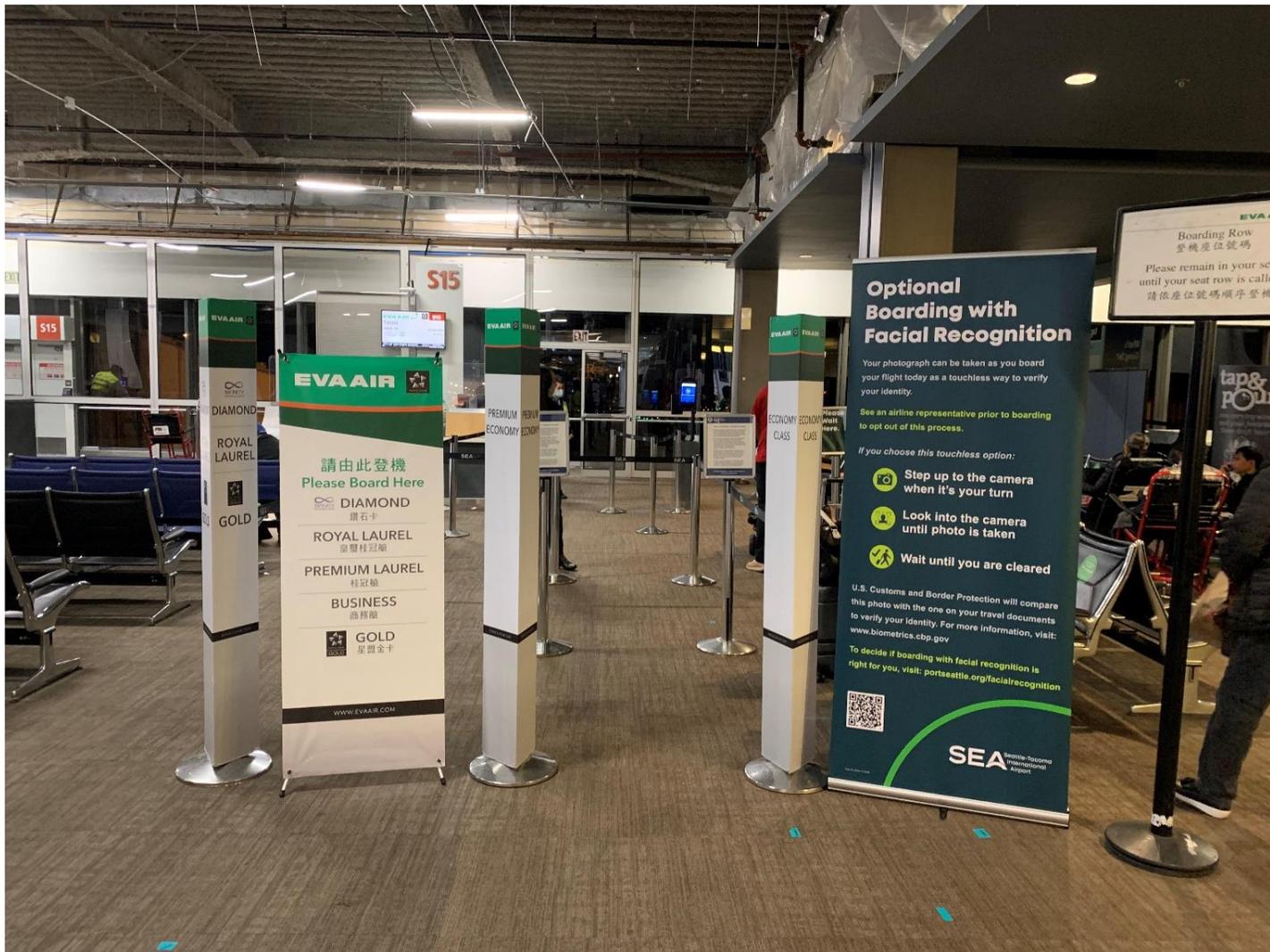


INTERNAL AUDIT REPORT



Information Technology Audit
Biometrics

January 2020 – May 2021

Issue Date: May 26, 2021
Report No. 2021-06



INTERNAL AUDIT

Redacted Version of Security Sensitive Report to Remove Security Sensitive Language

TABLE OF CONTENTS

Executive Summary	3
Background	4
Audit Scope and Methodology.....	6
Appendix A: Risk Ratings	7
Appendix B: Issues Identified and Corrected During the Audit.....	8

Executive Summary

Internal Audit (IA) completed an Information Technology (IT) audit of Biometric controls related to the Biometric Air Exit (BAX) project for the period January 2020 through May 2021.

The audit was performed to evaluate the adequacy of internal controls related to secure data storage, privacy, and network security around the processes for creating, storing, and transmitting biometric data for the BAX project. In addition, we reviewed compliance with the 49 requirements of the Port of Seattle's (Port's) "EX-23 Biometric Air Exit Policy" and the U.S. Customs and Border Protection's "Biometric Air Exit Business Requirements (v2.0)."

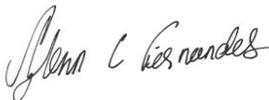
"U.S. Customs and Border Protection (CBP) is congressionally mandated to implement a biometric entry/exit system. CBP's Traveler Verification Service (TVS) offers a process for compliance with the pre-departure clearance of passengers under the Intelligence Reform and Terrorism Prevention Act. TVS uses facial comparison technology in a cloud environment to match live traveler photos with photos maintained in U.S. Government holdings. Stakeholder participation in biometric exit is voluntary and is not mandated by CBP."¹ While CBP has the authority to conduct their own BAX events for departing international flights, this review focused only on the Port's BAX processes; CBP currently has no plans to continue its own BAX screening at Seattle-Tacoma International Airport given the Port's full implementation of the program.

In reviewing the CBP requirements, Internal Audit noted that they included reasonable protections for data storage, privacy, and network security of the relevant biometric data, which consisted of images of departing international airline passengers. Our testing included reviewing the BAX processes for compliance with these requirements.

Based on the work we performed, and the information gathered, Internal Audit concluded that the BAX program has achieved reasonable compliance with both CBP and Port policy requirements.

There were a small number of non-compliant processes and several required processes which had not been implemented at the initial point of review in the audit. All the non-compliant items were corrected during the audit, and all the required processes were completed or were acceptably in-process to be completed. Appendix B is an abbreviated list of the issues identified and corrected during the audit. Additionally, it would be of value to include the BAX hardware/software in the annual Attack and Penetration Assessment that is conducted by the Information Security department.

Internal Audit would like to thank the Port's Aviation Innovation, External Relations Communications, Government Relations, Information Security, Information and Communications Technology, and Aviation Maintenance departments for their cooperation and partnership during this audit.



Glenn Fernandes, CPA
Director, Internal Audit

Responsible Management Team

Matt Breed, Chief Information Officer
Nate Caminos, Director, Government Relations
Ron Jimerson, Director, Information Security

Stuart Mathews, Director, Aviation Maintenance
Kathy Roeder, Director, Public Affairs Communications
David Wilson, Director, Aviation Innovation

¹ U.S. Customs and Border Protection Biometric Air Exit Requirements Document, v2.0

Background

The Port of Seattle (Port) is a public enterprise and employs approximately 2,000 employees. The Port owns and operates assets including Seattle-Tacoma International Airport (SEA), conference facilities, fishing and recreational boating marinas, industrial properties, and cruise ship terminals. This Information Technology audit included the following departments in its scope:

Information & Communication Technology (ICT) delivers and supports a wide variety of technology solutions to enable Port objectives.

The *Government Relations Department* is responsible for a wide variety of local, state, and federal policy advocacy, which not only includes engaging directly with elected officials and key agencies but also researching, developing and analyzing policies and policy positions that are in line with the Port's legislative priorities.

External Relations Communications is responsible for sharing information about the Port to external audiences using mass communications channels, such as media relations, the Port of Seattle website, social media, and email newsletters.

The *Information Security Department* is integrated with ICT, Maritime, and Aviation Maintenance. The department provides strategies, operations, and controls for protecting the Port's information systems and sensitive data while increasing business resiliency.

Aviation Maintenance provides services to support the operations of Seattle Tacoma International Airport, its tenants, and its guests.

Aviation Innovation incubates and promotes employee innovation with the Shark Tank and Crowdsourcing Innovation Challenge processes. The team also provides support for airline and passenger technology solutions.

In 2020, the Port continued its efforts to lead the development of biometric policies and procedures that emphasize travelers' privacy and civil liberties, while ensuring a safe, respectful, and efficient customer experience for those passengers departing SEA on international flights.

Following months of engagement with the aviation industry, federal officials, and civil liberties groups, the Port Commission (Commission), on March 10, 2020, directed staff to implement new policies governing the implementation of "Biometric Air Exit" (BAX) at SEA.

BAX is a federally regulated program that uses facial recognition to confirm the identities of departing international passengers at the boarding gate. All departing international passengers; U.S. citizen or foreign national, have the right to opt out of biometric processing and request manual screening to confirm their identity. Because of its voluntary and one-to-one nature, BAX complies with the Port's prohibition against mass surveillance using facial recognition technology.

To assure the Port can enforce policies related to data privacy and traveler rights, the Commission also authorized a Request for Proposals (RFP) for up to 30 BAX systems for installation at SEA, so that the Port – not the federal government – could control the traveler engagement aspects of this process. The contract award for that RFP required full compliance with the Port's BAX policies, such as ensuring that data transmitted to CBP by the Port or received by the Port from CBP is not stored or used for commercial purposes and that cameras are appropriately positioned to avoid photographing other passengers.

The initial SEA launch of BAX was implemented on December 17, 2020, at gate S16 (in the South Satellite) for EVA Air and is currently being used by EVA Air, Japan Airlines, Korean Air, Asiana Airlines, and Qatar Airways. The BAX system is comprised of 53 cameras installed at 15 S-gates in the South Satellite and 15 A-gates in the Main Terminal. Additionally, there is a separate on-going project to install

Redacted Version of Security Sensitive Report to Remove Security Sensitive Language

Biometrics

cameras at two N-gates in the North Satellite.

By implementing BAX, the Port was able to control the training of airline personnel and require that the training included sensitivity for dealing with passengers who may be concerned with facial recognition. Additionally, the Port was able to receive approval from CBP to develop and use its own signage at the departure gates to allow for considerably larger signs, with language that more clearly explains the passengers' rights for accepting or declining to use facial recognition.

Audit Scope and Methodology

We conducted this Information Technology audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. Those 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 a reasonable basis for our findings and conclusions based on our audit objectives.

The period audited was January 2020 through May 2021 and included the following procedures:

Policies and Requirements

- Obtained copies of Port's EX-23 Biometric Air Exit Policy and the CBP's Biometric Air Exit Business Requirements (v2.0) and assessed compliance.

Privacy and Security

- Evaluated CBP's Biometric Air Exit Business Requirements (v2.0) to determine whether they adequately addressed sensitive data protection.
- Evaluated relevant encryption settings.
- Performed testing to determine whether encryption settings were operating effectively.
- Evaluated logon accounts for appropriate security configurations.

Internal Audit also gained an understanding of the related internal controls by inquiring with the following Port management:

- 1) Director, ICT Technology Delivery
- 2) Director, ICT Infrastructure Services
- 3) Director, Public Affairs Communications
- 4) Senior Manager, Federal & International Government Relations
- 5) Director, Aviation Innovation
- 6) Manager, Information Security
- 7) Manager, Aviation Maintenance

Appendix A: Risk Ratings

Findings 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 a finding to be rated High, Medium, or Low. Findings rated Low will be evaluated and may or may not be reflected in the final report.

Rating	Financial Stewardship	Internal Controls	Compliance	Public	Commission/ Management
High	Significant	Missing or not followed	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	Potential for external audit issues and / or negative public perception	Requires attention
Low	Minimal	Functioning as intended but could be enhanced to improve efficiency	Mostly complies with Laws, Port Policies, Contracts	Low probability for external audit issues and/or negative public perception	Does not require immediate attention

Appendix B: Redacted

The contents of this appendix were redacted in order to create a non-security sensitive version of this report.

CBP or Policy #	Requirements	Issue and Corrective Action	Date Corrected (approximate)
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

Biometrics

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]