Port of Seattle

COMMISSION
AGENDA MEMORANDUM
BRIEFING ITEM

Item No.
Date of Meeting October 29, 2019

DATE: October 11, 2019
TO: Stephen P. Metruck, Executive Director
FROM: Eric Schinfeld, External Relations; Veronica Valdez, Commission Office
SUBJECT: Second Biometrics Technology Study Session

EXECUTIVE SUMMARY

The purpose of this study session is to provide the Commission additional details regarding biometrics and facial recognition technology, building off the first Commission Study Session on Biometrics on September 10, 2019.

In particular, this meeting will provide additional understanding of the federal approach to biometrics as well as work done by Port staff on this topic. The study session will help inform Commissioners as they work toward adoption of a Commission Motion guiding use of biometrics at Port facilities this year.

Biometrics are already being used at Port facilities – by the Port and by its private sector and federal partners – and these technologies are on track for broader implementation, particularly with regard to travelers and passengers. For example, U.S. Customs and Border Protection (CBP) is working toward implementation of facial recognition technology for all international commercial air travelers within the next four years. The advantages of these innovations for the Port of Seattle are clear: a faster, seamless, more convenient passenger processing experience, and access control for sensitive areas of Port facilities. Yet there are also many perceived concerns from the public and certain stakeholders: privacy, racial equity, cybersecurity and unforeseen uses that raise ethical questions.

Therefore, it is incumbent on the Port to have a strategic and comprehensive understanding of how this technology works, how it might be used and key policy and regulatory issues that might need to be addressed. The study session will include expert panelists who will present on these aspects of biometrics and answer Commissioner questions.

BACKGROUND

Biometric Technology at the Port

"Biometric authentication" – otherwise known as "biometrics" – uses biological measurements or physical characteristics to identify individuals. We commonly think of biometrics around fingerprint mapping, facial recognition and voice recognition, but it also includes retina scans, the way someone sits and walks, unique body odors, and even facial contortions that can serve as unique identifiers.

Many Port employees are issued iPhones with fingerprint and facial recognition as an alternative to password protection, and facial recognition is also used on Microsoft Windows

10; increasingly, biometric authentication will be utilized for computer system access by employees, contractors, and others who access the Port's cyber assets.

On the aviation side, Seattle-Tacoma International Airport (Sea-Tac) requires fingerprint scans by airport employees at many secure doors throughout the facility, and we offer travelers the option of using CLEAR to process through the Transportation Security Administration (TSA) checkpoints.

With regard to maritime, Port-issued identification cards currently utilize fingerprint biometrics to access secure areas or to limit access to Port facilities outside of normal business hours. In addition, federal government-issued Transportation Worker Identification Credential (TWIC) biometric smart cards are required to access regulated maritime and cruise operational areas. The Port and its maritime partners are also exploring additional forms of biometric identification in the future for these types of purposes. For example, the cruise industry will increasingly take advantage of biometrics as a passenger facilitation tool.

Biometric Policy Background

As part of its immigration enforcement mission, CBP has established an "end-to-end" process to collect biographic and/or biometric data from covered classes of nonimmigrant visitors upon their exit from the United States and matches it to data from their entry into the United States. CBP's goal is to determine whether foreign nationals overstayed their authorized periods of admission, as well as to confirm whether the departing individual is truly the same person who entered the United States. Currently, this process mainly uses biographic exit data provided by airline carriers, which is then matched to the entry data collected by CBP officers at the time that a foreign national was admitted to the United States.

Direction for U.S. Customs and Border Protection to move from biographic data collection to biometric data collection originated as a recommendation of the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission. In its final report, the 9/11 Commission concluded that "funding and completing a biometric entry-exit screening system for travelers to and from the United States is essential to our national security."

Based on the commission's recommendations, Congress included biometric entry/exit provisions in the Intelligence Reform and Terrorism Prevention Act of 2004. The FY 2013 Consolidated and Further Continuing Appropriations Act transferred entry/exit policy and operations to CBP. In addition, the FY 2016 Consolidated Appropriations Act authorized funding for a biometric exit program of up to $1 billion to be collected through fee surcharges over a period of 10 years.

More recently, President Trump included direction to expedite completion of this transition to biometric identification in section 7 of Executive Order 13769, which is known as the Muslim ban or travel ban: "The Secretary of Homeland Security shall expedite the completion and implementation of a biometric entry-exit tracking system for all travelers to the United States, as recommended by the National Commission on Terrorist Attacks Upon the United States."

CBP Data Privacy Standards

CBP has issued Privacy Impact Assessments (PIA) documenting each new phase of biometric testing and deployment. The most recent PIA from November 2018 is a comprehensive document describing how CBP promotes data privacy and appropriate data collection practices, including:

- Opt-out provisions: U.S. citizens who do not wish to submit to facial photo capture pursuant to these processes may request alternative processing, which typically involves a manual review of their travel documents by a CBP officer (CBPO).
- Deletion of U.S. citizen photos: Once a match is made and notated in the appropriate systems, U.S. citizens' photos are retained for no more than 12 hours, then deleted. CBP retains only a confirmation of the crossing and the associated biographic information. No photos of U.S. citizens are retained under this process.
- Routine testing: CBP regularly tests its facial matching algorithms to ensure high performance and maximize match rates while reducing the risk of false positives. Throughout this process, CBP has designed the tests in order to assess whether the process generates the same results across all demographics, including differences in skin tones.
- Prohibitions on additional uses: CBP's business requirements do not permit its private sector partners to retain or share the photos captured at the boarding gate. CBP shares the facial images of in-scope travelers within DHS, but does not share U.S citizens' biometric data with any other external federal entity. CBP may share information with federal, state, and local authorities for law enforcement, judicial proceedings, congressional inquiries, audits, and other lawful purposes; CBP updates its notices for any new uses.
- Notifications to travelers: CBP provides notice to travelers at the designated ports of entry through both physical and either LED message boards or electronic signs as well as verbal announcements in some cases to inform the public that CBP will be capturing the photos for identity verification purposes, and that U.S. citizens may currently request alternative processing from a CBPO, should they wish to opt-out of the biometric process. In addition, CBP's public notices notify travelers that CBP will retain the photos in secure DHS IT systems, with the exception of photos of U.S. citizens, which are not retained unless linked to an enforcement record. When CBP operates in conjunction with approved partner organizations, the public is informed that the partner is collecting the biometric data in coordination with CBP. Upon request, CBPOs provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular demonstration or program, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.

Facial Recognition Pilot Projects at Sea-Tac

At the direction of CBP, Sea-Tac's new International Arrivals Facility will open with full implementation of biometric entry, using facial recognition for both immigration and customs screening of almost all arriving passengers through the Federal Inspection Services (FIS) area. CBP requires Sea-Tac and its international departing airlines to implement a biometric exit system prior to the opening of IAF, so that, as described above, there is biometric data on the departing individual available to match to the individual's previously collected arrival data.

Note that this requirement is separate from airlines' goals of using biometrics as a customer facilitation technology; CBP's requirement is only biometrics at the boarding gate and only for departing international travelers. In addition, CBP does not require U.S. citizens to have their pictures taken; such travelers who do not wish to participate in a facial comparison process can request an alternative means of verifying their identities and documents. We will hear more from CBP at your October 29 study session about how this "opt-out" process works.

In preparation for the opening of the IAF and the associated implementation of biometric entry and exit at Sea-Tac, two pilot projects have taken place to-date:

- In 2018, CBP partnered directly with Lufthansa to allow the airline to run a pilot test of biometric exit technology. The biometric exit technology was used on one gate at Sea-Tac.
- In 2019 (July through September), Sea-Tac ran its own direct pilot of biometric exit technology, using a facial recognition solution developed by the Metropolitan Washington Airport Authority (Dulles). Airline participants were Japan Airlines and Emirates Airlines and technology was installed at two gates at Sea-Tac. Data on the pilot test results will be presented to you on October 29.

There are no additional pilot tests planned at Sea-Tac at this time.

Future Biometrics at Sea-Tac

Nationally, airports are approaching biometric exit in one of three ways: 1) allowing airlines to install their own proprietary facial recognition solutions at preferential gates, 2) installing an airport-wide solution that is provided to air carriers for their use, or 3) a hybrid model, which is allowing airlines to use their own solutions at preferential gates while using an airport solution at common use gates.

To-date, only Delta Air Lines has approached Sea-Tac with a desire to install facial recognition technology. While their ultimate goal is a "curb-to-gate" fully integrated biometric airport experience, Delta is only currently proposing implementation of this technology at their boarding gates. The use of proprietary airline technology at preferential gates is a standard practice at Sea-Tac on everything from ticketing computers to boarding pass scanners, and is allowed for under the terms of the airport's Signatory Lease and Operating Agreement (SLOA); biometrics would be treated in a similar manner.

In theory, the installation of Delta's technology at their preferential gates would not conflict with Sea-Tac's installation of a different technology at common use gates, based on the rare occurrence of other carriers using preferential gates. However, if there were to be a conflict where one carrier has proprietary technology installed and the other does not or has their own technology, SLOA does allow for the airport to standardize facial recognition technology at all Sea-Tac international departing gates by installing our own airport-wide system. Much of the final decision-making on these issues will rely on Commission direction related to Port-wide biometric policy.

Pending the outcome of the Commission's biometric policy discussions, the airport may request Commission approval of a Request for Proposal (RFP) for a facial recognition technology to be installed at up to 21 common use gates. No specific technology or technology provider has been presupposed at this point, although there are a limited number of providers who meet CBP's criteria for both operational and security requirements; these are listed in the CBP Business Requirements.

ATTACHMENTS TO THIS BRIEFING

None.

PREVIOUS COMMISSION ACTIONS OR BRIEFINGS

September 10, 2019 – First Commission Study Session on Biometrics