To: Port of Seattle Commissioner Ryan Calkins, Port of Seattle Commissioner Sam Cho
From: Eric Schinfeld, Veronica Valdez
Date: September 30, 2020
RE: **Completion of the Biometrics Policy Recommendation Process**

Overview
On December 10, 2019, the Port of Seattle Commission passed Motion 2019-13 (see Attachment A) adopting guiding principles for the public-facing use of biometric technology at Port facilities and directing Port staff to develop policy recommendations in collaboration with a Biometrics External Advisory Group (see Attachment B) that translate the guiding principles into tangible and enforceable Port policies.

Port staff identified five "use cases" for public-facing biometrics at Port facilities and drafted policy recommendations for each use case:

- Biometric Air Exit
- Biometrics for Law Enforcement & Security Functions
- Biometrics for Traveler Functions Using Private, Proprietary Systems (see Attachment C)
- Biometrics for Traveler Functions Using Government Systems (see Attachment D)
- Biometrics for Air & Cruise Entry (see Attachment E)

Biometric Air Exit was the first use case reviewed, and policy recommendations for this use case were approved by the Commission on March 10, 2020.[1] Policy recommendations for the Law Enforcement & Security Functions use case were tabled in response to the Commission's July 14, 2020 action[2] to extend the moratorium for this use, and have not been vetted at all by external stakeholders. *Therefore, the below summary and attached documents encompass the remaining three uses case policy recommendations developed by Port staff in consultation with the Biometrics External Advisory Group.*

It is important to note that not all members of the Biometrics External Advisory Group agree with the policy recommendations being submitted, for a wide range of reasons: from some stakeholders who see these recommendations as overly limiting and proscriptive, to other stakeholders believe the current state of facial recognition technology is incompatible with the Commission's Biometric Principles and should be banned for all uses at Port facilities. To that end, all stakeholder concerns are being submitted along with the staff recommendations to provide full transparency, and to give the Commission the full scope of information to make final decisions on next steps. *We have also offered external advisory group members the opportunity to submit their own letters – outlining changes they think should be made to the specific use case recommendations and/or reasons they think the entire approach should be different (see Attachment F).*

Finally, these recommendations are not meant to suggest that the Port *should* implement public-facing biometrics, but rather how to do so in alignment with our guiding principles if the Commission decides it is appropriate. Ultimately, it is the Commission's discretion to 1) accept these recommendations as is, 2) amend them as desired, or 3) table them for future consideration. If tabled, the Port and private sector operators will not implement any new public-facing biometric technologies at Port facilities until policies are approved.

---

[1] External Advisory Group review of the Biometric Air Exit use case was artificially truncated due to the Commission's March action; the original plan to submit all use cases to the Commission at the end of the process was changed when the Commission decided to proceed in reaction to US Customs and Border Protection's implementation of their own biometric air exit efforts at SEA. **Stakeholders did not get to fully vet or provide final input into these use case policies, and some believe that approval of these polices should be revisited.**
[2] Item 1g.

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, public-facing 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 the potential for a faster and more efficient travel experience, as well as the belief that it offers a more accurate security process than human review of documents. 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.

It is important to note that the COVID-19 pandemic has also increased interest in "touchless technologies" as a way to reduce potential transmission of disease. Facial recognition is certainly one technology that could reduce direct interactions like handing documents back-and-forth or touching screens. To that end, it is even more important that the Port have policies in place to govern these technologies if it is decided that they are needed.

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. Since the start of 2020, 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.

To that end, Port staff divided the recommendations into five use cases:

1) **Biometric Air Exit:** This is the use of biometrics, specifically facial recognition technology, to verify the identity of departing international air passengers using US Customs & Border Protection's (CBP) Traveler Verification System (TVS). *The policy recommendations for this use case were approved by the Port Commission on March 10, 2020, and implemented as Executive Policy.*

2) **Biometrics for Law Enforcement & Security Functions:** This would be the use of biometrics, including facial recognition, to perform public-facing law enforcement and security functions at Port facilities. On

July 14, 2020, the Port Commission extended its moratorium on these uses as part of its motion on assessing Port policing. *Therefore, staff did not vet its policy recommendations with the Biometrics External Advisory Group, and is not transmitting those recommendations to Commission.* If and when the Commission wishes to revisit the issue, Port staff will vet its draft policy recommendations with external stakeholders at that point.

3) **Biometrics for Traveler Functions Using Private, Proprietary Systems:** This set of recommendations is specific to any proposed use of biometrics for traveler functions by private-sector entities using proprietary systems. CLEAR is an example of this application. Examples of other potential future biometric applications for traveler functions could include boarding of departing cruise ships or domestic flights; ticketing and bag-check for airlines or cruise lines; access to tenant-controlled facilities such as an airline passenger lounge; access to a rental car at the Port's rental car facility; or use of biometrics for payment at airport restaurants or retail stores in lieu of credit card or cash.

4) **Biometrics for Traveler Functions Using Government Systems:** While most private sector uses would not be relevant to this use case, there are limited examples where a private sector entity might wish to use an existing government biometrics system, such as an airline using CBP's Traveler Verification System for international departing passenger ticketing or bag check. The Port itself could also choose to utilize biometrics for traveler functions, such as access to its parking garage; any Port use of biometrics utilizing a Port-controlled system is by definition a use of a government system, and therefore included in this use case.

5) **Biometrics for Air & Cruise Entry:** These recommendations are specific to CBP's use of biometrics, specifically facial recognition, utilizing their Traveler Verification System 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. The Port has no jurisdiction over these activities, but can still play an important transparency and accountability role.

Policy recommendations for use cases 3, 4 and 5 are the ones being transmitted to the Port Commission in the attached document.

Process

Almost as important as the outcomes of the Biometrics External Advisory Group is the process used to achieve these recommendations. The Port Commission has held multiple public meetings and study sessions on this topic, and the Port hired an outside facilitation firm to manage the advisory group process – to ensure full and equal participation from all stakeholders. Below is a list of all public and advisory group meetings that helped inform Port staff efforts to develop these recommendations.

- September 10, 2019: First Commission Study Session on Biometric Technology
- October 29, 2019: Second Commission Study Session on Biometric Technology
- December 10, 2019: Commission Public Meeting action on Biometrics Principles Motion
- January 17, 2020: External Advisory Group meeting #1
- February 7, 2020: External Advisory Group meeting #2
- February 18, 2020: Commission Biometrics Special Committee meeting
- February 25, 2020: Commission Public Meeting briefing on Biometric Air Exit policy recommendations
- March 6, 2020: External Advisory Group meeting #3
- March 10, 2020: Commission Public Meeting action on Biometric Air Exit policy recommendations

- March 31, 2020: Commission Biometrics Special Committee meeting
- April 14, 2020: Commission Public Meeting action to extend deadlines for policy recommendations
- July 10, 2020: External Advisory Group meeting #4
- July 24, 2020: External Advisory Group meeting #5
- August 7, 2020: External Advisory Group meeting #6
- August 21, 2020: External Advisory Group meeting #7
- September 25, 2020: External Advisory Group meeting #8

Summary of Recommendations
Before sharing specific recommendations, Port staff want to be very clear that these proposed policy recommendations do not reflect a consensus of the feedback received from the Biometrics External Advisory Group. **Stakeholders brought various perspectives to the table and many fell into one of two groups: 1) those that believe biometric technology is a benefit to travelers that does not require significant regulation or oversight by the Port, and 2) those that believe biometrics, particularly facial recognition, are fundamentally flawed, inequitable and unethical, and should be banned entirely from Port facilities.**

However, the Port staff still believe that the Biometrics External Advisory Group process was highly productive. Feedback from stakeholders was incorporated into the policy recommendations in substantive and tangible ways, and the staff recommendations are much improved due to their input. Staff believes that these recommendations set a high standard for when, where, and how biometrics could be used in public-facing ways at Port facilities, and that these recommendations are responsive to the Commission direction in Motion 2019-13 to translate the biometric principles into tangible, enforceable policies.

As mentioned above, there are substantive differences between each of the use cases based on issues such as how much control the Port has over the potential application; whether the application is regulated in some way by state or federal law; and what the specific uses are. However, a large majority of the policy recommendations are consistent across multiple use cases.

For the "Biometrics for Traveler Functions Using Private, Proprietary Systems and the "Biometrics for Traveler Functions Using Government Systems" use cases, the recommendations can generally be summarized as follows:

Justified
- If the Port has the ability to approve an application, the relevant Managing Director should consider certain criteria in deciding whether or not to approve the implementation, and consult with a newly created Technology Ethical Advisory Board. If the risks from the biometric implementation are deemed significant, then the Managing Director should deny the application.
- If the Managing Director plans to approve the request, they must first notify the Port's Executive Director and the Port Commission at least three (3) weeks in advance before providing that formal approval, and/or go through a Commission approval process. In specific circumstances, Port staff should also undergo a community engagement process before seeking Commission approval.

Voluntary
- When the Port has jurisdiction to do so, it should not approve biometrics that do not include an opt-in provision, unless there is a demonstrated need to do so, such as a public health mandate. In this context, opt-in refers to both opting-in to the overall system (enrolling your biometrics in a database or gallery) as well as opting in to participating in the system at the point of service. The Port should not

approve any applications for biometrics that operate by scanning large groups of people to identify those individuals who have opted in.

- The Port should develop guidelines for where and how biometrics can be used at Port facilities. In particular, these guidelines should include standards for "opt-in" and "opt-out"; and standards to avoid unintended image capture if facial recognition is implemented. Operators must demonstrate that they have been trained on these guidelines and standards.

Private

- When the Port has jurisdiction to do so, the Port should develop and enforce minimum biometric data security and privacy standards.

Equitable

- The Port should develop biometric training guidelines for personnel who will be administering biometric technology on travelers. The training must include, but not be limited to, the capabilities and limitations of biometrics, as well as how to deal with mismatching issues with sensitivity and discretion. All operators must demonstrate that they have received this training.
- Applications for use of this technology must demonstrate that it performs at high levels of accuracy both overall and between various characteristics, particularly those relevant to biometric identification, as identified under the Washington state definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions. Applicants must agree to 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.

Transparent

- The Port should develop a comprehensive communications plan that notifies the general public of the implementation of public-facing biometrics at Port facilities, and all related information. The Port should also produce an annual accountability report that includes all approved, publicly available information.
- The Port should periodically conduct its own performance evaluation, within the limitations of its authority, to ensure that Port employees and/or private sector operators are following all Port policies.

Legal

- Before the Port approves the implementation of public-facing biometrics, it must ensure that the proposal complies with all relevant state and federal laws, including privacy and discrimination laws.
- Port staff should actively track, and work with stakeholders to advocate for, state and federal laws and regulations that codify the goals of the Port's biometric principles.

Ethical

- The Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about any biometric programs.
- The Port should require that operators do not disclose personal data obtained from a biometric system to a federal or law enforcement agency, except in certain situations.
- The Port should work with local jurisdictions, nonprofit organizations and others to inform local immigrant and refugee communities 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.
- The Port should form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations.

Differences between the two use cases or variations based on the specific issues are too numerous to list in this memo, but a few examples are provided here according to the respective guiding principle:

- *Privacy:* For any proposed implementations of biometrics for traveler functions that have obligations related to U.S. Transportation Security Administration security and data privacy regulations (i.e. CLEAR), the proposal must demonstrate full alignment with the Port's Air Security Program rules and requirements.
- *Justified:* If Port staff receive approval from the Managing Director to implement biometrics other than biometric air exit, they must then submit a notice of intent to the Port Commission and commence an accountability report process as defined in state law that publicizes key aspects about the biometric technology.
- *Lawful:* For airlines proposing to use CBP's Traveler Verification System, they must also include documentation of their compliance with CBP's Business Requirements.

For the "Biometrics for Air & Cruise Entry" use, the recommendations can generally be summarized as follows:

Justified

- The Port should include the specific federal laws and statutes that allow CBP to implement biometrics at Port facilities in the annual accountability report so that travelers and the public understand.

Voluntary

- The Port should develop recommendations to CBP for their consideration regarding ways to avoid unintended image capture at Port facilities.
- The Port should continue to pursue whether opt-in 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.

Private

- The Port should request CBP audit reports on biometric entry systems on a regular basis and include appropriate information in the Accountability Report.

Equitable

- The Port should request biometric program accuracy rates from CBP on an annual basis.
- 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.
- The Port should develop suggested biometric training guidelines for personnel who will be administering the facial recognition technology on travelers, and how to deal with mismatching issues with sensitivity and discretion. The Port should share its training guidelines, specifically related to "cultural sensitivity and discretion", with CBP and cruise lines for their voluntary adoption.

Transparent

- The Port should request that CBP notify the Port if and when they intend to conduct biometric entry.
- The Port should develop a comprehensive communications plan that notifies the general public of the implementation and all related information.
- The Port should produce an annual accountability report that includes all approved, publicly available information.

Lawful

- Port staff should actively track and work with stakeholders to advocate for federal laws and regulations that support the Port's biometric principles. The Port should also identify existing pieces of legislation to support.

Ethical

- 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 and how to report incidents – in multiple languages and in culturally appropriate ways.

Conclusion

Over the last year, the Port Commission has heard passionate testimony from all sides of the biometrics issue. There are strongly held and divergent views on the efficacy, ethics, and justification for implementing public-facing biometrics at Port facilities. Therefore, it is incumbent on the Port to be thoughtful, transparent, and accountable in its decisions about whether or not to allow this technology to move forward.

As per Motion 2019-13, the policy recommendations for the three attached use cases shows how to implement public-facing biometrics technology at Port facilities in alignment with guiding principles if and when the Commission deems it appropriate. *In no way do these policy recommendations recommend the implementation of public-facing biometric technology at Port facilities.* Each proposal to use public-facing biometrics at Port facilities will need to be judged on its own merits, including the risks and benefits to the travelling public.

Staff is available to answer any questions about the specific recommendations, the process undertaken to achieve these recommendations, or proposed next steps.

Attachment A – Motion 2019-13: Commission Biometric Principles

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.

Attachment B – Port of Seattle 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
- Clay Thomas, Area Port Director, Area Port of Seattle, 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
- Brianna Auffray, Legal & 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

*Additional participants from these organizations also contributed.

Attachment C – Policy Recommendations for Biometrics for Traveler Functions by Private Sector Entities Using Proprietary Systems

1. BASICS OF BIOMETRICS FOR TRAVELER FUNCTIONS USING PRIVATE-SECTOR PROPRIETARY SYSTEMS

Some private sector operators at Port facilities see biometrics as a tool to automate and expedite normal customer functions. These potential uses are driven entirely by perceived efficiency or effectiveness, and not required by any local, state or federal regulation. The Port has significant control over whether and how these companies can implement biometrics for these purposes at Port facilities.

There are only a few current applications of biometrics for this kind of use at SEA, most notably CLEAR, which allows travelers to use fingerprint and iris scans as identity verification to advance to the front of TSA checkpoints. Examples of other potential future biometric (including facial recognition) applications for traveler functions could include:

- Boarding of departing domestic flights, or departing cruise ships;
- Ticketing and bag-check for airlines or cruise lines;
- Access to tenant-controlled facilities such as an airline passenger lounge;
- Access to a rental car at the Port's rental car facility;
- Use of biometrics for payment at airport restaurants or retail stores in lieu of credit card or cash; or
- Use of biometrics to inform dynamic signage targeting information or advertisements to travelers.

The COVID-19 pandemic may spur additional attention toward potential applications of biometric technology so as to avoid direct interactions that could spread the virus. To that end, it is even more important for the Port to anticipate potential needs and provide clear policy guidance.

In March 2020, the Washington State Legislature passed legislation explicitly setting policy guidelines for use of facial recognition biometrics by state and local governments; it did not pass legislation regulating private sector usage. However, the policy recommendations below reflect many of the policies that were considered by the State Legislature for private sector operators, so that – if state laws are eventually enacted regulating private sector use of facial recognition biometrics – Port policies already either meet or exceed those thresholds.

2. APPLYING THE PORT'S PUBLIC-FACING BIOMETRICS GUIDING PRINCIPLES TO THE USE OF BIOMETRICS FOR TRAVELER FUNCTIONS BY PRIVATE SECTOR ENTITIES USING PROPRIETARY SYSTEMS

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) requiring an explicit operational reason to use biometrics that outweighs potential risks, 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 reason, private sector operators would point to increased processing speeds and customer conveniences such as not having to take identification documents out. In addition, the

COVID-19 pandemic may spur additional attention toward potential applications of biometric technology so as to avoid direct interactions that could spread the virus. However, there needs to be a net benefit for the use of this technology to be considered a justified use; in other words, the benefits should outweigh potential costs like cybersecurity, data privacy risks, and any other potential harm that customers might experience from biometrics.

The Port does not condone mass surveillance, and so any proposed biometrics would only fit this definition if all biometric capture was done with an individual's awareness and willing participation. For example, the use of dynamic signage to personalize advertising to a traveler would not fit with this principle unless that person previously agreed to have their biometrics used in this way and the system doesn't scan other people in the process of looking for those who have opted-in; for example, someone would have to walk up directly to a screen and actively request targeted advertising from a system that they previously opted-in to.

Recommendations for protecting against unintended image capture of other individuals are included under the Voluntary principle.

2. Working Group Recommendations

"Justified" recommendations at a glance	
Port	Private Sector
• If a Port Managing Director receives a request by a private sector operator for implementation of biometrics for traveler functions using a proprietary system (or continuation in the case of a biometrics operator already operating at Port facilities prior to December 10, 2019), the Managing Director must seek feedback from the Technology Ethical Advisory Board and consider set criteria in deciding whether or not to approve the implementation. • If the Managing Director plans to approve the request, they must first notify the Port Executive Director and the Port Commission at least three (3) weeks before providing that formal approval to the private sector applicant. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through the performance evaluation process.	• A private sector operator proposing to implement biometrics for traveler functions at Port facilities using a proprietary system must receive approval from the relevant Managing Director. • A private sector operator already operating biometrics for traveler functions at Port facilities prior to December 10, 2019 must apply for approval from the Managing Director for continued operation at least six months in advance of the expiration of its existing lease, contract or operating agreement. • A private sector operator may not propose to implement biometrics explicitly for marketing or advertising purposes, unless it meets set criteria.

For Port

Recommendation 1a: If the Port's Aviation Managing Director, Maritime Managing Director or Economic Development Managing Director receives a request by a private sector operator for implementation of biometrics for traveler functions using a proprietary system (or continuation in the case of a biometrics operator already operating at Port facilities prior to December 10, 2019), the Managing Director must seek feedback from

the Technology Ethical Advisory Board and consider the following criteria in deciding whether or not to approve the implementation:

- Demonstrated operational benefit, which is defined as increased efficiency or effectiveness in passenger processing vs existing manual processes
- Compliance with all Port principles and policies
- Alignment with the Port's Equity, Diversity and Inclusion standards
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation vs. potential privacy and other risks. If the risks are deemed significant, then the Managing Director should deny the application regardless of the net-benefit calculation; "significant risk" should be clearly defined in partnership with the Technology Ethical Advisory Board, to include harms based on equity impacts.

Recommendation 2: If the Managing Director plans to approve the request after considering all of the above criteria, they must first notify the Port Executive Director and the Port Commission at least three (3) weeks before providing that formal approval to the private sector applicant; this notification is for the purpose of the Executive Director and/or Commission to ask additional questions, request a delay in approval until additional information is received, and/or reject the Managing Director's recommendation for approval. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through the performance evaluation process.

For Private Sector Operators

Recommendation 1b: A private sector operator proposing to implement biometrics for traveler functions at Port facilities using a proprietary system must receive approval from the relevant Managing Director. The request for this implementation must articulate how the operator will comply with the Port's Biometric Principles and any associated policies governing the use of biometric technology at Port facilities. In addition, it must explicitly state why biometrics are justified, using the above-listed criteria.

Recommendation 1c: A private sector operator already operating biometrics for traveler functions at Port facilities prior to December 10, 2019 must apply for approval from the relevant Managing Director for continued operation at least six months in advance of the expiration of its existing lease, contract or operating agreement, or within 6 months of the effective date of this policy, whichever is later. Port staff will be responsible for notifying the operator of the deadline, the biometrics approval process and all associated policies. The operator's request for continued operation must explicitly articulate how the service does or will comply with the Port's Biometric Principles, any associated policies governing the use of biometric technology at Port facilities, and why biometrics are justified, using the above-listed criteria.

Recommendation 1d: A private sector operator may not propose to implement biometrics explicitly for marketing or advertising purposes, unless:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;
- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and
- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

3. Stakeholder Concerns

- Stakeholder feedback: Justified principle should apply an equity perspective and should go beyond "operational benefit" to address and advance justice.
    - Port staff response: Added a criterion in Recommendation 1a that the application should be in alignment with the Port's Equity, Diversity and Inclusion standards
    - Added a requirement in Recommendation 1a that – if the risks are deemed significant – then the Managing Director should deny the application regardless of the net-benefit calculation.

- Stakeholder feedback: Port confirmed there will be no grandfathering-in of existing systems once the policies are approved. Will there be a suspension period?
    - Port staff response: Added recommendation 1c to address this concern.

- Stakeholder feedback: Regarding 1c, do existing operators require a one-time approval or each time a renewal approaches?
    - Port staff response: All approvals are one-time, unless a significant change occurs. Added to recommendations 1a and 2.

- Stakeholder feedback: It should be the responsibility of the Port to notify existing biometric operators when they are six months from their renewal date, in order for them to participate in the biometrics approval process identified in 1c.
    - Port staff response: Agreed, and updated accordingly.

- Stakeholder feedback: The Managing Directors have a lot of power to approve or deny; is there anyone else with veto power?
    - Port staff response: The Executive Director and Commission. Made this more explicit in recommendation 2.

- Stakeholder feedback: The phrase "if the risks are deemed significant" should be clearly defined around a set of criteria, most importantly including equity impacts.
    - Port staff recommendation: Added a process for developing that definition in recommendation 1a.

- Stakeholder feedback: The Port should not allow the use of biometrics-based advertising technology.
    - Port staff recommendation: Port staff appreciates the concerns, but rather than explicitly ban a particular function we believe we should very clearly define how such a function would only be in compliance with Port principles and policies in very limited scenarios. Added recommendations 1d and 5.

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.

The Port should not approve any private sector applications for biometrics for traveler functions at Port facilities using proprietary systems that are not opt-in for travelers, unless there is a legally-required mandate to do so – such as from a federal agency or a public health entity. In this context, opt-in refers to both opting-in to the overall system (enrolling your biometrics in a database or gallery) as well as choosing to participate in the system at the point of service (i.e. – at the ticketing counter).

In these limited scenarios for which opt-out is mandated, the Port should require reasonable provisions for those travelers that would like alternate accommodations.

As related to unintended image capture, the Port can specify requirements for the physical configuration and other aspects of the technology in an effort to prevent unintended image capture during biometric operations. Similarly, the Port should set standards for how unintended images are removed from the system.

2. Working Group Recommendations

"Voluntary" recommendations at a glance	
Port	Private Sector Operators
• The Port should not approve any applications by private sector entities for biometrics for traveler functions that are not "opt-in", unless there is a legally required mandate to do so. • The Port should develop guidelines for where and how biometrics can be used at Port facilities. In particular, these guidelines should include standards for "opt-in" and "opt-out", and standards to avoid unintended image capture as well as standards for how to handle biometric data accidentally collected by unintended capture. • The Port should not approve any applications for biometrics for traveler functions that scan individuals or groups without their knowledge and active participation.	• A private sector operator may not refer to a system as "opt-in" unless it meets set criteria. • As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must submit a plan for implementing "opt-in" or "opt-out" aligned with Port standards, and (if using facial recognition) for minimizing unintended capture of biometrics aligned with Port guidelines. • As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must demonstrate that their employees have received training aligned with the Port's guidelines.

For Port

Recommendation 3a: The Port should not approve any applications by private sector entities for biometrics for traveler functions that are not "opt-in", unless there is a legally-required mandate to do so – such as from a federal agency or a public health entity. In the limited scenarios for which opt-out is mandated, the Port should require reasonable provisions for those travelers that would like alternate accommodations. In this context, opt-in refers to both opting-in to the overall system (enrolling your biometrics in a database or gallery) as well as actively choosing to participate in the system at the point of service. Opting-in also must include comprehensive, clear, and accessible notice at the time of enrollment (i.e. – "informed consent") for individuals to know exactly

what they are opting-in for, how their data will be handled and protected and their rights to remove their data from the system.

Recommendation 4a: The Port should develop guidelines for where and how biometrics can be used at Port facilities. In particular, these guidelines should include:

- Standards for "opt-in" and "opt-out" to ensure a consistent customer experience, including how to cancel a subscription or other voluntary commitment such that an individual's biometric data is removed from the system; and
- Standards to avoid unintended image capture if facial recognition is implemented (such as by positioning a 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), as well as standards for how to handle biometric data accidentally collected by unintended capture.

Recommendation 5: The Port should not approve any applications for biometrics for traveler functions that scan individuals or groups without their knowledge and active participation. In particular, the Port should not approve any applications that operate by scanning large groups of people who have not opted-in in order to identify those individuals who have opted in.

For Private Sector Operators

Recommendation 3b: A private sector operator may not refer to a system as "opt-in" unless:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;
- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and
- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

Recommendation 4b: As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must submit a plan for implementing "opt-in" or "opt-out" aligned with Port standards, and (if using facial recognition) for minimizing unintended capture of biometrics aligned with Port guidelines.

Recommendation 4c: As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must demonstrate that their employees have received training aligned with the Port's guidelines.

3. Stakeholder Concerns

- Stakeholder feedback: Although the system is opt-in, it is unclear how or the extent to which a consumer can voluntarily remove themselves from the system.
    - Port staff response: This is explicitly included in Recommendations 3a, 4a and 10.

- Stakeholder feedback: Regarding recommendation 3a, "consensus national best practice" does not seem limiting enough and should be refined.
    - Port staff response: This phrase has been removed.

- Stakeholder feedback: The language around a mandate to do "opt-out" should be more specific.
    - Port staff response: Updated recommendation 3a.

- Stakeholder feedback: Recommendation 5 should explicitly ban all mass scanning, which is surveillance.
    - Port staff response: Agreed; only those individuals who are actively participating should be included in biometric data collection. Updated the recommendation accordingly.

- Stakeholder feedback: Opting-in to the system should include there being a voluntary subscription, and that the operator should not collect biometrics using an involuntary method.
    - Port staff response: Added recommendation 3b to make this explicit.

- Stakeholder feedback: What does it mean to "opt-in at the point of service"?
    - Port staff response: Opting-in at the point of service is meant as "actively participating in using the biometrics" (vs. being scanned without your awareness); it is not meant to imply that you have to sign up for the service each time you use it. Opting-in to the enrollment process happens once, and is defined here as choosing to provide your biometrics into the system/gallery. Adjusted recommendation 3a to make this clearer.

- Stakeholder feedback: Add a recommendation that includes comprehensive, clear, and accessible notice for passengers to know exactly what they are opting-in for at the time of enrollment.
    - Port staff response: Updated recommendation 3a.

- Stakeholder feedback: Need mechanisms for how to address what happens when unintended capture occurs.
    - Port staff response: Updated recommendation 4a.

- Stakeholder feedback: Should have an explicit requirement about the ability for individual to withdraw from the system.
    - Port staff response: Updated recommendation 4a.

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 implementation. Individuals want to know that their data is secure, not being used for any inappropriate purpose, and protected.

The Port has some ability to set and enforce minimum data privacy and cybersecurity standards for private sector operators at Port facilities through lease agreements or vendor contracts. For vendors like CLEAR that have obligations related to U.S. Transportation Security Administration security and data privacy regulations, the Port has the ability to ensure compliance with all Air Security Program rules and requirements.

The issue of giving individuals an opportunity to challenge violations of their rights is covered under the Ethical principle.

2. Working Group Recommendations

"Private" recommendations at a glance	
Port	Private Sector Operators
• The Port should develop minimum biometric data security and privacy standards for all private sector operators proposing to utilize biometrics for traveler functions.	• For any proposed private sector implementation of biometrics for traveler functions, the proprietary system must meet or exceed the Port's minimum standards for biometric data security and privacy guidelines. • For any proposed implementations of biometrics for traveler functions that have obligations related to U.S. Transportation Security Administration security and data privacy regulations, the proposal must demonstrate full alignment with all of the Port's Air Security Program rules and requirements.

For Port

Recommendation 6a: The Port should develop minimum biometric data security and privacy standards for all private sector operators proposing to utilize biometrics for traveler functions at Port facilities. Those standards should address data privacy protections at the point of service as well as throughout the proprietary system, such as potential data breach and data sharing. The standards should include requirements that any data collected should be used only for those purposes explicitly communicated to those individuals who participate in the biometric process, and that unauthorized third parties will not have access to or be sold any such data. These guidelines should be based – to the extent possible – on national and global standards already developed for evaluating the security of these technologies, such as the Center for Internet Security's Controls and Benchmarks or any relevant statues from the California Consumer Privacy Act, the European Union General Data Protection Regulation or Section 15 of the State of Illinois' Biometric Information Privacy Act.

For Private Sector Operators

Recommendation 6b: For any proposed implementation of biometrics for traveler functions, the proposal must meet or exceed the Port's minimum biometric data security and privacy standards.

Recommendation 6c: For any proposed implementations of biometrics for traveler functions that have obligations related to U.S. Transportation Security Administration security and data privacy regulations[3], the proposal must demonstrate full alignment with all of the Port's Air Security Program rules and requirements.

3. Stakeholder Concerns

- Stakeholder feedback: Need to consider privacy impacts both at the point of service & externalities regarding data usage and protection beyond the system.
    - Port staff response: Added this explicitly into Recommendation 6a.

[3] i.e. - CLEAR

- Stakeholder feedback: Should clearly call out that a private entity cannot sell your data to a third-party entity for any purpose.
    - Port staff response: Added to recommendation 6a.

- Stakeholder feedback: We should include Illinois' Biometric Privacy Act as a source for such policies.
    - Port staff response: Section 15 of the law is the one that deals with retention; collection; disclosure; and destruction of biometric information. It seems to be already quite aligned with the Port's proposed policies, and so we have added a reference to that section.

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 biometrics (specifically facial recognition technology) does not perform as effectively on individuals who are not male Caucasians, and that 2) regardless of why the technology identifies a mismatch, systems should be in place to resolve the issue with minimal impact to the customer.

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.[4] However, the NIST report does identify some algorithms as highly effective in terms of accuracy rates – both overall and across multiple characteristics. The NIST report provides an important baseline for performance levels that proposed implementations of biometric technology at Port facilities should meet to be considered for approved use at Port facilities.

Treating no-matches or mismatches with "cultural sensitivity and discretion" requires that individuals subject to additional document review are treated 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 customer. Where possible, mismatch issues should be handled at the point of service rather than removal to a secondary location. The Port also has an obligation to institute and/or ensure compliance with standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality.

2. Working Group Recommendations

"Equitable" recommendations at a glance	
Port	Private Sector Operators
• The Port should develop biometric training guidelines for personnel who will be administering biometric technology on travelers.	• When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their employee training for operating biometrics meets the Port's training guidelines.

[4] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

	• When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their technology demonstrates high levels of accuracy both overall and between various characteristics. • A private sector operator requesting implementation of biometrics for traveler functions must agree as a part of its application to make available an application programming interface (API) or other technical capability.

For Port

Recommendation 7a: The Port should develop biometric training guidelines for personnel who will be administering biometric technology on travelers. The training must include – but not be limited to – the capabilities and limitations of biometrics, as well as how to deal with mismatching issues with sensitivity and discretion; the Port's Office of Equity, Diversity and Inclusion should be an active participant in ensuring culturally appropriate procedures for handling such issues. For example, the training should suggest that – where possible – mismatch issues should be handled at the point of service rather than removal to a secondary location. The training should also include standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality.

For Private Sector Operators

Recommendation 7b: When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their employee training for operating biometrics meets the Port's training guidelines, including understanding of the capabilities and limitations of biometrics, and how to deal with mismatching issues with sensitivity and discretion.

Recommendation 8: When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington State definition of "protected class."[5] These demonstrations of accuracy must result from testing in operational conditions. "High levels of accuracy" should be defined not only relative to correctly matching the person with their image but also as an accuracy rate that is at least as good as human review. Where possible, the operator should include in their disclosure of accuracy rates the specific device and system settings – such as similarity thresholds – that maximize accuracy and provide the proper balance of accuracy, equity and security.

Recommendation 9: A private sector operator requesting implementation of biometrics for customer functions must agree as a part of its application to 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. Making an application

[5] The groups protected from discrimination by law. These groups include men and women on the basis of sex; any group which shares a common race, religion, color, or national origin; people over 40; and people with physical or mental handicaps.

programming interface or other technical capability does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data; providers bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing.

3. Stakeholder Concerns

- Stakeholder feedback: In general, high accuracy rates should not be a definition for equity. What constitutes a "high accuracy rate" needs to be clear, implementable, and considerate of relative differences between groups.
    - Port staff response: Added equity as a fundamental criterion under Recommendation 1a. Port staff is open to using a more specific/quantifiable definition of "high accuracy rate," and welcomes feedback on what that might be.

- Stakeholder feedback: Recommendation to use Washington State's definition of "protected class" rather than the federal definition. Selection should be made for the protected classes that are most relevant to biometric (including facial recognition) accuracy.
    - Port staff response: Changed in Recommendation 8.

- Stakeholder feedback: Trainings should be developed in consultation with civil rights organizations and made publicly available.
    - Port staff response: Added the Port's Office of Equity, Diversity and Inclusion to this process in recommendation 7a; making the training guidelines public is included in recommendation 11a.

- Stakeholder feedback: The Port needs to set an "acceptable" level of difference between overall accuracy rates, and the accuracy rate of the system for various demographics (i.e. – how much less accurate can the system be for people of color and yet still be approved).
    - Port staff response: As referenced above, the Port requires the system to be "highly accurate" for all groups, both overall and within specific demographics. No system will be approved that isn't highly accurate for all individuals. We are still open to suggestions for making this more quantifiable.

- Stakeholder feedback: Accuracy rates should be publicly communicated, specifically regarding how accurate the system is for differing groups.
    - Port staff response: This is included in the annual accountability report in recommendation 11a.

- Stakeholder feedback: Would like to see language here about what oversight there will be over similarity thresholds as different thresholds will skew towards either false matches or mismatches.
    - Port staff response: Added language to recommendation 8, and to the accountability report in recommendation 11a for public disclosure.

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 biometrics for traveler functions at Port facilities to be clearly communicated to anyone visiting Port facilities, 2) the need to ensure that travelers participating in biometrics for these functions are informed in a clear, concise manner about how the biometrics are used, and their rights related to the system, and 3) the need for accountability reports to be created and published for the public. This requires clear, consistent and standardized communications protocols, in coordination with private sector operators.

Similarly, information about the system must be continuously verified. Performance data should be a key aspect of the Port's review of any biometric implementation taking place at its facilities, and publicly verified and approved findings should be made public.

2. Working Group Recommendations

"Transparent" recommendations at a glance	
Port	Private Sector Operators
• If the Port approves the implementation of any biometrics for traveler functions, it should develop a comprehensive communications plan. • If the Port approves the implementation of any biometrics for traveler functions, the Port should work with the Technology Ethical Advisory Board to produce an annual accountability report. • The Port should periodically conduct performance evaluations to ensure that private sector operators are following all Port policies. If private sector operators are consistently violating the Port's policies after more than two notifications asking for corrective action, the Port reserves the right to withdraw its approval of the biometric implementation.	• If the Port approves the implementation of any biometrics for traveler functions, that private sector operator should partner with the Port on implementation of the Port's biometrics communications plan. • If the Port approves the implementation of any biometrics for traveler functions, the private sector operator should share to the extent possible all requested information for inclusion in the accountability report. The operator should also share, to the extent possible, the Port's annual accountability report through relevant communications channels.

For Port

Recommendation 10a: If the Port approves the implementation of any biometrics for traveler functions, it should develop a comprehensive communications plan that notifies the general public of the implementation and all related information, including their rights with regard to the program, how to remove themselves from the program, and recourse in case of violations of those rights and/or data breaches. The communications plan should include specific communications on-site, including announcements, signage, flyers and web content. The communications plan should include effort to reach local immigrant and refugee communities – in multiple languages and in culturally appropriate ways; languages should be determined based on the most common ones spoken by airport and/or cruise passengers and – if at the airport – also languages appropriate to the specific flight (as per feedback from airlines and cruise lines, as well as federal "origin and destination" data).

Recommendation 11a: If the Port approves the implementation of any biometrics for traveler functions, the Port should work with the Technology Ethical Advisory Board to 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;
- A clear use and data management policy, including protocols for:
    - How and when the service will be deployed or used and by whom including, but not limited to, the factors that will be used to determine where, when, and how the technology is deployed, and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances.
    - Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose or purposes for which the service will be used;
    - Data integrity and retention policies applicable to the data collected using the service, including how the operator will maintain and update records used in connection with the service, how long it will keep the data, and the processes by which data will be deleted;
- The Port and the private sector operator's privacy guidelines;
- Traveler rights with regard to the biometric system;
- The Port's biometric training guidelines;
- The operator'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 the Port's and the operator's rules and guidelines, including complaints alleging violations;
- Any publicly available data about the accuracy and effectiveness of the system, including accuracy overall as well as accuracy for specific demographics; and, where possible, any specific device and system settings – such as similarity thresholds – that speak to how the operator is balancing accuracy, equity and security;
- Benchmarking data against the operational results of the biometric system at other ports;
- An assessment of compliance with the Port's Biometrics Principles and policies;
- Any Port conducted performance evaluations;
- Feedback about the public's experience, sought proactively in customer surveys, including whether travelers believe that they fully understand the information about the system;
- Any available information on data sharing within the U.S. Department of Homeland Security, such as what data is requested and by whom, within the limitations of the Port to require this information; and
- Any private sector operator's disclosure of individuals' biometric data, within the limitations of the Port to access and disclose law enforcement activity.

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

Recommendation 12: The Port should periodically conduct performance evaluations to ensure that Port staff and/or private sector operators are following all Port policies, including those related to privacy, customer

service, communication and unintended image capture. In particular, the Port should ensure that images are retained no longer than necessary, and not used only for their intended purpose. For any implementations of biometrics for passenger processing that have obligations related to U.S. Transportation Security Administration security and data privacy regulations, the Port should ensure compliance with all Air Security Program rules and requirements. If private sector operators are consistently violating the Port's policies after more than two notifications asking for corrective action, the Port reserves the right to withdraw its approval of the biometric implementation.

For Private Sector Operators

Recommendation 10b: If the Port approves the implementation of any biometrics for traveler functions, that private sector operator should partner with the Port on implementation of the Port's biometrics communications plan.

Recommendation 11b: If the Port approves the implementation of any biometrics for traveler functions, the private sector operator should share, to the extent possible, all requested information for inclusion in the accountability report, including its assessment of compliance with the Port's principles and policies, and any known or reasonably suspected violations, including complaints alleging violations. The operator should also share, to the extent possible, the Port's annual accountability report through relevant communications channels.

3. Stakeholder Concerns

- Stakeholder feedback: Port should get an independent auditor to conduct the performance evaluations, to ensure objectivity.
    - Port staff response: Port staff appreciates the concern, but there is going to be significant transparency to the performance evaluations which should overcome any potential staff bias; for example, the results of the performance evaluations will be published as part of the accountability report, which will be created in partnership with the Technology Ethical Advisory Board. All Port staff programs are also subject to the review of the Port's Internal Auditor, an independent office that reports to the Commission.

- Stakeholder feedback: Communications plan should be tailored to reach diverse communities, in the same way that the outreach under the Ethical principle is articulated.
    - Port staff response: Added language to recommendation 10.

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 compliance with any relevant local, state and federal laws regarding the use of biometrics, consumer data privacy and other privacy and consumer protection laws. There are several efforts in Congress regarding regulation of biometrics use by state and local government as well as the private sector. However, there is not currently a comprehensive federal legal framework regulating biometrics and associated data; as the law develops, the Port and its private sector partners will adjust accordingly.

In March 2020, the Washington State Legislature passed legislation explicitly setting policy guidelines for use of facial recognition biometrics by state and local governments. However, private sector activity at Port facilities is not currently addressed by state law.

2. Working Group Recommendations

"Lawful" recommendations at a glance	
Port	Private Sector Operators
• Before the Port approves the implementation of biometrics for traveler functions, it must ensure that the proposal complies with all relevant state and federal laws, including privacy and discrimination laws. • Port staff should actively track and work with stakeholders to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.	• As part of its application to the Port to implement biometrics for traveler functions, a private sector operator must include its compliance with all relevant state and federal laws, including privacy and discrimination laws.

For Port

Recommendation 13a: Before the Port approves the implementation of biometrics for traveler functions, it must ensure that the proposal complies with all relevant state and federal laws, including privacy and discrimination laws. Discrimination against individuals covered by the Washington State definition of protected class is prohibited.

Recommendation 14: Port staff should actively track and work with stakeholders, including private sector operators at Port facilities, to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.

For Private Sector Operators

Recommendation 13b: As part of its application to the Port to implement biometrics for traveler functions, a private sector operator must include its compliance with all relevant state and federal laws, including privacy and discrimination laws.

3. Stakeholder Concerns

- Stakeholder feedback: Is it possible to state that discrimination against individuals covered by the Washington State definition of protected class is prohibited?
    - Port staff response: Updated recommendations 13a & b.

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 biometric 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).[6]

The Welcoming Port Policy commits the Port to "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 to 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."

To that end, it is essential that any use of biometrics for traveler functions at Port facilities address whether and how any data collected will be shared with federal agencies or law enforcement or used for any purpose other than the explicit travel function.

2. Working Group Recommendations

"Ethical" recommendations at a glance	
Port	Private Sector Operators
• If the Port approves the implementation of any use of biometrics for traveler functions, the Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about that biometric program. • If the Port approves the implementation of any use of biometrics for traveler functions, the Port should require that private sector operators do not disclose personal data obtained from a biometric system to a federal or law enforcement agency, except when such disclosure is required or necessary. • If the Port approves any use of biometrics for traveler functions, the Port should work with local jurisdictions, nonprofit organizations and others to inform local immigrant and refugee	• If the Port approves the implementation of any use of biometrics for traveler functions, the Port should work with participating private sector operators to inform local immigrant and refugee communities, in multiple languages and in culturally appropriate ways, about resources for 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.

[6] https://www.portseattle.org/sites/default/files/2018-05/2018_05_08_SM_8a_reso.pdf

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. • The Port should form a Technology Ethical Advisory Board – composed of community stakeholders, academics, technology experts and other key stakeholders – to advise on the ethical issues raised by implementation of biometric technology and other innovations.	

For Port

Recommendation 15: If the Port approves the implementation of any use of biometrics for traveler functions, the Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about that biometric 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 16: If the Port approves the implementation of any use of biometrics for traveler functions, the Port should require that private sector operators do not disclose personal data obtained from a biometric system to a federal or law enforcement agency, except when such disclosure is:

- Pursuant to the consent of the consumer to whom the personal data relates;
- Required by federal, state, or local law or in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury;
- Necessary to prevent or respond to a national security issue or an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the operator; or
- To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec.2258A.

Recommendation 17a: If the Port approves any use of biometrics for traveler functions, 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.

Recommendation 18: The Port should form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations. This advisory board should be consulted on a regular basis to ensure that Port technology implementation – specifically new biometrics programs – are fully aligned with this principle.

For Private Sector Operators

Recommendation 17b: If the Port approves the implementation of any use of biometrics for traveler functions, the private sector operators should work with the Port to inform local immigrant and refugee communities, in multiple languages and in culturally appropriate ways, about resources for 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.

3. Stakeholder Concerns

TBD

Port of Seattle

Attachment D – Policy Recommendations for Biometrics for Traveler Functions Using Government Systems

1. BASICS OF BIOMETRICS FOR TRAVELER FUNCTIONS USING GOVERNMENT SYSTEMS

Many private sector operators at Port facilities believe that biometrics offer an important tool to expedite traveler functions, such as bag check and ticketing. These functions are driven entirely by perceived business need and benefit, and not required by any local, state or federal government regulation. The COVID-19 pandemic may spur additional attention toward potential applications of biometric technology so as to avoid direct interactions that could spread the virus.

While most private sector uses would not be relevant to this use case, there are limited examples where a private sector entity might wish to use an existing government biometrics system, such as an airline using CBP's TVS system for international departing passenger ticketing or bag check.[7] The Port itself could also choose to utilize biometrics for traveler functions, such as access to its parking garage; again, COVID-19 prevention is bringing additional consideration of this possibility. Any Port use of biometrics utilizing a Port-controlled system is by definition a use of a government system, and therefore included in this use case.

In March 2020, the Washington State Legislature passed legislation explicitly setting policy guidelines for use of facial recognition biometrics by state and local governments; the policies for Port uses outlined below are fully aligned with that legislation, not just for facial recognition but for all biometrics.[8]

The State of Washington did not pass legislation regulating private sector usage in 2020. However, where possible, the policy recommendations below reflect many of the policies that were considered, so that – if state laws are eventually enacted regulating private sector use of facial recognition biometrics – Port policies will already either meet or exceed those thresholds.

2. APPLYING THE PORT'S PUBLIC-FACING BIOMETRICS GUIDING PRINCIPLES TO BIOMETRICS FOR TRAVELER FUNCTIONS USING GOVERNMENT SYSTEMS

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) requiring an explicit operational reason 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 reason, proponents can point to increased processing speeds and customer conveniences such as not having to take travel documents out. In addition, the COVID-19 pandemic may spur additional attention toward potential applications of biometric technology so as to avoid direct interactions that could spread the virus. However, there needs to be a net benefit for the use of this technology to be considered

[7] TVS is a system of related databases operated by CBP containing the biometric facial recognition "template" of individuals that are ticketed on international flights.

[8] http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200316151028

a justified use; in other words, the benefits should outweigh potential costs like cybersecurity, data privacy risks, and any potential harm that travelers might experience.

The Port does not condone mass surveillance, and so any proposed biometrics would only fit this definition if all biometric capture was done with travelers' awareness and willing participation. Recommendations for protecting against unintended image capture of other individuals are included under the Voluntary principle.

2. Working Group Recommendations

"Justified" recommendations at a glance	
Port	Private Sector Operators
• If a Port Managing Director receives a request for private sector implementation of biometrics for travel functions using CBP's TVS system, the Managing Director should only consider the request if a Biometric Exit program has already been implemented. If Biometric Air Exit is already occurring, then the Managing Director must seek feedback from the Technology Ethical Advisory Board and consider set criteria in deciding whether or not to approve the additional implementation. • If the Managing Director plans to approve the private sector request after considering all the above criteria, they must first notify the Port Executive Director and the Port Commission at least three (3) weeks before providing that formal approval to the private sector applicant. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through performance evaluation. • If Port staff request to implement a public-facing biometric system at Port facilities using a Port-controlled system or using CBP's TVS system for purposes other than "Biometric Air Exit" or "Biometric Air & Cruise Entry", they must first seek approval from their Managing Director, who must seek feedback from the Technology Ethical Advisory Board and consider set criteria in deciding whether or not to approve the implementation. • Port staff may not propose to implement biometrics explicitly for marketing or	• A private sector operator proposing to implement biometrics for traveler functions at Port facilities using a proprietary system must receive approval from the relevant Managing Director.

advertising purposes, unless it meets set criteria. • If Port staff receive approval from the Managing Director, they must then submit a notice of intent to the Port Commission and commence an accountability report process as defined in state law. • After the accountability report process is completed as described above, if the proposed implementation of biometrics for traveler functions by Port staff does not require a Commission authorization, the Managing Director must notify the Port Executive Director and the Port Commission at least three (3) weeks before the technology is procured. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through performance evaluation. • If the proposed implementation of biometrics for traveler functions by Port staff requires a procurement, then the vendor solicitation document must include a request for explanation of how the technology will comply with the Port's Biometric Principles and policies. • If the requested implementation of biometrics by Port staff does require a Commission authorization, then the Commission memo must include the final accountability report, an explanation of how the proposal complies with the Port's Biometric Principles and policies, a recommendation from the relevant Managing Director on how and why this request meets the Justified principle and any feedback from the Technology Ethical Advisory Board.	

For Port

Recommendation 1a: If the Aviation Managing Director or Maritime Managing Director receives a request for private sector implementation of biometrics for travel functions using CBP's TVS system, the Managing Director should only consider the request if a Biometric Exit program has already been implemented. If Biometric Air Exit

is already occurring, then the Managing Director must seek feedback from the Technology Ethical Advisory Board and consider the following criteria in deciding whether or not to approve the additional implementation:

- Demonstrated operational benefit, which is defined as increased efficiency or effectiveness in passenger processing vs existing manual processes
- Compliance with all Port principles and policies
- Compliance with all CBP requirements, such as documentation that the proposed process has been approved by CBP, and is in compliance with CBP's Biometric Air Exit Requirements and TVS application programming interface (API) specifications.
- Alignment with the Port's Equity, Diversity and Inclusion standards
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation vs. potential privacy and other risks. If the risks are deemed significant, then the Managing Director should deny the application regardless of the net-benefit calculation; "significant risk" should be clearly defined in partnership with the Technology Ethical Advisory Board, to include harms based on equity impacts.

Recommendation 2: If the Managing Director plans to approve the request after considering all the above criteria, they must first notify the Port Executive Director and the Port Commission at least three (3) weeks before providing that formal approval to the private sector applicant. This notification is for the purpose of the Executive Director and/or Commission to ask additional questions, request a delay in approval until additional information is received, and/or reject the Managing Director's recommendation for approval. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through performance evaluation.

Recommendation 1b: If Port staff request to implement a public-facing biometric system at Port facilities using a Port-controlled system or using CBP's TVS system for purposes other than "Biometric Air Exit" or "Biometric Air & Cruise Entry", they must first seek approval from their Managing Director, who must seek feedback from the Technology Ethical Advisory Board and consider the following criteria in deciding whether or not to approve the implementation:

- Demonstrated operational benefit, which is defined as increased efficiency or effectiveness in passenger processing vs existing manual processes
- Compliance with all Port principles and policies
- Compliance with all CBP requirements if using the CBP TVS system, such as documentation that the proposed process has been approved by CBP, and is in compliance with CBP's Biometric Air Exit Requirements and TVS application programming interface (API) specifications.
- Alignment with the Port's Equity, Diversity and Inclusion standards
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation vs. potential privacy and other risks. If the risks are deemed significant, then the Managing Director should deny the application regardless of the net-benefit calculation; "significant risk" should be clearly defined in partnership with the Technology Ethical Advisory Board, to include harms based on equity impacts.

Recommendation 1c: Port staff may not propose to implement biometrics explicitly for marketing or advertising purposes, unless:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;

- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and
- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

Recommendation 3: If Port staff receive approval from the Managing Director, they must then submit a notice of intent to the Port Commission and commence an accountability report process as defined in state law that publicizes key aspects about the biometric technology, such as the name of the service, vendor, and version; a description of its general capabilities and limitations; the type or types of data inputs that the technology uses; how that data is generated, collected, and processed; a description of the purpose and proposed use of the technology, including what decision or decisions will be used to make or support it; a clear use and data management policy; any complaints or reports of bias regarding the service received by the vendor; testing procedures; information on the service's rate of false matches; a description of any potential impacts of the service on civil rights and liberties; and procedures for receiving feedback from individuals affected by the use of the service and from the community at large.

Prior to finalizing the accountability report, the Port must – in compliance with state law – allow for a public review and comment period; hold at least three community consultation meetings; and consider the issues raised by the public through the public review and comment period and the community consultation meetings. The final adopted accountability report must be clearly communicated to the public at least ninety days prior to the Port putting the service into operational use, and be posted on the Port's website.

Recommendation 4: After the accountability report process is completed as described above, if the proposed implementation of biometrics for traveler functions by Port staff does not require a Commission authorization[9], the Managing Director must notify the Port Executive Director and the Port Commission at least three (3) weeks before the technology is procured. This notification is for the purpose of the Executive Director and/or Commission to ask additional questions, request a delay in approval until additional information is received, and/or reject the Managing Director's recommendation for approval. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies or 2) multiple violations of Port policies as identified through performance evaluation.

Recommendation 5: If the proposed implementation of biometrics for traveler functions by Port staff requires a procurement, then the vendor solicitation document must include a request for explanation of how the technology will comply with the Port's Biometric Principles and policies.

Recommendation 6: If the requested implementation of biometrics by Port staff does require a Commission authorization[10], then the Commission memo must include the final accountability report, an explanation of how the proposal complies with the Port's Biometric Principles and policies, a recommendation from the relevant Managing Director on how and why this request meets the Justified principle and any feedback from the Technology Ethical Advisory Board.

<u>For Private Sector Operators</u>

Recommendation 1d: A private sector operator proposing to implement biometrics for traveler functions at Port facilities using CBP's TVS system must receive approval from the Aviation or Maritime Managing Director. The

[9] Commission authorization is required for procurements valued at or above $300,000.
[10] Ibid.

request for this implementation must articulate how the operator will comply with the Port's Biometric Principles and any associated policies governing the use of biometric technology at Port facilities, how the proposal complies with CBP's protocols, and why biometrics are justified, using the above-listed criteria.

3. Stakeholder Concerns

- Stakeholder feedback: Need to confirm what authority the Aviation Managing Director has over private sector vendors if a request is denied.
    - Port response: The Port has the ability to utilize lease agreements and other operating agreements to set standards that impact the overall customer experience at the airport, and so a denial of such a request would be enforceable.

- Stakeholder feedback: Justified principle should apply an equity perspective and should go beyond "operational benefit" to address and advance justice.
    - Port staff response: Added a criterion in recommendations 1a & 1b that the application should be in alignment with the Port's Equity, Diversity and Inclusion standards
    - Added a requirement in recommendations 1a & 1b that – if the risks are deemed significant – then the Managing Director should deny the application regardless of the net-benefit calculation.

- Stakeholder feedback: The Managing Directors have a lot of power to approve or deny; is there anyone else with veto power?
    - Port staff response: The Executive Director and Commission. Made this more explicit in recommendations 2 & 4.

- Stakeholder feedback: The phrase "if the risks are deemed significant" should be clearly defined around a set of criteria, most importantly including equity impacts.
    - Port staff recommendation: Added a process for developing that definition in recommendations 1a and 1b.

- Stakeholder feedback: The Port should not allow the use of biometrics-based advertising technology.
    - Port staff recommendation: Port staff appreciates the concerns, but rather than explicitly ban a particular function we believe we should very clearly define how such a function would only be in compliance with Port principles and policies in very limited scenarios. Added recommendation 1c.

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.

The Port should not approve any applications for biometrics for traveler functions at Port facilities that are not opt-in for travelers, unless there is a mandate to do so – such as from a federal agency or a public health entity. In this context, opt-in refers to both opting-in to the overall system (enrolling your biometrics in a database or gallery) as well as choosing to participate in the system at the point of service (i.e. – at the ticketing counter).

In these limited scenarios for which opt-out is mandated, the Port should require reasonable provisions for those travelers that would like alternate accommodations.

As related to image capture, the Port can specify requirements for the physical configuration and other aspects of the technology in an effort to prevent unintended image capture during biometric operations. Similarly, the Port should set standards for how unintended images are removed from the system.

2. Working Group Recommendations

"Voluntary" recommendations at a glance	
Port	Private Sector Operators
• The Port should not approve any applications for biometrics for traveler functions are not "opt-in", unless there is a legally-required mandate to do. In the limited scenarios for which opt-out is mandated, the Port should require reasonable provisions for those travelers that would like alternate accommodations. Opting-in also must include comprehensive, clear, and accessible notice at the time of enrollment (i.e. – "informed consent") for individuals to know exactly what they are opting-in for. • Port staff may not refer to a system as "opt-in" unless it meets set criteria. • The Port should develop guidelines for where and how biometrics can be used at Port facilities, including standards for "opt-in" and "opt-out", standards to avoid unintended image capture if facial recognition (or a similar image-based biometrics system) is implemented, as well as standards for how to handle biometric data accidentally collected by unintended capture. • As part of an application for use of biometrics for traveler processing at Port facilities, Port staff must submit a plan for meeting the Port's "opt-in" or "opt-out guidelines, as well as for minimizing unintended capture (if an image is used as part of the biometrics).	• A private sector operator may not refer to a system as "opt-in" unless it meets set criteria. • As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must submit a plan for implementing "opt-in" or "opt-out" aligned with Port guidelines, and for minimizing unintended capture of biometrics aligned with Port standards. • As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must demonstrate that their employees have received training aligned with the Port's guidelines.

• If the Port approves the implementation of biometrics for traveler functions by Port staff that requires a procurement, then the vendor proposal must include how its technology can help minimize the unintended capture of images of nontravelers or visitors, if an image is used as part of the biometrics. • The Port should not approve any applications for biometrics for traveler functions that scan individuals or groups without their knowledge and active participation. In particular, the Port should not approve any applications that operate by scanning large groups of people in order to identify those individuals who have opted in. • If the Port approves any implementation of public-facing biometrics at Port facilities, the Port should design training standards for all users of biometric technology that includes the abovementioned guidelines. • As part of an application for use of biometrics for traveler functions at Port facilities, Port staff must demonstrate that they have received training aligned with the Port's abovementioned guidelines.	

For Port

Recommendation 7a: The Port should not approve any applications for biometrics for traveler functions are not "opt-in", unless there is a legally-required mandate to do – such as from a federal agency or a public health entity. In the limited scenarios for which opt-out is mandated, the Port should require reasonable provisions for those travelers that would like alternate accommodations. In this context, opt-in refers to both opting-in to the overall system (enrolling your biometrics in a database or gallery) as well as actively participating in the system at the point of service. Opting-in also must include comprehensive, clear, and accessible notice at the time of enrollment (i.e. – "informed consent") for individuals to know exactly what they are opting-in for, how their data will be handled and protected and their rights to remove their data from the system.

Recommendation 7b: Port staff may not refer to a system as "opt-in" unless:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;
- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and

- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

Recommendation 8a: The Port should develop guidelines for where and how biometrics can be used at Port facilities. In particular, these guidelines should include:

- Standards for "opt-in" and "opt-out" to ensure a consistent customer experience, including how to cancel a subscription or other voluntary commitment such that an individual's biometric data is removed from the system; and
- Standards to avoid unintended image capture if facial recognition (or a similar image-based biometrics system) is implemented (such as by positioning a 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), as well as standards for how to handle biometric data accidentally collected by unintended capture.

Recommendation 8b: As part of an application for use of biometrics for traveler processing at Port facilities, Port staff must submit a plan for meeting the Port's "opt-in" or "opt-out guidelines, as well as for minimizing unintended capture (if an image is used as part of the biometrics).

Recommendation 9: If the Port approves the implementation of biometrics for traveler functions by Port staff that requires a procurement, then the vendor proposal must include how its technology can help minimize the unintended capture of images of nontravelers or visitors, if an image is used as part of the biometrics.

Recommendation 10: The Port should not approve any applications for biometrics for traveler functions that scan individuals or groups without their knowledge and active participation. In particular, the Port should not approve any applications that operate by scanning large groups of people in order to identify those individuals who have opted in.

Recommendation 11a: If the Port approves any implementation of public-facing biometrics at Port facilities, the Port should design training standards for all users of biometric technology that includes the abovementioned guidelines.

Recommendation 11b: As part of an application for use of biometrics for traveler functions at Port facilities, Port staff must demonstrate that they have received training aligned with the Port's abovementioned guidelines.

For Private Sector Operators

Recommendation 7c: A private sector operator may not refer to a system as "opt-in" unless:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;
- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and
- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

Recommendation 8c: As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must submit a plan for implementing "opt-in" or "opt-out" aligned with Port standards, and for minimizing unintended capture of biometrics aligned with Port guidelines.

Recommendation 11c: As part of its application for biometrics for traveler functions at Port facilities, a private sector operator must demonstrate that their employees have received training aligned with the Port's guidelines.

3. Stakeholder Concerns

- Stakeholder feedback: Opt-in option gives every traveler a choice. Clarify if Port will set "opt-in" standards/definition. If not, private operators should provide standards in request plan.
    - Port response: Added to recommendations 7a, b & c and 8a, b & c.

- Stakeholder feedback: Explain redress for unintended capture.
    - Port response: Updated recommendation 8a.

- Stakeholder feedback: Comprehensive training should be reviewed and authorized by all parties to minimize risks to the consumer.
    - Port response: Port training standards will be made public as part of the accountability report process.

- Stakeholder feedback: What to do regarding cruise embarkation & disembarkation not at port facilities, when does the port lose its authority?
    - Port response: The Port has the ability to utilize lease agreements and other operating agreements to set standards that impact the overall customer experience at Port-controlled facilities. The Port does not have the ability to regulate activities outside of Port-controlled facilities, such as on an airplane or cruise ship or in a CBP Federal Inspection Services (FIS) area.

- Stakeholder feedback: Although the system is opt-in, it is unclear how or the extent to which a consumer can voluntarily remove themselves from the system.
    - Port staff response: This is explicitly included in Recommendation 8a and 19a.

- Stakeholder feedback: Regarding recommendation 7a, "consensus national best practice" does not seem limiting enough and should be refined.
    - Port staff response: This phrase has been removed.

- Stakeholder feedback: The language around a mandate to do "opt-out" should be more specific.
    - Port staff response: Updated recommendation 7a.

- Stakeholder feedback: Recommendation 10 should explicitly ban all mass scanning, which is surveillance.
    - Port staff response: Only those individuals who are actively participating should be included in biometric data collection. Updated the recommendation accordingly.

- Stakeholder feedback: Opting-in to the system should include there being a voluntary subscription, and that the operators should not collect biometrics using an involuntary method.
    - Port staff response: Added recommendations 7b & 7c to make this explicit.

- Stakeholder feedback: What does it mean to "opt-in at the point of service"?
    - Port staff response: Opting-in at the point of service is meant as "actively participating in using the biometrics" (vs. being scanned without your awareness); it is not meant to imply that you have to sign up for the service each time you use it. Opting-in to the enrollment process

happens once, and is defined here as choosing to provide your biometrics into the system/gallery. Adjusted recommendation 7a to make this more clear.

- Stakeholder feedback: Add a recommendation that includes comprehensive, clear, and accessible notice for passengers to know exactly what they are opting-in for at the time of enrollment.
    - Port staff response: Updated recommendation 7a.

- Stakeholder feedback: Need mechanisms for how to address what happens when unintended capture occurs.
    - Port staff response: Updated recommendation 8a.

- Stakeholder feedback: Should have an explicit requirement about the ability for individual to withdraw from the system.
    - Port staff response: Updated recommendation 8a.

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 implementation. Individuals want to know that their data is secure, not being used for any inappropriate purpose, and protected.

For Port controlled activities, the Port has the ability to set and enforce minimum data privacy and cybersecurity standards. For private sector operators proposing to use CBP's TVS system as part of the biometric implementation for traveler functions, CBP has published a Privacy Impact Assessment report that outlines its efforts to protect data privacy,[11] and requires operators to sign a Business Requirement document committing to follow those private guidelines. For example, CBP's business requirements do not permit its private sector partners to retain or share the photos captured. However, the enforcement of these business requirements is currently the sole responsibility of CBP; there is no present mechanism for the Port to enforce these business requirements.

The issue of giving individuals an opportunity to challenge violations of their rights is covered under the Ethical principle.

2. Working Group Recommendations

"Private" recommendations at a glance	
Port	Private Sector Operators

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

• The Port should develop biometric data security and privacy guidelines for biometrics for traveler functions. • For any proposed implementation of biometrics for traveler functions by Port staff using a Port-controlled system, the proposal must meet or exceed the Port's minimum biometric data security and privacy standards. • For any Port implementation of biometrics for traveler functions that requires a procurement, all vendor proposals must include an explanation of how the technology solution will meet the Port's biometric Privacy principles and policies, including by providing relevant privacy policies, data collection and storage practices, and cybersecurity practices. • The Port should endeavor to seek clarification from the State of Washington Attorney General whether Port collection and transmission of biometric data at Port facilities is exempt from state public disclosure requirements, so as to protect personally identifying information from release. • Any Port staff implementation using CBP's TVS system must meet all of CBP's Biometric Requirements regarding encryption and other security standards.	• Any implementation using CBP's TVS system must meet all of CBP's Biometric Requirements regarding encryption and other security standards.

For Port

Recommendation 12a: The Port should develop minimum biometric data security and privacy standards for biometrics for traveler functions at Port facilities. Those standards should address data privacy protections at the point of service as well as throughout the proprietary system, such as potential data breach and data sharing. The standards should include requirements that any data collected should be used only for those purposes explicitly communicated to those individuals who participate in the biometric process, and that unauthorized third parties will not have access to or be sold any such data. These guidelines should be based – to the extent possible – on national and global standards already developed for evaluating the security of these technologies, such as the Center for Internet Security's Controls and Benchmarks or any relevant statues from the California Consumer Privacy Act, the European Union General Data Protection Regulation or Section 15 of the State of Illinois' Biometric Information Privacy Act.

Recommendation 12b: For any proposed implementation of biometrics for traveler functions by Port staff using a Port-controlled system, the proposal must meet or exceed the Port's minimum biometric data security and privacy standards.

Recommendation 12c: For any Port implementation of biometrics for traveler functions that requires a procurement, all vendor proposals must include an explanation of how the technology solution will meet the Port's biometric Privacy principles and policies, including by providing relevant privacy policies, data collection and storage practices, and cybersecurity practices.

Recommendation 13: The Port should endeavor to seek clarification from the State of Washington Attorney General whether Port collection and transmission of biometric data at Port facilities is exempt from state public disclosure requirements, so as to protect personally identifying information from release.

Recommendation 14a: For any proposed Port implementation of biometrics for traveler functions using CBP's TVS system other than for "Biometric Air Exit" or "Biometric Air or Cruise Entry", use of biometric data must meet all of CBP's Biometric Requirements regarding encryption and other security standards; data must be deleted in accordance with CBP's Biometric Requirements; and unauthorized third-parties should not be provided access to any such data as stated in the CBP Biometric Requirements.

For Private Sector Operators

Recommendation 14b: For any proposed private sector implementation of biometrics for traveler functions using CBP's TVS system, use of biometric data must meet all of CBP's Biometric Requirements regarding encryption and other security standards; data must be deleted in accordance with CBP's Biometric Requirements; and unauthorized third-parties should not be provided access to any such data as stated in the CBP Biometric Requirements.

3. Stakeholder Concerns

- Stakeholder feedback: Identify international best practices regarding data privacy standards
    - Port response: Recommendation 12a has been updated to recognize existing standards from which to build off.

- Stakeholder feedback: Need to consider privacy impacts both at the point of service & externalities regarding data usage and protection beyond the system.
    - Port staff response: Added this explicitly into Recommendation 12a.

- Stakeholder feedback: Should clearly call out that a private entity cannot sell your data to a third-party entity for any purpose.
    - Port staff response: Added to recommendation 12a.

- Stakeholder feedback: We should include Illinois' Biometric Privacy Act as a source for such policies.
    - Port staff response: Section 15 of the law is the one that deals with retention; collection; disclosure; and destruction of biometric information. It seems to be already quite aligned with the Port's proposed policies, and so we have added a reference to that section.

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 biometrics (specifically facial recognition technology) does not perform as effectively on individuals who are not male Caucasians, and that 2) regardless of why the technology identifies a mismatch, systems should be in place to resolve the issue with minimal impact to the traveler.

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.[12] However, the NIST report does identify some algorithms, such as the NEC algorithm used by CBP in its Biometric Entry/Exit program, as highly effective in terms of accuracy rates – both overall and across multiple characteristics.

The NIST report provides an important baseline for performance levels that proposed implementations of biometric technology at Port facilities must meet to be considered for approved use at Port facilities. For those proposed implementations that involve use of the CBP TVS system, the Port can work directly with CBP to understand system performance and accuracy. The Port also has an obligation to institute and/or ensure compliance with standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality.

Treating no-matches or mismatches with "cultural sensitivity and discretion" requires that individuals subject to additional document review are treated 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. Where possible, mismatch issues should be handled at the point of service rather than removal to a secondary location.

2. Working Group Recommendations

"Equitable" recommendations at a glance	
Port	Private Sector Operators
• The Port should develop biometric training guidelines for personnel who will be administering biometric technology on travelers. The training must include – but not be limited to – the capabilities and limitations of biometrics, as well as how to deal with mismatching issues with sensitivity and discretion. • When requesting implementation of biometrics for traveler functions, Port staff must verify that they have been trained on operating biometrics to the Port's training guidelines, including understanding of the capabilities and limitations of biometrics, and how to deal with mismatching issues with sensitivity and discretion. • When requesting implementation of biometrics for traveler functions, Port staff	• When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their employee training for operating biometrics meets the Port's training guidelines, including understanding of the capabilities and limitations of biometrics, and how to deal with mismatching issues with sensitivity and discretion. • When requesting implementation of biometrics for traveler functions, private sector operators must verify that their technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington state definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions.

[12] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

must verify that the technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington state definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions. • If the desired implementation of biometrics for traveler functions by Port staff requires a procurement, then the vendor proposal must include an explanation of how it will meet the Port's Equity principle and policies. Vendors will need to provide, to the extent applicable, information regarding how their equipment and services enhance, to the extent possible, accuracy levels in identifying peoples of all backgrounds, gender, and age. • Port staff requesting implementation of biometrics for customer functions must agree as a part of their application to 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. • The Port should request updated accuracy rates from CBP – including a request for any available data segmented by key traveler characteristics – before approving any proposed use of biometrics for traveler functions that would use the CBP TVS system.	• A private sector operator requesting implementation of biometrics for traveler functions must agree as a part of its application to 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.

For Port

Recommendation 15a: The Port should develop biometric training guidelines for personnel who will be administering biometric technology on travelers. The training must include – but not be limited to – the capabilities and limitations of biometrics, as well as how to deal with mismatching issues with sensitivity and discretion; the Port's Office of Equity, Diversity and Inclusion should be an active participant in ensuring culturally appropriate procedures for handling such issues. For example, the training should suggest that – where possible – mismatch issues should be handled at the point of service rather than removal to a secondary location. The training should also include standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality.

Recommendation 15b: When requesting implementation of biometrics for traveler functions, Port staff must verify that they have been trained on operating biometrics to the Port's training guidelines, including understanding of the capabilities and limitations of biometrics, and how to deal with mismatching issues with sensitivity and discretion.

Recommendation 16a: When requesting implementation of biometrics for traveler functions, Port staff must verify that the technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington state definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions. "High levels of accuracy" should be defined not only relative to correctly matching the person with their image but also as an accuracy rate that is at least as good as human review. Port staff should include in their disclosure of accuracy rates the specific device and system settings – such as similarity thresholds – that maximize accuracy and provide the proper balance of accuracy, equity and security.

Recommendation 16b: If the desired implementation of biometrics for traveler functions by Port staff requires a procurement, then the vendor proposal must include an explanation of how it will meet the Port's Equity principle and policies. Vendors will need to provide, to the extent applicable, information regarding how their equipment and services enhance, to the extent possible, accuracy levels in identifying peoples of all backgrounds, gender, and age.

Recommendation 17a: Port staff requesting implementation of biometrics for customer functions must agree as a part of their application to 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. Making an application programming interface or other technical capability does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data; providers bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing.

Recommendation 18: The Port should request updated accuracy rates from CBP – including a request for any available data segmented by key traveler characteristics – before approving any proposed use of biometrics for traveler functions that would use the CBP TVS system.

For Private Sector Operators

Recommendation 15c: When requesting implementation of biometrics for traveler functions, the private sector operator must verify that their employee training for operating biometrics meets the Port's training guidelines, including understanding of the capabilities and limitations of biometrics, and how to deal with mismatching issues with sensitivity and discretion.

Recommendation 16c: When requesting implementation of biometrics for traveler functions, private sector operators must verify that their technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington state definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions. "High levels of accuracy" should be defined not only relative to correctly matching the person with their image but also as an accuracy rate that is at least as good as human review. Where possible within CBP regulations, the operator should include in their disclosure of accuracy rates the specific device and system settings – such as similarity thresholds – that maximize accuracy and provide the proper balance of accuracy, equity and security.

Recommendation 17b: A private sector operator requesting implementation of biometrics for traveler functions must agree as a part of its application to 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. Making an application programming interface or other technical capability does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data; providers bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing.

3. Stakeholder Concerns

- Stakeholder feedback: Identify comprehensive list of "various characteristics" as stated in recommendation 16.
    - Port response: Updated to reference federal definition.
    - Stakeholder response: Recommendation to use Washington State's definition of "protected class" rather than the federal definition. Selection should be made for the protected classes that are most relevant to biometric (including facial recognition) accuracy.
    - Port staff response: Changed to state definition.

- Stakeholder feedback: Recommendation 17 regarding making available technical abilities for independent testing is too broad.
    - Port response: Updated the language to reflect the final version of the state law regulating local government use of facial recognition.

- Stakeholder feedback: In general, high accuracy rates should not be a definition for equity. What constitutes a "high accuracy rate" needs to be clear, implementable, and considerate of relative differences between groups.
    - Port staff response: Added equity as a fundamental criterion under recommendations 1a and 1b. Port staff is open to using a more specific definition of "high accuracy rate," and welcomes feedback on what that might be.

- Stakeholder feedback: Trainings should make clear that there will be consultation by civil rights organizations and made publicly available
    - Port staff response: Added the Port's Office of Equity, Diversity and Inclusion to this process in recommendation 15a; making the training guidelines public is already listed in recommendation 20a.

- Stakeholder feedback: The Port needs to set an "acceptable" level of difference between overall accuracy rates, and the accuracy rate of the system for various demographics (i.e. – how much less accurate can the system be for people of color and yet still be approved).
    - Port staff response: As referenced above, the Port requires the system to be "highly accurate" for all groups, both overall and within specific demographics. We are still open to suggestions for making this more quantifiable, but no system will be approved that isn't highly accurate for all individuals.

- Stakeholder feedback: Accuracy rates should be publicly communicated, specifically regarding how accurate the system is for differing groups.
    - Port staff response: This is included in the annual accountability report.

- Stakeholder feedback: Would like to see language here about what oversight there will be over similarity thresholds as different thresholds will skew towards either false matches or mismatches.
    - Port staff response: Added language to recommendations 16a and 16c, and to the accountability report in recommendation 20a for public disclosure.

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 public-facing use of biometrics at Port facilities to be clearly communicated to anyone visiting Port facilities, 2) the need to ensure that travelers participating in biometrics are informed in a clear, concise manner about how the biometrics are used, and their rights related to the system, and 3) the need for accountability reports to be created and published for the public. This requires clear, consistent and standardized communications protocols, in coordination with private sector operators.

Similarly, information about the system must be continuously verified. Performance data should be a key aspect of the Port's review of any biometric implementation taking place at its facilities, and publicly verified and approved findings should be made public.

2. Working Group Recommendations

"Transparent" recommendations at a glance	
Port	Private Sector Operators
• If the Port approves the implementation of biometrics for traveler functions, it should develop a comprehensive communications plan that notifies the general public of the implementation and all related information. • If the Port approves the implementation of biometrics for traveler functions, the Port should produce an annual accountability report that includes all approved, publicly available information. • The Port should periodically conduct its own performance evaluation, within the limitations of its authority, to ensure that Port employees and/or private sector operators are following all Port policies.	• If the Port approves the implementation of any biometrics for traveler functions, the private sector operators should partner with the Port on implementation of the Port's biometrics communications plan. • If the Port approves the implementation of any biometrics for traveler functions, the private sector operator should share to the extent possible all requested information for inclusion in the accountability report. The operator should also share, to the extent possible, the Port's annual accountability report through relevant communications channels.

For Port

Recommendation 19a: If the Port approves the implementation of any biometrics for traveler functions, it should develop a comprehensive communications plan that notifies the general public of the implementation and all related information, including their rights with regard to the program, how to remove themselves from the program if possible, and recourse in case of violations of those rights and/or data breaches. The communications plan should include specific communications on-site, including announcements, signage, flyers and web content. The communications plan should include effort to reach local immigrant and refugee communities – in multiple languages and in culturally appropriate ways; languages should be determined based on the most common ones spoken by airport and/or cruise passengers and – if at the airport – also languages appropriate to the specific flight (as per feedback from airlines and cruise lines, as well as federal "origin and destination" data).

Recommendation 20a: If the Port approves the implementation of any biometrics for traveler functions, the Port should work with its Technology Ethical Advisory Board to 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;
- A clear use and data management policy, including protocols for:
    - How and when the service will be deployed or used and by whom including, but not limited to, the factors that will be used to determine where, when, and how the technology is deployed, and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances.
    - Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose or purposes for which the service will be used;
    - Data integrity and retention policies applicable to the data collected using the service, including how the operator will maintain and update records used in connection with the service, how long it will keep the data, and the processes by which data will be deleted;
- The Port and the private sector operator's privacy guidelines, as well as CBP's privacy guidelines if relevant;
- Traveler rights with regard to the biometric system;
- The Port's biometric training guidelines;
- The operator'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 the Port's and the operator's rules and guidelines, including complaints alleging violations;
- Any publicly available data about the accuracy and effectiveness of the system, including accuracy overall as well as accuracy for specific demographics; and, where possible, any specific device and system settings – such as similarity thresholds – that speak to how the operator is balancing accuracy, equity and security.
- Benchmarking data against the operational results of the biometric system at other ports;
- An assessment of compliance with the Port's Biometrics Principles and policies, as well as CBP's Biometric Air Exit Requirements, if relevant;

- Any Port conducted performance evaluations, as well as any publicly available CBP audits of the biometric air exit system, if relevant;
- Feedback about the public's experience, sought proactively in customer surveys, including whether travelers believe that they fully understand the information about the system;
- Any available information on data sharing within the U.S. Department of Homeland Security, such as what data is requested and by whom, within the limitations of the Port to require this information from CBP, if relevant; and
- Any private sector operator's disclosure of individuals' biometric data, within the limitations of the Port to access and disclose law enforcement activity.

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

Recommendation 21: The Port should periodically conduct its own performance evaluation, within the limitations of its authority, to ensure that Port employees and/or private sector operators are following all Port policies, including those related to privacy, customer service, traveler communication and unintended image capture. In particular, the Port should ensure that images are retained no longer than necessary, and not used only for their intended purpose. If an operator is consistently violating the Port's policies after more than two notifications asking for corrective action, the Port reserves the right to withdraw its approval of the biometric implementation.

For Private Sector Operators

Recommendation 19b: If the Port approves the implementation of any biometrics for traveler functions, the private sector operator should partner with the Port on implementation of the Port's biometrics communications plan.

Recommendation 20b: If the Port approves the implementation of any biometrics for traveler functions, the private sector operator should share to the extent possible all requested information for inclusion in the accountability report, including its assessment of compliance with the Port's principles and policies, and any known or reasonably suspected violations, including complaints alleging violations. The operator should also share, to the extent possible, the Port's annual accountability report through relevant communications channels.

3. Stakeholder Concerns

- Stakeholder feedback: Involve neutral third party in accountability report
    - Port response: Added the Technology Ethical Advisory Board to this process.

- Stakeholder feedback: Port should compile communication plan regardless if biometrics application for passenger processing is approved or not.
    - Port response: Agreed. That is a Port commitment, and will be included in an overarching biometrics policy summary once all five use cases are completed.

- Stakeholder feedback: What are the consequences for failure of the Port's performance evaluation?
    - Port response: See updated recommendation 21.

- Stakeholder feedback: Port should get an independent auditor to conduct the performance evaluations, to ensure objectivity.
    - Port staff response: Port staff appreciates the concern, but there is going to be significant transparency to the performance evaluations which should overcome any potential staff bias;

for example, the results of the performance evaluations will be published as part of the accountability report, which will be created in partnership with the Technology Ethical Advisory Board. All Port staff programs are also subject to the review of the Port's Internal Auditor, an independent office that reports to the Commission.

- Stakeholder feedback: Communications plan should be tailored to reach diverse communities, in the same way that the outreach under the Ethical principle is articulated.
    - Port staff response: Added language to recommendation 19a.

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 compliance with any relevant local, state and federal laws regarding the use of biometrics, consumer data privacy and other privacy and consumer protection laws. There are several efforts in Congress regarding regulation of biometrics use by state and local government as well as the private sector. However, there is not currently a comprehensive federal legal framework regulating biometrics and associated data; as the law develops, the Port and its private sector partners will adjust accordingly.

In March 2020, the Washington State Legislature passed legislation explicitly setting policy guidelines for use of facial recognition biometrics by state and local governments. The Port is bound to comply with these state thresholds. However, private sector activity at Port facilities is not currently addressed by state law.

For private sector operators proposing to use CBP's TVS system as part of its implementation, lawfulness also includes compliance with CBP's Business Requirements.

2. Working Group Recommendations

"Lawful" recommendations at a glance	
Port	Private Sector Operators
• Before the Port approves the implementation of biometrics for traveler functions, it must ensure that the proposal complies with all relevant state and federal laws, including privacy and discrimination laws. • Port staff should actively track, and work with stakeholders to advocate for, state and federal laws and regulations that codify the goals of the Port's biometric principles. • For Port staff proposing to use CBP's TVS system, they must also include documentation of their compliance with CBP's Business Requirements.	• As part of its application, a private sector operator must include its compliance with all relevant state and federal laws, including privacy and discrimination laws. • The Port should engage its private sector operators in its advocacy for state and federal laws and regulations that support the goals of the Port's biometric principles. • For private sector operators proposing to use CBP's TVS system, they must also include documentation of their compliance with CBP's Business Requirements.

For Port

Recommendation 22a: Before the Port approves the implementation of biometrics for traveler functions, it must ensure that the proposal complies with all relevant state and federal laws, including privacy and discrimination laws. Discrimination against individuals covered by the Washington State definition of protected class is prohibited.

Recommendation 23: Port staff should actively track and work with stakeholders, including private sector operators at Port facilities, to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.

Recommendation 24a: For Port staff proposing to use CBP's TVS system as part of its implementation of biometrics for traveler functions, they must also include documentation of their compliance with CBP's Business Requirements.

For Private Sector Operators

Recommendation 22b: As part of its application to the Port to implement biometrics for traveler functions, a private sector operator must include its compliance with all relevant state and federal laws, including privacy and discrimination laws. Discrimination against individuals covered by the Washington State definition of protected class is prohibited.

Recommendation 24b: For private sector operators proposing to use CBP's TVS system as part of its implementation of biometrics for traveler functions, they must also include documentation of their compliance with CBP's Business Requirements.

3. Stakeholder Concerns

- Stakeholder feedback: Port should continue to track State legislation regarding facial recognition services.
    - Port response: That is already included in recommendation 23.

- Stakeholder feedback: Is it possible to state that discrimination against individuals covered by the Washington State definition of protected class is prohibited?
    - Port staff response: Updated 22a & b.

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 biometric 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).[13]

The Welcoming Port Policy commits the Port to "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 to 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."

To that end, it is essential that any applications of biometrics for traveler functions at Port facilities address whether and how any data collected will be shared with federal agencies or law enforcement agencies or used for any purpose other than the traveler function.

For those operators proposing to use CBP's TVS system as part of their implementation of biometric technology at Port facilities, such an implementation would not provide CBP with any additional information that it does not already have; it already compiles galleries of travelers' facial biometrics from photos that travelers are required to submit (i.e., passport or visa application pictures). In addition, both airlines and cruise lines already provide CBP with passenger manifests and traveler data through the Advance Passenger Information System (APIS) system. That is why CBP refers to biometric exit and 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	Private Sector Operators
• The Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about any biometric programs. • The Port should require that operators do not disclose personal data obtained from a biometric system to a federal or law enforcement agency, except in certain situations. • The Port should work with local jurisdictions, nonprofit organizations and others to inform local immigrant and refugee communities about resources for sharing concerns about	• If the Port approves the implementation of any use of biometrics for traveler functions, the Port should work with participating private sector operators to inform local immigrant and refugee communities, in multiple languages and in culturally appropriate ways, about resources for 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.

[13] https://www.portseattle.org/sites/default/files/2018-05/2018_05_08_SM_8a_reso.pdf

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. • The Port should form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations.	

For Port

Recommendation 25: If the Port approves the implementation of any use of biometrics for traveler functions, the Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about that biometric 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 26: If the Port approves the implementation of any use of biometrics for traveler functions, the Port should require that operators do not disclose personal data obtained from a biometric system to a federal agency or law enforcement agency, except when such disclosure is:

- Pursuant to the consent of the consumer to whom the personal data relates;
- Required by federal, state, or local law or in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury;
- Necessary to prevent or respond to a national security issue or an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the operator; or
- To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec.2258A.

Recommendation 27a: If the Port approves any use of biometrics for traveler functions, 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.

Recommendation 28: The Port should form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations. This advisory board should be consulted on a regular basis to ensure that Port technology implementation – specifically new biometrics programs – are fully aligned with this principle.

For Private Sector Operators

Recommendation 27b: If the Port approves the implementation of any use of biometrics for traveler functions, the Port should work with participating private sector operators to inform local immigrant and refugee communities, in multiple languages and in culturally appropriate ways, about resources for 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.

3. Stakeholder Concerns

TBD

Port of Seattle

Attachment E – Policy Recommendations for Biometric Entry

1. 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."

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.

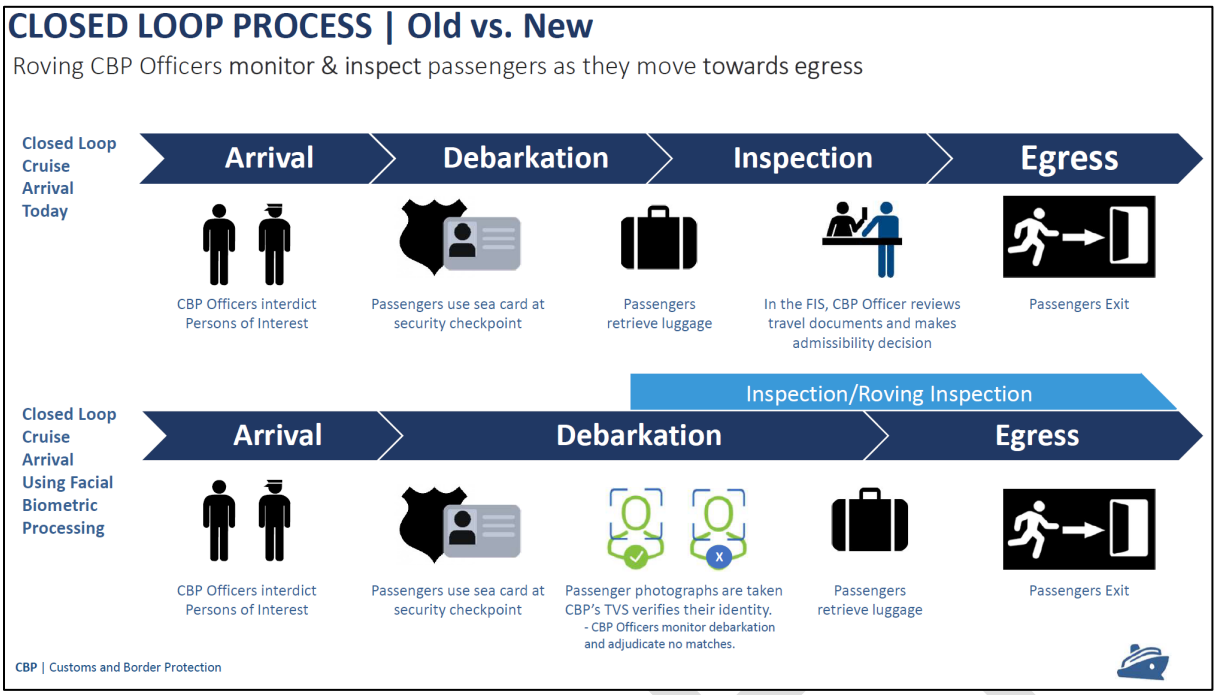
The Port of Seattle has very limited ability to influence, much less direct, the activities of CBP and the Biometric Entry process. In the Seattle region, this process will operate slightly differently between air and cruise environments. At the airport, arriving international passengers will enter the Federal Inspection Services (FIS) facility and be screened via TVS with additional screening by an in-person CBP officer[14]. At Seattle cruise terminals, biometric entry will take place either on board the cruise ship or in the cruise terminal's FIS[15]. Because Alaska cruises homeporting from Seattle are considered by CBP to be "closed loop",[16] CBP would then only conduct additional screening for select travelers[17]. 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:

[14] 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.

[15] The only current application of TVS for biometric entry 0is on-board Norwegian cruise ships at Pier 66

[16] 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.

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



2. 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 are not involved 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 include the specific federal laws and statutes that allow CBP to implement biometrics at Port facilities in the annual accountability report.	N/A

Recommendation 1: 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 include the specific federal laws and statutes that allow CBP to implement biometrics at Port facilities in the annual accountability report so that travelers and the public understand.

3. Stakeholder Concerns

- Stakeholder feedback: Recommendations regarding notification belong in Transparency, not Justified.
  - Port staff response: These recommendations have been moved accordingly.

- Stakeholder feedback: Mass surveillance is taking place any time any information is collected by the federal government, so this use case violates the Commission Principles.
  - Port staff response: The Commission Motion defines mass surveillance as use of biometrics "on large groups of people without a lawful purpose, rather than single-use for travelers." All international travel already involves submitting information to airlines and cruise lines that is shared with the federal government, and so your concern is not with biometrics but rather with the existing US homeland security policies; biometrics are only automating an existing practice. In addition, this use of biometrics is voluntary for US residents, and the Commission sees "surveillance" as something that is done involuntarily and often without people's knowledge.

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.[18] 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	
Port	CBP
If CBP implements biometric entry, the Port recommend ways for minimizing unintended image capture and should communicate those recommendations to CBP and cruise lines. The Port should design training standards to help cruise employees explain opt-out provisions.	CBP policy states that legal U.S. residents are allowed to opt-out of biometric screening

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-in 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

- Stakeholder feedback: It is essential that travelers have all information about everything involved with how their data will be used – including how it is shared within the federal government – so that they can make an informed decision about opting-out.
    - Port staff response: We will highlight the ability to opt-out, but it will be very difficult to educate most travelers about every single potential issue and risk related to participating in CBP's biometric entry program – simply because travelers are busy and have limited attention to these

[18] 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."

issues. But we will be as explicit as possible, and provide links to additional information for those travelers that want to learn. And CBP already has most of this information, so the use of biometrics only adds one additional data point to the existing process.

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.[19] 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

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

CBP's efforts related to explaining their data privacy efforts; see recommendations under the "Transparent" principle.

3. Stakeholder Concerns

- Stakeholder feedback: The Port does not have control over CBP's use of this data, so it cannot ensure that this use of the technology meets the Port's privacy standards.
    - Port staff response: The Port does not have jurisdiction over federal agencies, nor does it have the ability to prohibit CBP use of biometric entry. However, we will gain as much information as possible on CBP's privacy policies, and share that information as part of the annual accountability report. CBP is subject to federal privacy laws and regulations.

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.

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.[20] 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
The Port should request updated accuracy rates from CBP. The Port should develop suggested training recommendations for personnel administering the	The port does not have jurisdiction over the CBP algorithm or customer service protocols.

[20] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

facial recognition technology on travelers. The Port should discuss its desired customer service standards with CBP and cruise lines.	

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. For example, the training should suggest that – where possible – mismatch issues should be handled at the point of service rather than removal to a secondary location. The training should also include standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality. The Port's Office of Equity, Diversity and Inclusion and their external stakeholders should be an active participant in the development of the training guidelines to ensure culturally appropriate procedures for handling such issues, and Port customer service staff and their external stakeholders should be engaged in developing the customer service aspects of this training.

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

- Stakeholder feedback: Training recommendations should be developed in consultation with external stakeholders.
  - Port staff response: Added this to the recommendation.

- Stakeholder feedback: Accuracy does not equal equity. The definition of this principle is insufficient.
  - Port staff response: These recommendations address two issues – accuracy and cultural sensitivity when mismatches occur. We welcome additional feedback on other policy recommendations to address this principle.

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
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. If CBP implements biometric entry, the Port should produce: a) a comprehensive communications plan b) an accountability report each of which should be shared publicly through all Port communication channels. Each report should include all available information released by CBP.	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. The port cannot require CBP to share information, but CBP does provide a number of relevant reports that the Port can share publicly.

For Port

Recommendation 8a: 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.

Recommendation 9: 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. The communications plan should include effort to reach local immigrant and refugee communities – in multiple languages and in culturally appropriate ways; languages should be determined based on the most common ones spoken by airport and/or cruise passengers and – if at the airport – also languages appropriate to the specific flight (as per feedback from airlines and cruise lines, as well as federal "origin and destination" data). Where possible, the Port should partner with airlines, cruise lines and CBP to implement these communication efforts.

Recommendation 10: 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;
- The specific federal laws and statutes that allow CBP to implement biometrics at Port facilities;
- 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 Cruise Lines

Recommendation 8a: 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.

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

- Stakeholder feedback: Will the Port be able to put up their own signs in the FIS?
    - Port staff response: We do not have the authority to put signs in the FIS without CBP approval, but we will ask for their permission to do so. We will also utilize many other efforts without our control, including web and social media content, and will partner with airlines and cruise lines to get information into their pre-arrival announcements where possible. The communications will be in multiple languages.

- Stakeholder feedback: Where the technology is facial recognition, the communications should make that clear, not just "biometrics".
    - Port staff response: Agreed.

- Stakeholder feedback: The communications should not just be a positive public relations campaign for how great biometrics are.
    - Port staff response: Agreed.

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 11: Port staff should actively track and work with stakeholders to advocate for federal laws and regulations that support the Port's biometric principles. The Port should not only support general legislative principles, but also identify existing pieces of legislation to support. A list of specific bills should be submitted to the Commission as part of the annual state and federal legislative agenda for approval.

For CBP

CBP is subject to applicable federal law and regulations.

3. Stakeholder Concerns

- Stakeholder feedback: What specific legislation will the Port endorse? There are several bills that already exist.
    - Port staff response: Added additional criteria to the recommendation.

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).[21]

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 12: 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.

[21] https://www.portseattle.org/sites/default/files/2018-05/2018_05_08_SM_8a_reso.pdf

Recommendation 13: 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 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

- Stakeholder feedback: The outreach should not just be a positive public relations campaign for how great biometrics are, or an attempt to "make surveillance comfortable for vulnerable populations."
    - Port staff response: Agreed.

Attachment F – Biometric External Advisory Group Feedback on the Policy Recommendations