



**PORT OF SEATTLE PUBLIC-FACING BIOMETRICS POLICY
BIOMETRIC AIR & CRUISE ENTRY RECOMMENDATIONS**

DRAFT AS OF AUGUST 7, 2020



TABLE OF CONTENTS

1. Executive Summary
2. Introduction
3. Basics of Biometric Air & Cruise Entry
4. Applying the Port's Public-Facing Biometrics Guiding Principles to Biometric Entry
 1. Justified
 2. Voluntary
 3. Private
 4. Equitable
 5. Transparent
 6. Lawful
 7. Ethical
5. Appendix
 1. Biometrics Working Group
 2. Biometrics External Advisory Group
 3. Commission Biometrics Policy Motion

1. EXECUTIVE SUMMARY

Biometrics is the measurement and analysis of physical and behavioral characteristics that are used to identify individuals through technology. Examples of physical characteristics include the unique features of an individual's face or their fingerprint, while examples of behavioral characteristics includes an individual's voice, signature, or how they walk.

Due to technological advances, perceived customer benefits and federal requirements, there is a significant increase in public-facing biometric technology deployment by public and private sector users, including in airport and seaport settings. In fact, biometrics are already being used at dozens of U.S. airports and cruise terminals, by those who see the technology as a major benefit to travelers – both because of a faster and more efficient travel experience, as well as a more accurate security process. However, many members of the public and various advocacy organizations have expressed concerns about the rapidly expanding use of biometrics. These stakeholders have raised issues around privacy, equity and civil liberties, as well as the potential for unregulated “mass surveillance.”

Public-facing biometrics are already used in various forms at the Port of Seattle's aviation and maritime facilities, such as 1) CLEAR, a private company providing an option to those customers who want expedited screening at U.S. Transportation Security Administration (TSA) checkpoints to voluntarily supply their biometric data in order to verify their identities, 2) U.S. Customs and Border Protection (CBP) use of biometrics at Seattle-Tacoma International Airport (SEA) to validate departing international traveler identities, and 3) use of biometrics on Norwegian Cruise Line ships docked at Pier 66 to validate the identities of disembarking passengers. CBP will also use facial recognition technology to screen almost all arriving international passengers once SEA's International Arrivals Facility (IAF) opens in the coming year.

In advance of any expansion of biometric uses at Port of Seattle facilities by the Port or its private sector tenants, the Port of Seattle Commission desires to develop proper policy frameworks and clear guidelines to reduce potential misuse and abuse of biometrics, while improving public understanding of the benefits and risks of this technology in various applications. On December 10, 2019, after holding two Study Sessions, conducting stakeholder outreach and doing multiple site visits, the Port Commission adopted seven “biometrics guiding principles,” and directed staff to translate those principles into tangible, enforceable policies. Specifically, the Port strives to balance operational needs, business priorities and regulatory mandates with protections for the interests and rights of passengers, employees and other visitors to our facilities.

Over the last six months, a working group of Port staff has collaborated with an external advisory group of key stakeholders to accomplish that task. **One of the key findings from this process is that the various use cases of biometrics require separate analysis as to how the Port should (consistent with local, state and federal requirements) apply the biometrics guiding principles to develop policy.** One unified set of policies is not practical because of key differences from one use case to another, such as who manages the data, requirements imposed by state or federal law, and the benefits and risks associated with each use.

This set of recommendations is specific to “biometric entry,” which is the use of facial recognition utilizing the CBP Traveler Verification Service (TVS) to validate the identities of arriving international¹ passengers as they exit a cruise ship or international flight. Additional recommendations for other use cases are provided separately.

The recommendations that have resulted from the working group and external advisory group process are listed below, along with concerns from some external advisors who do not support some of these recommendations. All sides of the discussion are represented here to provide Port Commissioners full information prior to adoption of any policies.

DRAFT

¹ As will be discussed in greater detail in this document, disembarking cruise passengers are considered international arrivals because of their transit through international waters.

2. INTRODUCTION

The goal of the Port's Biometric Working Group is to translate the seven biometrics principles adopted by the Port Commission into tangible, enforceable policies that ensure, to the greatest extent possible, that the use of public-facing biometrics at Port facilities conform to these principles.

The recommendations below are specific to biometric entry, which is the use of facial recognition utilizing the CBP Traveler Verification Service (TVS) to confirm the identities of arriving international passengers as they exit aircraft or cruise ships. Entry into the United States is a federally regulated process, and all persons arriving at a port-of-entry to the United States are subject to inspection by CBP before entering the country.² Therefore, the Port has very limited ability to influence, much less direct, the activities of CBP and the Biometric Entry process.

The Port has endeavored to recommend policies of general applicability wherever possible; however, some recommendations are divided into 1) recommendations that apply to the Port, and 2) recommendations related to CBP. Where the Port lacks authority to mandate compliance with particular policies, the recommendation is to work collaboratively with stakeholders to achieve voluntary compliance where appropriate, and/or highlight how these stakeholders' own policies match Port principles. The Port should also advocate for the adoption of new laws and regulations that align with the Port's biometric principles.

Finally, while the recommendations below represent the thinking of Port staff, there is not consensus among all members of the Port's External Advisory Group on these recommendations. Therefore, stakeholder concerns about each recommendation are also included below so that the Port Commission can consider all perspectives before they adopt any final policies. Ultimately, the Port Commission is the governing body that can approve any recommendations and adopt policies.

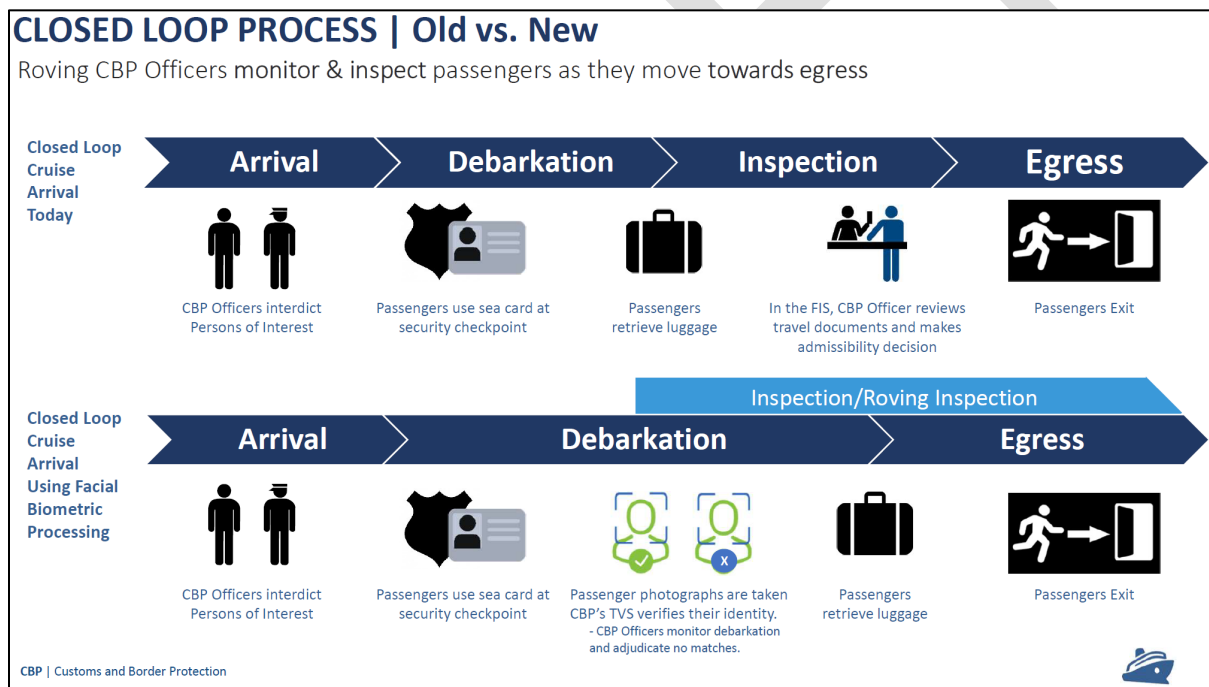
3. BASICS OF BIOMETRIC ENTRY

Biometric entry is intended to meet CBP's goal of ensuring individuals entering the country are truly the same person who is authorized to do so. Direction for CBP to move 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 9/11 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 costing 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."

² Technically, a person has not "entered the country" until they have passed through CBP screening and left the FIS.

CBP has begun implementing its biometric entry program through its development of the Traveler Verification Service (TVS) and associated pilot programs. TVS is essentially a system of related databases hosted by CBP, containing the biometric facial recognition “template” of individuals. These templates are based on images previously collected by CBP or other federal agencies, such as from passport or visa application photos. TVS allows CBP to deploy camera systems that capture an image of an individual, at which point the TVS system attempts to match the image to a “gallery” of biometric templates; if it confirms a match, the system transmits a “match/no match” confirmation.

The Port of Seattle has very limited ability to influence, much less direct, the activities of CBP and the Biometric Entry process. In the Seattle region, this process will operate slightly differently between air and cruise environments. At the airport, arriving international passengers will enter the Federal Inspection Services (FIS) facility and be screened via TVS with additional screening by an in-person CBP officer³. At Seattle cruise terminals, biometric entry will take place either on board the cruise ship or in the cruise terminal’s FIS⁴. Because Alaska cruises homeporting from Seattle are considered by CBP to be “closed loop”,⁵ CBP would then only conduct additional screening for select travelers⁶. In other words, once cruise passenger identities are verified by TVS, most individuals are treated by CBP as if they never left the country. A comparison of arriving cruise passenger processing – now versus future – is shown below:



³ The exception is many flights from Canada, and a limited number of other airports like Dublin that also have U.S. pre-clearance facilities. These passengers are considered the same as domestic arrivals because they went through FIS procedures at their airport of departure.

⁴ The only current application of TVS for biometric entry is on-board Norwegian cruise ships at Pier 66

⁵ Most cruises beginning and ending in the U.S. are considered "Closed Loop," vessels that depart a U.S. port and return to the same U.S. port upon completion of the voyage.

⁶ Based in part on their evaluation of the Advance Passenger Information System (APIS) data provided by cruise lines in advance of boarding.

4. APPLYING THE PORT’S PUBLIC-FACING BIOMETRICS GUIDING PRINCIPLES TO BIOMETRIC AIR AND CRUISE ENTRY

a. Justified

The Port Commission’s Biometrics Motion states that:

Biometric technology at port facilities should be used only for a clear intended purpose that furthers a specific operational need. The port does not condone biometrics for “mass surveillance” – for example, use of facial recognition on large groups of people without a lawful purpose, rather than single-use for travelers.

1. Key Issues to address

The Justified principle essentially speaks to two key issues of concern: 1) making explicit an operational need to use biometrics, and 2) ensuring that biometrics are not used for “mass surveillance” at Port facilities. The Commission motion defines mass surveillance as scanning large groups of people without lawful purpose, rather than use on one person at one time with their active participation.

As it relates to a specific operational need, identity verification is a core activity mandated by CBP as part of the international arrivals process. CBP and Congress have determined that biometric entry is operationally necessary to ensure national security and ensure compliance with immigration laws. CBP refers to biometric entry as the automation of an existing verification process, since it is replacing the current process of manual verification of identities. CBP already has the picture of most travelers, gathered from U.S. passport or foreign visitor visa application photos.

In the cruise environment, cruise lines also recognize that a benefit of the use of biometrics as a passenger facilitation tool is to more quickly process the thousands of individuals who all disembark at the same time. Because there are limited numbers of CBP officers available for cruise passenger processing, cruise lines benefit from CBP efforts to make cruise ship disembarkation to be as efficient as possible. In the airport environment, airlines have no involvement in decisions related to biometric entry.

Biometric entry is not mass surveillance. Biometric entry captures an image of individuals with their awareness and active participation, which aligns with the Commission’s definition.

2. Working Group Recommendations

“Justified” recommendations at a glance	
Port	CBP/Cruise
The port should request notification from CBP and cruise lines in advance of any implementation of biometric entry.	<p>Cruise lines should notify the Port if and when CBP implements biometric entry on board cruise ships docked at Port cruise facilities or in the CBP FIS within Port cruise facilities.</p> <p>CBP should notify the Port if and when they implement biometric entry at Port facilities.</p>

The Port

Recommendation 1a: Due to both practical and legal considerations, the Port may not deny CBP the right to implement biometric entry at SEA, on board cruise ships or in the CBP FIS in cruise terminals. However, the Port should request that CBP notify the Port if and when they intend to conduct biometric entry, so that the Port can maintain situational awareness and begin implementation of the associated recommendations below.

Cruise Lines

Recommendation 1b: Cruise lines should notify the Port if and when CBP implements biometric entry on board cruise ships docked at Port cruise facilities or in the CBP FIS within Port cruise facilities.

CBP

Recommendation 1c: CBP should notify the Port if and when they are implementing biometric entry at Port facilities.

3. Stakeholder Concerns

TBD

b. Voluntary

The Port Commission's Biometrics Motion states that:

The use of biometrics to identify and validate travelers through port facilities should be voluntary, and reasonable alternatives should be provided for those who do not wish to participate – through a convenient “opt-in” or “opt-out” process, except in specific situations authorized by the port or required by federal law such as U.S. Customs and Border Protection’s (CBP) entry and exit requirements for non-U.S. citizens. Unintended capture of data by biometric technology from those travelers opting out of such biometric data collection, or of any non-travelers or other visitors at the airport, should be prevented; any unintended capture of this data should not be stored.

1. Key Issues to address

There are two main aspects of the Voluntary principle: 1) providing for an opt-in or opt-out procedure, and 2) preventing unintended image capture.

Because biometric entry is a federal program, opt-out provisions are regulated by CBP. Current CBP policy states that travelers are allowed to opt-out of biometric screening.⁷ However, it is essential that all travelers fully understand this right and the consequences of opt-ing out; similarly, the Port must advocate for opt-out procedures are respectful and appropriate.

As related to image capture, the Port can suggest ways to prevent unintended image capture during biometric entry operations for CBP consideration.

2. Working Group Recommendations

“Voluntary” recommendations at a glance

⁷ From CBP guidelines: “While U.S. Citizens who are entering or exiting the country are generally required to be in possession of a valid U.S. passport, CBP does not require U.S. Citizens or exempt aliens to have their pictures taken. Travelers who do not wish to participate in this facial comparison process may notify a CBP Officer or an airline, airport or cruise line representative in order to seek an alternative means of verifying their identities and documents.”

Port	CBP
<p>If CBP implements biometric entry, the Port recommend ways for minimizing unintended image capture and should communicate those recommendations to CBP and cruise lines.</p> <p>The Port should design training standards to help cruise employees explain opt-out provisions.</p>	<p>CBP policy states that legal U.S. residents are allowed to opt-out of biometric screening</p>

For Port

Recommendation 2: The Port should develop recommendations to CBP for their consideration regarding ways to avoid unintended image capture at Port facilities – for example, by positioning the camera in a direction that does not face the main passenger area, use of a screen behind the individual being photographed, or use of a camera with a minimal field view. While CBP has jurisdiction over this topic, the Port’s unique expertise regarding its facilities would be offered as a value-add to CBP.

Recommendation 3: The Port should continue to pursue whether opt-out is an option for biometric entry at Port facilities. If not, the Port should design training guidelines to help cruise line employees to educate disembarking passenger about CBP rules regarding opt-out.

For CBP

As stated above, current CBP policy states that legal U.S. residents are allowed to opt-out of biometric screening. Enshrining this regulation in legislation is part of the Port’s federal advocacy efforts outlined in the Lawful principle.

3. Stakeholder Concerns

TBD

c. Private

The Port Commission’s Biometrics Motion states that:

Data collected by biometric technology at port facilities or by port employees from travelers through port facilities should be stored only if needed, for no longer than required by applicable law or regulations, and should be protected against unauthorized access. The port opposes this data being knowingly sold or used for commercial purposes unrelated to processing travelers at port facilities without their clear and informed consent. Individuals should be provided a process to challenge instances where they feel their rights have been violated.

1. Key Issues to address

The Private principle is an essential aspect of travelers’ confidence in their participation in any biometric entry program. Individuals want to know that their data is secure, not being used for any inappropriate purpose, and protected.

CBP has published a Privacy Impact Assessment report that outlines its efforts to protect data privacy as part of its TVS system.⁸ There is no present mechanism for the Port to monitor or enforce these privacy guidelines. Biometric entry must meet CBP’s Business Requirements that outline compliance with these privacy regulations. For example, CBP’s business requirements do not permit its private sector partners to retain or share the photos captured during the biometric entry process.

2. Working Group Recommendations

“Private” recommendations at a glance	
Port	CBP
The Port should request CBP audit reports on biometric entry systems on a regular basis.	The port does not have jurisdiction over CBP's privacy policies or procedures but supports ongoing audits on CBP's biometric entry and exit system and that these audits be made publicly available.

For Port

Recommendation 4: The Port should request CBP audit reports on biometric entry systems on a regular basis and include appropriate information in the Accountability Report (see recommendation under “Transparent” principle).

For CBP

The Port is not legally authorized to regulate CBP’s privacy policies or procedures. CBP is generally required to comply with federal privacy laws and regulations, and it sets forth its compliance with many such requirements in the Privacy Impact Assessment noted above. However, there is no comprehensive federal framework specifically governing privacy protections for biometric data. The Port will encourage CPB to continuously audit their biometric entry and exit system and ensure those audits are publicly available. The Port can help enhance CBP’s efforts related to explaining their data privacy efforts; see recommendations under the “Transparent” principle.

3. Stakeholder Concerns

TBD

d. Equitable

The Port Commission’s Biometrics Motion states that:

The port opposes discrimination or systemic bias based on religion, age, gender, race or other demographic identifiers. Biometric technology used at port facilities or by port employees should be reasonably accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues with proper cultural sensitivity and discretion.

1. Key Issues to address

The Equitable principle essentially speaks to two key issues: 1) concern that facial recognition technology does not perform as effectively on individuals who are not male Caucasians, and that 2) regardless of why the CBP algorithm identifies a mismatch, systems should be in place to resolve the issue with minimal impact to the traveler.

⁸ https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf

A recent study by the National Institute of Standards and Technology (NIST) found that facial recognition technology’s ability to identify individuals with diverse characteristics varies significantly based on the algorithm at the heart of the system, the application that uses it, and the data inputs.⁹ However, the NIST report confirmed that the NEC algorithm used by CBP in its Biometric Entry program ranked first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP. The specific algorithm used is a component of the CBP-supplied TVS.

Treating no-matches or mismatches with “cultural sensitivity and discretion” requires that individuals who are not verified through TVS are subject to additional document review in a manner and location that draws the least possible attention to the situation and does not create a feeling of fear or discomfort for the traveler.

The Port does not have jurisdiction over CBP officer customer service protocols, but can develop and share customer service guidelines.

2. Working Group Recommendations

“Equitable” recommendations at a glance	
Port	CBP
<p>The Port should request updated accuracy rates from CBP.</p> <p>The Port should develop suggested training recommendations for personnel administering the facial recognition technology on travelers. The Port should discuss its desired customer service standards with CBP and cruise lines.</p>	<p>The port does not have jurisdiction over the CBP algorithm or customer service protocols.</p>

For Port

Recommendation 5: The Port should request biometric program accuracy rates from CBP on an annual basis, including a request for any available data segmented by key traveler characteristics. The Port should also request that CBP make available an application programming interface (API) or other technical capability, to enable legitimate, independent, and reasonable tests of those biometric technologies for accuracy and unfair performance differences across distinct subpopulations.

Recommendation 6: The Port should develop suggested biometric training guidelines for personnel who will be administering the facial recognition technology on travelers, including the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.

Recommendation 7: The Port should share its training guidelines, specifically related to “cultural sensitivity and discretion”, with CBP and cruise lines for their voluntary adoption.

3. Stakeholder Concerns

TBD

⁹ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

e. Transparent

The Port Commission’s Biometrics Motion states that:

Use of biometric technology for passenger processing at port facilities should be communicated to visitors and travelers. Individuals should be notified about any collection of their biometric data to facilitate travel at port facilities, and how that data may be used, in easily understood terms. Reports on the performance and effectiveness of the technology should also be made public to ensure accountability.

1. Key Issues to address

The Transparent principle essentially speaks to three key issues: 1) the need for any use of biometric entry to be clearly communicated to anyone travelling through Port facilities, 2) the need to ensure that passengers using biometric entry are informed in a clear, concise manner about biometric entry, how it is used, and their rights related to the system, and 3) the need for accountability reports to be created and published for the public.

The Transparent principles requires that passengers should be made aware that biometric entry is going to be used on their arriving international flights or cruises, understand what it is, and be informed of their rights related to the program (including their ability to opt-out). While the Port cannot direct cruise line or CBP actions in this regard, there is opportunity for coordination with airlines, cruise lines and CBP.

Similarly, information about the system should be shared, and publicly available findings should be communicated.

2. Working Group Recommendations

“Transparent” recommendations at a glance	
Port	CBP
<p>If CBP implements biometric entry, the Port should produce:</p> <ul style="list-style-type: none"> a) a comprehensive communications plan b) an accountability report <p>each of which should be shared publicly through all Port communication channels. Each report should include all available information released by CBP.</p>	<p>The port cannot require CBP to share information, but CBP does provide a number of relevant reports that the Port can share publicly.</p>

For Port

Recommendation 8: If CBP implements biometric entry at or proximate to Port facilities, the Port should develop a comprehensive communications plan that notifies the general public of the implementation and all related information. The communications plan should include specific communications within the airport or cruise terminal, where possible, including announcements, signage, flyers and web content. Where possible, the Port should partner with airlines, cruise lines and CBP to implement these communication efforts.

Recommendation 9: If CBP implements biometric entry at or proximate to Port facilities, the Port should produce an annual accountability report that includes all approved, publicly available information on topics such as:

- A description of the biometrics being used, including the name of the biometric vendor and version;
- The system’s general capabilities and limitations;
- How data is generated, collected, and processed;
- A description of the purpose and proposed use of the biometrics, and its intended benefits, including any data or research demonstrating those benefits;
- CBP’s privacy guidelines;
- Traveler rights with regard to the biometric entry system;
- The Port’s biometric training guidelines;
- Any publicly available information about CBP’s testing procedures, including its processes for periodically undertaking operational tests of the service;
- A description of any potential impacts of the service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the service;
- Procedures for receiving feedback, including the channels for receiving feedback from individuals affected by the use of the service and from the community at large, as well as the procedures for responding to feedback;
- Any known or reasonably suspected violations of CBP’s rules and guidelines, including complaints alleging violations;
- Other relevant data, including any publicly available data shared by CPB about the accuracy and effectiveness of its system;
- Benchmarking data against the operational results of the biometric system at other ports;
- Feedback about the public’s experience, sought proactively in customer surveys, including whether travelers believe that they fully understand the information about the system;
- Other relevant data, including any publicly available data shared by CPB about the accuracy and effectiveness of its system; and
- Any publicly available audits of the CBP biometric entry system.

This accountability report should be shared publicly through appropriate Port communications channels.

For CBP

The Port does not have jurisdiction over CBP’s transparency procedures. However, CBP does provide notice to travelers at ports of entry through physical signage, verbal announcements and/or flyers with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the program. As stated above, the Port can implement additional signage and communications on this topic.

As it relates to evaluation of the technology’s accuracy and effectiveness, the Port cannot require CBP to share this information, but it can request and help publicize CBP-provided performance data.

3. Stakeholder Concerns

TBD

f. Lawful

The Port Commission’s Biometrics Motion states that:

Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including privacy laws and laws prohibiting discrimination or illegal search against individuals or groups.

1. Key Issues to address

The Lawful principle essentially speaks to the legal justification for CBP’s biometric entry program. As discussed above, CBP has stated that the biometric entry/exit program is based on several Congressional (Intelligence Reform and Terrorism Prevention Act of 2004; FY 2013 Consolidated and Further Continuing Appropriations Act; FY 2016 Consolidated Appropriations Act) and Administration (Executive Order 13769) authorizations.

There are several active conversations in Congress regarding the need for additional regulation of the federal government’s use of facial recognition technology. This is a rapidly evolving area of the law and the extent to which biometric entry may be further regulated is not yet clear.

2. Working Group Recommendations

“Lawful” recommendations at a glance	
Port	CBP
Port staff should actively advocate for additional federal biometric regulations	CBP is subject to all federal law and regulations

For Port

Recommendation 10: Port staff should actively track and work with stakeholders to advocate for federal laws and regulations that support the Port’s biometric principles.

For CBP

CBP is subject to applicable federal law and regulations.

3. Stakeholder Concerns

TBD

g. Ethical

The Port Commission’s Biometrics Motion states that:

The port and its partners should act ethically when deploying biometric technology or handling biometric data. Ethical behavior means actions which respect key moral principles that include honesty, fairness, equality, dignity, diversity and individual rights. In particular, use of biometrics at port facilities should comply with Resolution No. 3747, establishing the port’s Welcoming Port Policy Directive to increase engagement with, and support for, immigrant and refugee communities.

1. Key Issues to address

As mentioned by several of the Port’s external stakeholders, the Ethical principle is an important complement to the Lawful principle, because of the current lack of comprehensive state and federal laws governing facial recognition technology.

Several of the recommendations on this topic are covered under other principles like Equity (treating people fairly and with dignity), Privacy (protecting individual rights) and Justified (no “mass

surveillance”). However, the most tangible aspect of this principle is alignment with the Port’s “Welcoming Port Policy” (Resolution 3747).¹⁰

The Welcoming Port Policy commits the Port “to foster a culture and environment that make it possible for our region to remain a vibrant and welcoming global gateway where our immigrant communities, refugee residents, and foreign visitors can fully participate in – and be integrated into – the social, civic, and economic fabric of our region.” To the extent consistent with federal laws and obligations, the practical applications of this policy include not denying anyone services based on immigration status; prohibiting any Port employees, including law enforcement officers, from unnecessarily asking about citizenship or immigration status; and taking tangible steps to make all visitors to its facilities feel welcome and safe. As it relates to immigration enforcement, the policy includes calls for the Port – within the restrictions of federal law – to “defer detainer requests from ICE”; restrictions on “providing federal immigration agents with access to databases without a judicial warrant”; and restrictions on carrying out “a civil arrest based on an administrative warrant.”

The biometric entry program does not provide CBP with any additional information that it already does not have: CBP already compiles galleries of travelers’ facial biometrics from photos that travelers are required to submit (i.e., passport or visa application pictures). The airlines and cruise lines already provide CBP with passenger manifests and traveler data through the APIS system. That is why CBP refers to biometric entry as an “automation of an existing system” rather than a new border security measure.

2. Working Group Recommendations

“Ethical” recommendations at a glance	
Port	CBP
The Port should engage with local immigrant and refugee communities in multiple languages and culturally appropriate ways to educate and ensure they know their rights when it comes to biometric entry at Port facilities	CBP is bound by all relevant federal laws as referenced above – including anti-discrimination and civil liberties statutes.

For Port

Recommendation 11: If CBP implements biometric entry at Port facilities, the Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about the biometric entry program. Specifically, the Port should ensure that these communities are fully informed about the program, the technology and their rights – in multiple languages and in culturally appropriate ways.

Recommendation 12: If CBP implements biometric entry at Port facilities, the Port should work with local jurisdictions, nonprofit organizations and others to inform local immigrant and refugee communities – in multiple languages and in culturally appropriate ways – about resources for sharing concerns about any incidents in which they do not feel they have been afforded their full legal rights and/or their treatment has not been fully respectful.

For CBP

CBP is bound by all relevant federal laws as referenced above – including anti-discrimination and civil liberties statutes. The best way to ensure ethical behavior is to enshrine it in statute, which relates back

¹⁰ https://www.portseattle.org/sites/default/files/2018-05/2018_05_08_SM_8a_reso.pdf

to the advocacy recommendations above. In addition, the Port will continue to engage regularly with CBP to share our expectations that all individuals traveling through our facilities have full access to their legal rights and are receiving appropriate treatment.

3. Stakeholder Concerns

TBD

DRAFT

APPENDIX

○ Appendix A – Port Biometrics Working Group

- Matt Breed, Chief Information Officer
- Julie Collins, Director, Customer Experience
- Commander Lisa Drake, Port of Seattle Police Department
- Laurel Dunphy, Director, Airport Operations
- Marie Ellingson, Manager, Cruise Operations and Business Development
- Eric ffitch, Manager of State Government Relations, External Relations
- Bookda Gheisar, Senior Director, Office of Equity, Diversity and Inclusion
- James Jennings, Director, Airline Relations
- Ron Jimerson, Chief Information Security Officer
- John McLaughlin, Senior Port Counsel
- Anne Purcell, Senior Port Counsel
- Russ Read, Manager, Maritime Security
- Wendy Reiter, Director, Aviation Security
- Kathy Roeder, Director of Communications, External Relations
- Eric Schinfeld, Senior Manager of Federal Government Relations, External Relations
- Deputy Chief Mark Thomas, Port of Seattle Police Department
- Veronica Valdez, Commission Specialist
- Todd VanGerpen, Manager, Aviation Innovation
- Dave Wilson, Director, Aviation Innovation

○ **Appendix B – Port Biometrics External Advisory Group**

- Ian Baigent-Scales, Airport Customer Development Manager - Airport Operations, Virgin Atlantic Airways
- Sasha Bernhard, Legislative Assistant, Office of US Representative Suzan DelBene
- Dana Debel, Managing Director, State and Local Government Affairs, Delta Air Lines
- Adele Fasano, Director, Field Operations, Seattle Field Office, US Customs & Border Protection
- Eric Holzapfel, Deputy Director, Entre Hermanos
- Suzanne Juneau, Executive Director, Puget Sound Business Travel Association
- Scott Kennedy, State and Local Government Affairs Manager, Alaska Airlines
- Jennifer Lee, Technology & Liberty Project Director, ACLU
- Maggie Levay, Director Guest Port Services, Royal Caribbean
- McKenna Lux, Policy Manager, CAIR-WA
- Yazmin Mehdi, Outreach Director, Office of US Representative Pramila Jayapal
- Nina Moses, Stakeholder Relations Manager, US Transportation Security Administration
- Irene Plenefisch, Government Affairs Director, Microsoft Corporation
- Sheri Sawyer, Senior Policy Advisor, Office of Washington State Governor Jay Inslee
- Victoria Sipe, Director Shore Operations, Holland America Group
- Rich Stolz, Executive Director, One America
- Elizabeth Tauben, Manager Port Guest Services & Clearance, Norwegian Cruise Line Holdings
- Jennifer Thibodeau, Public Policy Manager - Western States, Amazon Web Services
- Jevin West, Director, Center for an Informed Public, University of Washington

○ Appendix C – Commission Biometrics Motion

MOTION 2019-13: A MOTION OF THE PORT OF SEATTLE COMMISSION

adopting guiding principles for the public-facing use of biometric technology at Port of Seattle maritime and aviation facilities; establishing a working group to develop policy recommendations governing public-facing biometric use at the port; and establishing deadlines for further actions.

AMENDED AND ADOPTED DECEMBER 10, 2019

INTRODUCTION

Biometrics is the measurement and analysis of physical and behavioral characteristics that are used to identify individuals through technology. An example of a physical characteristic includes the unique features of an individual's face or their fingerprint. An example of a behavioral characteristic includes an individual's voice, signature, or how they walk.

The Port of Seattle has long used various forms of biometrics at its aviation and maritime facilities – for access control and verification of employee, contractor, vendor, and consultant identity. However, biometric technology – particularly facial recognition – is increasingly being deployed on the customer-facing side of airport and cruise operations, as both an identity validation and a customer facilitation tool to speed up check-in, boarding, and screening processes.

As with any developing technology, public sector leaders have an obligation to ensure appropriate and responsible use of not only the technology itself, but the related data that is generated. The port commission believes proper biometric policy should balance operational needs, business priorities, and regulatory mandates with protections for the interests and rights of passengers, employees, and other visitors to our facilities.

TEXT OF THE MOTION

Port of Seattle Principles for Public-Facing Biometric Technology

The commission hereby adopts the following principles to guide the use of public-facing biometric technology at Port of Seattle facilities:

- (1) **Justified:** Biometric technology at port facilities should be used only for a clear intended purpose that furthers a specific operational need. The port does not condone biometrics for “mass surveillance” – for example, use of facial recognition on large groups of people without a lawful purpose, rather than single-use for travelers.
- (2) **Voluntary:** The use of biometrics to identify and validate travelers through port facilities should be voluntary, and reasonable alternatives should be provided for those who do not

wish to participate – through a convenient “opt-in” process where possible or “optout” process if “opt-in” is not possible, except in specific situations authorized by the port or required by federal law such as U.S. Customs and Border Protection’s (CBP) entry and exit requirements for non-U.S. citizens. Unintended capture of data by biometric technology from those travelers opting out of such biometric data collection, or of any non-travelers or other visitors at the airport, should be prevented; any unintended capture of this data should not be stored.

- (3) **Private:** Data collected by biometric technology at port facilities or by port employees from travelers through port facilities should be stored only if needed, for no longer than required by applicable law or regulations, and should be protected against unauthorized access. The port opposes this data being sold or used for commercial purposes unrelated to processing travelers at port facilities without their clear and informed consent. Individuals should be provided a process to challenge instances where they feel their rights have been violated.
- (4) **Equitable:** The port opposes discrimination or systemic bias based on religion, age, gender, race, or other demographic identifiers. Biometric technology used at port facilities or by port employees should be accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues with proper cultural sensitivity and discretion.
- (5) **Transparent:** Use of biometric technology for passenger processing at port facilities should be communicated to visitors and travelers. Individuals should be notified about any collection of their biometric data to facilitate travel at port facilities, and how that data may be used, in easily understood terms. Reports on the performance and effectiveness of the technology should also be made public to ensure accountability.
- (6) **Lawful:** Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including state and federal privacy and consumer data protection laws and laws prohibiting discrimination or illegal search against individuals or groups.
- (7) **Ethical:** The port and its partners should act ethically when deploying biometric technology or handling biometric data. Ethical behavior means actions which respect key moral principles that include privacy, honesty, fairness, equality, dignity, diversity, and individual rights. In particular, use of biometrics at port facilities should comply with Resolution No. 3747, establishing the port’s Welcoming Port Policy Directive to increase engagement with, and support for, immigrant and refugee communities.

These principles will apply until a more comprehensive policy is put in place, through the working group process laid out below.

Biometric Working Group

Through this motion, a port working group is established to develop further recommendations governing port policy related to use of public-facing biometric technology, which shall be submitted to the commission by the end of the first quarter of 2020. Issues to be addressed by this working group include the following:

- the strategic use and objectives of biometrics;
- procurement;

- transparency and accountability for biometric implementation;
- auditing of this technology to ensure compliance and accuracy, and auditing prior to approval of expansion of technology;
- commitments or agreements with airlines, cruise operators, and other port tenants and users;
- handling biometric data collected and stored from the technology;
- protection of personally identifying information;
- data security protocols and protection from unlawful or unauthorized access;
- alignment with the port's Welcoming Port Policy;
- state and federal policy priorities;
- outreach and public awareness strategy to prepare travelers and community members;
- and any other relevant topics that arise.

In addition, the working group should develop a comprehensive list of known public-facing biometric implementation being planned at port facilities over the next five years.

The working group will include, but not be limited to, representatives from the following port departments: Aviation Security; Aviation Operations; Airport Innovation; Maritime Security; Maritime Operations; Commission Office; Office of Equity, Diversity, and Inclusion; Information and Communications Technology; Information Security; Government Relations; Legal; and Police. The working group shall also engage active participation from an advisory group comprised of community partners, travelers, maritime and aviation industry partners, and other impacted stakeholders. The working group shall meet at least once a month. The policy recommendations shall be delivered to commission by the end of the first quarter of 2020. The commission may create a special committee (an ad hoc, limited term commission committee) to oversee these efforts and expects a policy governing the use of public-facing biometric technology to be delivered to the commission by the end of the second quarter of 2020.

Implementation of Public-Facing Biometric Technology at Port facilities

Upon adoption of the port's policy by the end of the second quarter of 2020, public-facing biometric technology may be implemented at port facilities if it demonstrates alignment with biometric principles and meets the port's operational requirements. Port leadership will implement an approval process for any proposals for new or expanded use of public-facing biometric technology to ensure alignment with these principles. Any proposal for new or expanded use of public-facing biometric technology will be communicated in advance directly to the port commission and through the port's external communications channels. The use of public-facing biometric technology at port facilities is subject at all times to the port's requirements. The port's biometric policies should be incorporated into commitments or agreements governing the use of biometric technology at port facilities.

Because the port does not have jurisdiction over the use of biometrics by the federal government at our facilities, the port will communicate these principles to CBP and other federal partners such as the U.S. Transportation Security Administration (TSA) and U.S. Coast Guard. We will not only notify them of our desired standards, but also work with these agencies and Congress to ensure that federal programs in place at port facilities are aligned as closely as possible with port policy regarding utilization of public-facing biometric technology.

STATEMENT IN SUPPORT OF THE MOTION

Due to technological advances, perceived customer benefits, and federal requirements, there will be a significant increase in public-facing facial recognition technology deployment by public and private sector users over the next few years, including in airport and seaport settings that will impact travelers and other visitors to our facilities. In advance of this expansion, the port commission believes that it has an obligation to institute proper policy frameworks and clear guidelines to reduce potential misuse and abuse, while improving public understanding of the benefits and risks. Specifically, the port must ensure individual privacy, civil liberties, and equity, and that biometric technology and use of the associated data is aligned with state and federal laws intended to protect those rights.

Biometrics are used in various forms at the port's aviation and maritime facilities:

- Across the port, port-issued identification cards currently utilize fingerprint biometrics to access secure or restricted areas or to permit authorized personnel access to port facilities outside of normal business hours or in locations where there is no other monitoring of access. In addition, 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.
- At Seattle-Tacoma International Airport (SEA), airport employees are required to scan their fingerprint at many secure doors throughout the facility. SEA also offers travelers the option of using CLEAR to validate the identity of a traveler as they process through TSA checkpoints using biometric technology instead of using traditional identification and validation methods.
- On the maritime side, biometric data is required by federal regulation for issuance of TSA-issued Transportation Worker Identification Credential (TWIC) smart cards that are required to access maritime facilities regulated by the U.S. Coast Guard and cruise terminal operational areas. In addition, the cruise industry is increasingly taking advantage of biometrics as a passenger facilitation tool; for example, Norwegian Cruise Line and CBP have partnered for use of facial recognition for disembarkation of guests at Pier 66.

One of the leading drivers of the expected deployment of public-facing biometrics over the next few years is implementation by CBP of a Congressionally mandated biometric exit-entry screening process for international air passengers. SEA's International Arrivals Facility will incorporate facial recognition for almost all arriving passengers (other than those U.S. citizens who opt out), and CBP is working with the port and its airline partners to incorporate this technology into departing international passenger processes.

Facial recognition is also increasingly being utilized by the port's private sector partners. Delta Air Lines opened the first full biometric airport terminal in Atlanta in November 2018, and is working to bring aspects of their "curb to gate" experience to SEA. Similarly, many of the port's cruise partners are working to streamline the check-in and boarding process for their travelers through facial recognition.

Some members of the public and various advocacy organizations have expressed concerns about the rapidly expanding use of facial recognition. These stakeholders have raised issues around privacy, equity, and civil liberties, although their main focus has been on broad law enforcement use of this technology for "mass surveillance" rather than the kind of customer facilitation uses that are being considered at port facilities. They view the use of appropriate regulation to ensure protections against abuse, discrimination, and unintended consequences to be a condition for approval of the use of these technologies.