PORT OF SEATTLE PUBLIC-FACING BIOMETRICS POLICY

BIOMETRICS FOR TRAVELER FUNCTIONS USING GOVERNMENT SYSTEMS RECOMMENDATIONS

DRAFT AS OF JULY 24, 2020

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

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

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

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

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

Since the beginning 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.

This set of recommendations is specific to any proposed use of biometrics specifically for traveler functions that utilize government systems, excluding "Biometric Air Exit" or "Biometric Air & Cruise Entry", which are covered under separate use cases. As an example, an airline use of their own biometrics system for traveler access to their corporate lounge would not be covered under this use case, but an airline use of CBP's Traveler Verification System (TVS) for international departing passenger

ticketing or bag check is covered under this use cases. All Port-controlled uses of biometrics are covered under this use case, and policies for Port uses are fully aligned with the legislation passed by the Washington State Legislature in March of this year that set very specific standards for how and when local governments can use facial recognition technology.[1]

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

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

2. INTRODUCTION

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

It is important to note that the Port has broad authority to establish policies that govern the activities of Port staff and the use of Port resources, to the extent such policies are consistent with federal law. Private sector stakeholders operating at Port facilities are also subject to the Port's policies, to the extent that the Port's policies do not conflict with private stakeholders' own federal obligations and/or the terms of their agreements with the Port – such as lease agreements or operating agreements with the Port, which may vary on a case-by-case basis. The Port has very limited authority to influence, much less direct, the activities of federal agencies.

This set of recommendations is specific to any proposed use of biometrics for traveler functions that utilize government systems, excluding "Biometric Air Exit" or "Biometric Air & Cruise Entry", which are covered under separate use cases. As an example, an airline use of their own biometrics system for traveler access to their corporate lounge would not be covered under this use case, but an airline use of CBP's Traveler Verification System (TVS) for international departing passenger ticketing or bag check is covered under this use cases. All Port-controlled uses of biometrics are covered under this use case.

The Port has endeavored to recommend policies of general applicability wherever possible; however, some recommendations are divided into 1) recommendations that apply to the Port and 2) recommendations that apply to private sector operators utilizing CBP's TVS.

Where the Port lacks authority to mandate compliance with particular policies, the recommendation is to work collaboratively with these stakeholders to achieve voluntary compliance where appropriate, and/or highlight how these stakeholders' own policies match Port principles. The Port should also advocate for the adoption of new laws and regulations that align with the Port's biometric principles.

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

3. BASICS OF 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 the federal government. 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.[2] 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.[3]

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.

4. 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, private sector operators 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 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.

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

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

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 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 consider set criteria in deciding whether or not to approve the implementation. The Managing Director should also seek feedback from the Technology Ethical Advisory Board, once it is established. • 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. • Port staff proposing to implement biometrics for traveler functions at Port facilities using CBP's TVS system for purposes other than "Biometric Air Exit" or "Biometric Air & Cruise Entry" must receive approval from the Aviation or Maritime Managing Director. The request for this implementation must explicitly articulate the 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	• A private sector operator must explicitly articulate how the implementation will comply with the Port's Biometric Principles and policies, as well as why biometrics are preferable over existing manual processes, and the cost-benefit analysis of utilizing biometrics. • If a private sector operator requests to implement biometrics for traveler functions using the CBP TVS system, they must provide as a part of their documentation that the proposed process has been approved by CBP, specifically documenting compliance with CBP's Biometric Air Exit Requirements and TVS application programming interface (API) specifications.

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. • 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 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 where applicable
- 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.

The Managing Director should also seek feedback from the Technology Ethical Advisory Board, once it is established (see recommendation under Ethical).

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.

Recommendation 1b: If Port staff request to implement a public-facing biometric system at Port facilities using a Port-controlled system, they must first seek approval from their Managing Director, who must 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 where applicable
- 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.

The Managing Director should also seek feedback from the Technology Ethical Advisory Board, once it is established (see recommendation under Ethical).

Recommendation 1c: Port staff proposing to implement biometrics for traveler functions at Port facilities using CBP's TVS system for purposes other than "Biometric Air Exit" or "Biometric Air & Cruise Entry" must receive approval from the Aviation or Maritime Managing Director. The request for this implementation must explicitly articulate the above criteria.

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[4], the Managing Director must notify the Port Executive Director and the Port Commission at least three (3) weeks before the technology is procured.

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[5], 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 Private Sector Operators

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 request for this implementation must explicitly articulate:

- A 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 where applicable
- 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.

They must also provide as a part of their documentation that the proposed process has been approved by CBP, specifically documenting compliance with CBP's Biometric Air Exit Requirements and TVS application programming interface (API) specifications.

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 Recommendation 1a & 1b that the application should be in alignment with the Port's Equity, Diversity and Inclusion standards
    - Added a requirement in Recommendation 1a & 1b that – if the risks are deemed significant – then the Managing Director should deny the application regardless of the net-benefit calculation.

b. Voluntary

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

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 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 (i.e. – at the ticketing counter).

In these limited scenarios for which opt-out is the standard instead, reasonable provisions should still be made 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.

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 are not "opt-in", 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. In these limited scenarios for which opt-out is the standard instead, the Port should require reasonable provisions for those travelers that would like alternate accommodations. • 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	• 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.

"opt-out", and standards to avoid unintended image 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 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. • The Port should not approve any applications for biometrics for traveler functions that operate by scanning large groups of people 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.	

<u>For Port</u>

Recommendation 7: The Port should not approve any applications by private sector entities for biometrics for traveler functions are not "opt-in", 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. In these limited scenarios for which opt-out is the standard instead, the Port should require reasonable provisions for those travelers that would like alternate accommodations.

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 to a 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.

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 operate by scanning large groups of people 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 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 8a, b & c.

- Stakeholder feedback: Explain redress for unintended capture.
    - Port response: Updated recommendation 19a under Transparency related to Port performance evaluation standards.

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

- Stakeholder feedback: The Port should categorically refuse biometrics (facial/emotional recognition) for advertisement purposes.
  - Port staff response: Added Recommendation 10 to limit applications to one-to-one interactions, which would protect against the issues raised.

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 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,[6] 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.

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

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 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 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 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 and the European Union General Data Protection Regulation.

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.

For Private Sector Operators

Recommendation 14: 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.

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.[7] 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 must verify that the technology demonstrates high levels of accuracy both overall and between various characteristics – particularly	• 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.

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

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. 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.

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.

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 private sector operator's agreement to make 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 Recommendation 1a. Port staff is open to using a more specific definition of "high accuracy rate," and welcomes feedback on what that might be.

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	• If the Port approves the implementation of any biometrics for traveler functions, the private sector operators should partner with

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.	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.

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;
- Other relevant data, including any publicly available data about the accuracy and effectiveness of the system, as well as any publicly available data shared by CPB about the accuracy and effectiveness of its system, if relevant;
- 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.

For uses that involve CBP's TVS system, the report should also include information about compliance with CBP's Biometric Requirements and any related publicly-available performance data.

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.

<u>For Private Sector Operators</u>

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.

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	• 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.

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.	• 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 airlines 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.

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.

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.

Recommendation 24: 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.

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).[8]

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 private sector 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.	• 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.

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

• 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.	

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 – 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. 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

APPENDIX

Appendix A – Port Biometrics Working Group

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

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

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

- **Appendix C – Commission Biometrics Motion**

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

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

AMENDED AND ADOPTED
DECEMBER 10, 2019

INTRODUCTION

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

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

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

TEXT OF THE MOTION

Port of Seattle Principles for Public-Facing Biometric Technology
The commission hereby adopts the following principles to guide the use of public-facing biometric technology at Port of Seattle facilities:

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

(2) **Voluntary:** The use of biometrics to identify and validate travelers through port facilities should be voluntary, and reasonable alternatives should be provided for those who do not wish to participate – through a convenient "opt-in" process where possible or "optout"

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

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

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

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

(6) **Lawful:** Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including state and federal privacy and consumer data protection laws and laws prohibiting discrimination or illegal search against individuals or groups.

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

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

Biometric Working Group

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

- the strategic use and objectives of biometrics;
- procurement;
- transparency and accountability for biometric implementation;

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

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

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

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

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

STATEMENT IN SUPPORT OF THE MOTION

Due to technological advances, perceived customer benefits, and federal requirements, there will be a significant increase in public-facing facial recognition technology deployment by public and private

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

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

- Across the port, port-issued identification cards currently utilize fingerprint biometrics to access secure or restricted areas or to permit authorized personnel access to port facilities outside of normal business hours or in locations where there is no other monitoring of access. In addition, many port employees are issued iPhones with fingerprint and facial recognition as an alternative to password protection, and facial recognition is also used on Microsoft Windows 10.
- At Seattle-Tacoma International Airport (SEA), airport employees are required to scan their fingerprint at many secure doors throughout the facility. SEA also offers travelers the option of using CLEAR to validate the identity of a traveler as they process through TSA checkpoints using biometric technology instead of using traditional identification and validation methods.
- On the maritime side, biometric data is required by federal regulation for issuance of TSA-issued Transportation Worker Identification Credential (TWIC) smart cards that are required to access maritime facilities regulated by the U.S. Coast Guard and cruise terminal operational areas. In addition, the cruise industry is increasingly taking advantage of biometrics as a passenger facilitation tool; for example, Norwegian Cruise Line and CBP have partnered for use of facial recognition for disembarkation of guests at Pier 66.

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

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

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