminal, various industrial and commercial properties, along with the central harbor portfolio, and conference and event centers.

On August 24, 2024, the Port identified system outages consistent with a cyberattack. Incident response processes were initiated, and systems were deliberately taken "off-line." The Port partnered with third parties and federal partners and restored systems, once it was deemed safe.

Due to the manual nature of processes within Maritime, the impact of monitoring and accounting for revenue was minimally impacted. For example, prior to the cyberattack, Fishermen's Terminal staff performed daily boat checks to determine what boats are moored. This check is performed twice each day and the information was recorded by hand in a notebook and then entered into the Marina Vessel Management System (MVMS). The manual recording continued, uninterrupted, and the information was entered into MVMS once it was restored, several months later.

In general, we concluded that Port management's, monitoring, compliance, and internal controls aligned with established policies and procedures. We did not identify any issues that warranted reporting.



Glenn Fernandes, CPA
Director, Internal Audit

Responsible Management Team

Stephanie Jones Stebbins, Managing Director Maritime
Lisa Lam, Director, Accounting and Financial Reporting
Delmas Whittaker, Chief Operating Officer Maritime

Background

In August 2024, the Port experienced a widescale cyberattack carried out by a known criminal organization called Rhysida. Unusual and unauthorized activity was detected and isolated but the attack impacted Port businesses and hindered many services.

The Maritime Division within the Port manages industrial property connected with maritime business, marinas, Fishermen’s Terminal, cruise, grain and maritime operations. They are tasked with overseeing the cruise business, four recreational marinas, Terminal 91, Fishermen’s Terminal, various industrial and commercial properties, along with the central harbor portfolio and conference and event centers. The table below reflects operating revenues (in 000s) from each Maritime sector as of 2024, 2023, and 2022 (Source: 2024 Annual Comprehensive Financial Report).

<u>Maritime Division</u>	<u>2024</u>	<u>2023</u>	<u>2022</u>
Cruise Operations	36,723	40,372	29,197
Recreational Boating	17,663	16,584	14,957
Maritime Portfolio	6,875	6,070	8,608
Fishing and Operations	10,567	10,451	9,524
Grain Terminal	4,478	1,887	4,297
Other	12	(81)	179
Total Maritime Operating Revenues	76,318	75,283	66,762

Based on total operating revenues over the past three years, we opted to focus on the following three departments during our audit: Cruise Operations, Recreational Boating, and Fishing and Operations. While each of the departments has its own unique processes and procedures, they all heavily rely on manual controls, such as twice daily boat checks and secondary reviews when reporting revenues. Recordkeeping is primarily captured in Excel before being submitted to AFR and/or PeopleSoft. The manual nature of processes minimized the impact of monitoring and accounting for revenue. However, because PeopleSoft was offline, customer billings were delayed.

Payroll processing was also affected. To make sure employees were paid on time, the Port’s Payroll team opted to pay employees based on their last paycheck immediately prior to the cyberattack. This occurred for one pay period until an interim process was used that relied on excel spreadsheets to track employee hours. Finally, when systems, including Maximo and PeopleSoft were restored, payroll processes resumed to “normal” operations. However, many corrections and adjustments were identified.

These corrections and adjustments were identified when Payroll prepared individual reconciliation statements for each employee. Payments to underpaid employees were made by the middle of November. Employees who received overpayments were contacted individually and given the option to pay back the amount in full or set up repayment plans. As of early 2025, Payroll has been fully back to normal operations.

Audit Scope and Methodology

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and The Institute of Internal Auditors' Global Internal Audit 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 the evidence obtained provides such a basis.

We used a risk-based, judgmental approach to select items for testing. As a result, the findings reflect only the items tested and should not be interpreted as representative of, or extrapolated to, the entire population.

The period audited was August 2024, through August 2025 and included the following procedures:

Interviews and Process Walkthroughs

- Conducted walkthroughs and inquiries with key employees in the selected departments (Cruises, Fishing, and Recreational Boating) to gain an understanding of:
 - Each department's typical daily operations, as well as their operations post-cyberattack
 - How revenue is being recorded and billed
- Conducted inquiries with the Port's Payroll department to gain an understanding of how Payroll was processed immediately after the cyberattack, as well as how both overpayments and underpayments were resolved
- Conducted walkthroughs and inquiries with Marine Maintenance to gain an understanding of how payroll was processed until Maximo was reinstated

Document Review

- Obtained and reviewed key documents, such as:
 - Internal Excel workbooks and spreadsheets prepared by each department for AFR
 - PeopleSoft reports (i.e. Billing Batch Detail Reports, Interface Detail Summary)
 - Payroll records and pay stubs for selected employees
 - Listings of over and underpayments to employees

Validation and Testing

- Billing of Revenue:
 - Selected two months from the audit period (September 2024 and July 2025) and performed detail testing for each of the three departments selected
 - Verified that the internally prepared revenue schedules agreed to PeopleSoft
 - Investigated and inquired about variances
- Payroll Processing:
 - Selected ten hourly Maritime employees and tested five different pay periods for each
 - Verified and recalculated each employee's paystub to check the mathematical accuracy of total earnings using hours submitted multiplied by hourly rate
 - Investigated and inquired about variances
 - Verified that each employee was appropriately included in the listing of over and underpayments

Appendix A: Risk Ratings

Observations identified during the audit are assigned a risk rating, as outlined in the table below. Only one of the criteria needs to be met for an observation to be rated High, Medium, or Low. Low rated observations will be evaluated and may or may not be reflected in the final report.

Rating	Financial/ Operational Impact	Internal Controls	Compliance	Public	Commission/ Management
High	Significant	Missing or partial controls	Non-compliance with Laws, Port Policies, Contracts	High probability for external audit issues and / or negative public perception	Requires immediate attention
Medium	Moderate	Partial controls Not functioning effectively	Partial compliance with Laws, Port Policies Contracts	Moderate probability for external audit issues and / or negative public perception	Requires attention
Low	Minimal	Functioning as intended but could be enhanced	Mostly with Laws, Port Policies, Contracts	Low probability for external audit issues and/or negative public perception	Does not require immediate attention